Distribución de pesos de códigos cíclicos a partir de sumas exponenciales y curvas algebraicas

Paula Mercedes Chiapparoli

Director: Dr. Ricardo A. Podestá

Trabajo especial de
Licenciatura en Matemática

Facultad de Matemática, Astronomía, Física y Computación
Universidad Nacional de Córdoba
Argentina

Resumen

Este trabajo trata sobre el espectro o distribución de pesos de códigos lineales y cíclicos. Esto es en general una tarea ardua y sólo se conoce el espectro de algunas familias de códigos. Estudiaremos distintas formas de encontrar dichas distribuciones de pesos a través de diferentes caminos.

Primero veremos resultados generales para códigos lineales, que en particular dan una respuesta general al caso de los códigos MDS. Luego, nos enfocaremos en códigos cíclicos generales viéndolos como códigos traza (combinando los teoremas de Delsarte y las identidades de MacWilliams). A partir de aquí haremos uso de dos estrategias generales, una que involucra ciertas sumas exponenciales (Gauss, Weil y/o Kloosterman) y otra basada en el conteo de puntos racionales de curvas algebraicas asociadas a los códigos (típicamente de Artin-Schreier). Usaremos estas técnicas para obtener los espectros de familias de códigos muy conocidas como Hamming, BCH y Reed-Muller.

Finalmente, aplicaremos estos métodos a dos familias de códigos menos conocidos como los códigos de Melas y de Zetterberg. En los casos binario y ternario, el cálculo de dichos espectros se puede realizar usando curvas elípticas y la traza de operadores de Hecke de ciertas formas modulares asociadas a ellas. El trabajo contiene numerosos ejemplos, muchos de ellos nuevos.

Abstract

This work deals with the spectrum or weight distribution of linear and cyclic codes. This is in general a difficult task and the spectrum is only known for some families of codes. We will study different ways to find these distributions through different ways.

We will first see general results for linear codes, which in particular give a general answer to the case of MDS codes. Then, we will focus on general cyclic codes by viewing them as trace codes (combining Delsarte's theorems and MacWilliams identities). From this point on we will use two general strategies, one that involves certain exponential sums (Gauss, Weil or Kloosterman) and another one based on counting the number of rational points of algebraic curves (typically Artin-Schreier) associated with the codes. We will use these techniques to obtain the spectra of well-known families of codes such as Hamming, BCH, and Reed-Muller codes.

Finally, we will apply these methods to two lesser known code families, the Melas codes and the Zetterberg codes. In the binary and ternary cases, the computation of the mentioned spectra can be performed by using elliptic curves and the trace of Hecke operators of certain modular forms associated to them. The work contains several examples, many of them new.

Índice General

Introducción

En este trabajo nos interesa estudiar el espectro o distribución de pesos de códigos lineales y cíclicos.

Códigos lineales y cíclicos

Un $[n, k, d]_q$-código lineal es un subespacio $\mathcal{C} \subset \mathbb{F}_q^n$ tal que n es la longitud, k la dimensión y d la menor distancia de Hamming entre las palabras del código. El peso de una palabra código se define como la cantidad de coordenadas no nulas. Notemos que la distancia mínima coincide con el peso mínimo y, por lo tanto, $d = \min\{w(c) \,:\, c \in \mathcal{C},\, c \neq 0\}$. El código dual de $\mathcal{C}$ es $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \,:\, x \cdot c = 0, \text{ para todo } c \in \mathcal{C}\}$.

Definimos el espectro o la distribución de pesos de $\mathcal{C}$ como $Spec(\mathcal{C}) = (A_0, A_1, \ldots, A_n)$, donde

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

y su polinomio enumerador de pesos como

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

Encontrar el espectro de un código lineal no resulta sencillo y se trata de un problema abierto en general. Veremos un resultado que puede ayudarnos en ciertos casos en el capítulo 3.

Un código lineal sobre $\mathbb{F}_q$ se dice cíclico si cumple que $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ entonces $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Podemos asignarle a $c \in \mathcal{C}$ el polinomio

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R_{q,n} = \frac{\mathbb{F}_q[X]}{(X^n - 1)}.$$

Así, identificamos a los códigos cíclicos con ideales en $R_{q,n}$. Luego, existe un único polinomio mónico $g(x)$ que genera a $\mathcal{C}$ como ideal, el polinomio generador del código. Como $g(x)$ divide a $x^n - 1$, entonces existe un polinomio $h(x)$ tal que $x^n - 1 = g(x)h(x)$, el polinomio de chequeo de $\mathcal{C}$. Si $h(x)$ es irreducible, el código $\mathcal{C}$ se dice irreducible.

Sea S un $\mathbb{F}_q$-subespacio lineal de dimensión finita de $\mathbb{F}_{q^m}[X]$, entonces

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

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 $(\mathrm{Tr}(f(x)))_{x\in\mathbb{F}_{q^m}^*}$ como $(\mathrm{Tr}(f(\alpha^i)))_{i=0}^{q^m-2}$ (salvo permutaciones de coordenadas). En tal caso, si ponemos $g(x) = f(\alpha^{-1}x)$, entonces $g \in S$ y se tiene que

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

De este modo, el código

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

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, $\mathrm{Tr}(\mathcal{C}'_S) = \mathcal{C}_S$ resulta un código cíclico sobre $\mathbb{F}_q$.

Los códigos cíclicos irreducibles son de esta forma, es decir, son traza de otros códigos y, en el caso de los códigos reducibles, el teorema de Delsarte nos dice que el código dual es de esta forma. Entonces, podemos dedicarnos a encontrar la distribución de pesos de códigos traza (en el caso de los códigos reducibles, encontramos el espectro del dual y usamos la Identidad de MacWilliams para encontrar la distribución que buscamos).

Distribución de pesos de códigos cíclicos

Consideremos entonces un código $\mathcal{C}_S$. Si c es una palabra en $\mathcal{C}_S$, entonces se tiene que

$$w(c) = \#\{x \in \mathbb{F}_{q^m}^* \,:\, \mathrm{Tr}(f(x)) \neq 0\} = n - \#\{x \in \mathbb{F}_{q^m}^* \,:\, \mathrm{Tr}(f(x)) = 0\}.$$

Además, $\mathrm{Tr}(f(x)) = 0$ si y sólo si existe un $y \in \mathbb{F}_{q^m}$ tal que $y^q - y = f(x)$. Entonces, el peso $w(c)$ está estrictamente relacionado con el número de puntos racionales de la curva

$$Y^q - Y = f(X).$$

Por otro lado, si $\omega_q = e^{\frac{2\pi i}{q}}$ tenemos que

$$\sum_{s\in\mathbb{F}_q} \omega_q^{s\mathrm{Tr}(f(x))} = \begin{cases} q, & \text{si } \mathrm{Tr}(f(x)) = 0, \\ 0, & \text{si } \mathrm{Tr}(f(x)) \neq 0. \end{cases}$$

Por lo que se tiene que

$$w(c) = n - \tfrac{1}{q}\Big(q^m - 1 + \sum_{s\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}^*} \omega_q^{\mathrm{Tr}(sf(x))}\Big),$$

donde $\displaystyle\sum_{x\in\mathbb{F}_{q^m}^*} \omega_q^{\mathrm{Tr}(sf(x))}$ es una suma exponencial.

En general, encontrar la cantidad de puntos racionales de estas curvas o calcular las sumas exponenciales no es fácil.

En este trabajo, encontramos el espectro de códigos de Hamming, BCH y de Melas a partir de estos dos caminos. En el siguiente cuadro, daremos para los códigos más conocidos la $f(x)$ correspondiente y clasificaremos las sumas asociadas.

Códigos cíclicos	Curvas Artin-Schreier	Sumas exponenciales
Hamming	$f(x) = \lambda x, \quad \lambda \in \mathbb{F}_q$	Sumas de Gauss (solo algunas se conocen)
BCH	$f(x) = \lambda x + \mu x^3, \quad \lambda, \mu \in \mathbb{F}_q$	En el caso binario, son Sumas de Weil (son conocidas)
Melas	$f(x) = \lambda x + \mu x^{-1}, \quad \lambda, \mu \in \mathbb{F}_q$	Sumas de Kloosterman (no son conocidas)

Notemos además que si conocemos el valor de una cierta suma exponencial o la cantidad de puntos de determinada curva, podríamos definir códigos cíclicos, usando ciertas $f(x)$ los cuáles tendrían un espectro conocido.

Vale la pena notar que si bien el valor de muchas de las sumas que asociamos a los códigos más conocidos no se sabe, existen sumas conocidas, como las sumas de Weil que nos permiten encontrar el espectro del código BCH binario.

Resumen

Este trabajo consta de 6 capítulos, divididos en tres partes claramente identificables, más un apéndice. La primer parte, formada por los Capítulos 1 y 2, está dedicada a preliminares matemáticos. La segunda parte está compuesta por el tercer y cuarto capítulos y se ocupa del estudio clásico del espectro de códigos lineales y cíclicos. La tercera parte, que es la parte central del trabajo, la conforman los Capítulos 5 y 6 y se ocupa de la distribución de códigos cíclicos especiales, como los códigos de Melas y Zetterberg, utilizando conceptos y métodos más sofisticados a partir de curvas elípticas y formas modulares.

• *Primera parte: Preliminares.* En esta primera parte veremos los conceptos y resultados mas importantes que utilizaremos en el resto del trabajo. En el primer capítulo vemos preliminares generales sobre: (a) cuerpos finitos y la función traza, (b) curvas elípticas (puntos racionales en ellas, j-invariante), (c) formas modulares y cuspidales y traza de los operadores de Hecke, (d) número de clase de Kronecker de formas cuadráticas y relación con número de clase de cuerpos cuadráticos y por último (e) sumas exponenciales de Gauss, de Weil, de Jacobi y de Kloosterman. Todos estos ingredientes serán utilizados a la hora de estudiar la distribución de pesos de códigos cíclicos.

En el segundo capítulo nos ocupamos de cuestiones específicas de códigos lineales. Allí definimos códigos lineales y sus duales, las matrices generadoreas y de paridad que los describen, y la distribución de pesos de dichos códigos. Damos dos resultados clásicos que, usados en conjunto, serán fundamentales para el trabajo: la identidad de MacWilliamns (§2.4) y el teorema de Delsarte (§2.7). La primera relaciona el polinomio enumerador de pesos de un código con el de su dual, el segundo relaciona códigos definidos en extensiones de un cuerpo y sus duales. En la Sección 2.5 introducimos los polinomios de Krawtchouk, una familia de polinomios ortogonales discretos muy ubicuos en combinatoria en general y en teoría de códigos en particular, con los cuales se tiene una versión alternativa de las identidades de MacWilliams. En la Sección 2.6 introducimos los códigos cíclicos (es decir aquellos códigos lineales que son invariantes por permutaciones cíclicas) y sus propiedades básicas. Como es usual, estos códigos se estudian mejor a través de polinomios usando el mapa de $(a_0, a_1, \ldots, a_{n-1}) \mapsto a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ de $\mathbb{F}_q^n$ en $\mathbb{F}_q[x]$ y viendo al código como un ideal en un anillo cociente de polinomios. Mas precisamente, si $\mathcal{C}$ es un código cíclico de longitud n sobre $\mathbb{F}_q$, a partir del mapa mencionado se puede ver al código como un ideal de $\mathbb{F}[x]/(x^n - 1)$. Finalmente, damos las familias de códigos lineales y cíclicas más conocidas como Hamming, BCH, Reed-Muller, etc.

• *Segunda parte: Espectro de códigos lineales y cíclicos.* En el Capítulo 3, nos dedicamos de la distribución de pesos de códigos lineales. Primero definimos el concepto de código de género a lo sumo g y damos un resultado general que da el espectro de un código lineal parcialemente, ya que una parte de los números A_i resultan conocidos, y el resto sólo se encuentra acotado inferior y superiormente (ver Teorema 3.3). En algunos casos, permite conocer el espectro de forma íntegra como en el caso de códigos MDS (ver §3.1.2) y los códigos de Hamming (§3.1.3). Lo que sucede con los códigos de Hamming es que su dual tiene sólo un peso no-nulo, de modo que el espectro de Hamming se obtiene por MacWilliams a partir de su dual. Esto podría usarse con códigos duales de códigos con pocos pesos como lo son los códigos de 2 o 3 pesos. En la Sección 3.2 presentamos una relación del espectro de un código cíclico irreducible con el número de soluciones ecuaciones diagonales sobre cuerpos finitos, que a su vez están en términos de sumas exponenciales como sumas de Gauss y periodos de Gauss. Éste es un resultado clásico de Wolfmann, que anticipa que las sumas exponenciales serán de gran utilidad en el estudio del cálculo del espectro de códigos cíclicos, lo que será abordado en el capítulo siguiente.

En el Capítulo 4, damos una estrategia general para intentar encontrar el espectro de códigos cíclicos, combinando los resultados del teorema de Delsarte y la identidad de MacWilliams. A su vez, esta estrategia, da la posibilidad de atacar el problema desde dos

ángulos muy interesantes y en algún sentido complementarios. Por un lado el espectro de un código cíclico es equivalente al cálculo explícito de ciertas sumas exponenciales y por otro lado al número de puntos racionales de ciertas curvas de Artin-Schreier. Dependiendo del código en particular, estas sumas exponenciales resultarán ser sumas de Gauss o similares, sumas de Weil, sumas de Kloosterman o similares. En el caso de las curvas, a veces resultan curvas que pueden ser transformadas en curvas elípticas, lo cual nos brinda una estructura adicional para su estudio. Aplicaremos estas técnicas a los códigos de Hamming cíclicos (todos los binarios y algunos q-arios) y a los códigos BCH (los cíclicos mas famosos y usados, que incluyen a los Reed-Solomon). Si bien ya conocemos el espectro de Hamming de capítulos previos, lo utilizamos para entender y familiarizarnos con los nuevos métodos (§4.1). En el caso de los códigos BCH obtenemos sumas de Weil, las cuales fueron calculados por Coulter en 3 trabajos en 1998-1999 y curvas elípticas supersingulares. En §4.2 realizamos el cálculo de la distribución de pesos de la familia de códigos BCH binarios 2-correctores ($d = 5$) de ambas formas, calculando primero el espectro del código dual (ver Tablas 4.3 y 4.4) y luego usando la identidad de MacWilliams para dar el espectro del BCH en términos de polinomios de Krawtchouk enteros en las fórmulas (4.5) y (4.6).

• *Tercera parte: Espectro de códigos de Melas y de Zetterberg.* En el Capítulo 5 está dedicado al espectro de los códigos de Melas. Éstos tienen polinomio generador $(m_\alpha(x)m_{\alpha^{-1}}(x))$ y tiene similitudes y diferencias con los BCH binarios definidos por $(m_\alpha(x)m_{\alpha^3}(x))$. Seguimos la estrategia que mencionamos en el capítulo anterior para encontrar la distribución de pesos de éstos códigos. En particular. Las sumas exponenciales que aparecen en este caso son sumas de Kloosterman, que no son conocidas en general. Sin embargo, obtendremos el espectro a partir de las curvas. Las curvas de Artin-Schreier asociadas son, via cambios de varibales, curvas elípticas no-supersingulares. En este caso, el cálculo de la distribución de pesos del código dual de Melas es mucho mas complicado que el del BCH (curvas elípticas supersingulares) y el estudio de estas curvas nos lleva a utilizar trazas de operadores de Hecke en formas modulares en $S(\Gamma_1(N))$ y números de clase de Kronecker. Estas son ideas de Schoof, van der Geer y van der Vlugt, plasmadas en numerosos artículos (ver por ejemplo [], [], []). Calculamos explícitamente el espectro en los casos binario y ternario (ver Teoremas). Cabe destacar que los casos $q \geq 5$ se encuentran abiertos, ya que para utilizar la misma técnica habría que tener mas información sobre la descomposición de los Jacobianos de las curvas que al momento no está disponible.

En el último capítulo nos ocupamos de los códigos de Zetterberg. Estos códigos están definidos usando el grupo de raíces $q+1$-ésimas de la unidad en $\mathbb{F}_{q^2}^*$. Si bien su definición es diferente a la de los códigos de Melas, al estudiar su espectro, descomponiendo el cuerpo en producto directo y usando un truco en la traza, se lo puede relacionar con el espectro del código de Melas. El resultado para Zetterberg binarios se da en el Teorema 6.2. En §6.2 exploramos una relación entre los códigos de Zetterberg arbitrarios y dos dos curvas de Artin-Schreier particulares. Esto nos permitirá en la sección siguiente obtener la distribución de pesos de los códigos de Zetterberg ternarios. El espectro de los códigos de Zetterberg q-arios se obtiene a partir del espectro de códigos de Melas q-arios.

Por último, en el apéndice, se encuentran calculados los espectros de varios códigos binarios particulares siguiendo alguno de los caminos utilizados previamente. Se pueden encontrar las distribuciones de pesos completas y sus correspondientes cuentas auxiliares de los códigos de Hamming $H_2(3)$ y $H_2(4)$, el BCH $B_2(3)$, los códigos de Melas $M_2(3)$ y $M_2(4)$ y el código de Zetterberg $Z_2(4)$.

Capítulo 1

Preliminares

En este capítulo introducimos todos los conceptos que serán necesarios para el resto del trabajo, salvo los códigos que serán tratados en el siguiente capítulo. En primer lugar, repasamos la definición de cuerpos finitos y la función traza de una extensión de cuerpos y mostramos sus principales propiedades. En segundo lugar, nos dedicamos a las curvas elípticas y sus puntos racionales. En la siguiente sección, nos ocupamos de las formas modulares y los operadores de Hecke asociados. En particular, enunciamos un importante teorema (Eichler-Selberg) que nos da la traza de estos operadores. También, definimos el número de clase de Kronecker y damos una tabla de valores. Por último, enumeramos las principales características de las sumas exponenciales de Gauss, Weil, Kloosterman y Jacobi.

La bibliografía consultada para este capítulo es la siguiente: para cuerpos finitos los libros de Lidl-Niederreiter y Wan ([27], [46]), para curvas elípticas el Silverman-Tate ([40]), para formas modulares el Diamond-Shurman ([12]) y para sumas exponenciales el libro de Berndt-Evans-Williams y los trabajos de Coulter ([3], [7], [8], [9]). El libro de Hiramatsu-Köhler ([17]) y el Handbook sobre cuerpos finitos de Mullen-Panario ([34]) son referencias para todos estos temas.

1.1 Cuerpos finitos y la función traza

En esta sección vemos algunos resultados sobre cuerpos finitos. Además, definimos la traza de una extensión y damos algunas de sus propiedades más importantes.

Cuerpos finitos

A un cuerpo que tiene un número finito de elementos lo llamaremos *cuerpo finito*. Para p primo, $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ es un cuerpo finito de p elementos. Si F es un cuerpo finito y p un número primo, denotamos por $\mathbb{F}_p$ a la imagen isomorfa de $\mathbb{Z}/p\mathbb{Z}$ en F.

Notemos que a partir de $\mathbb{F}_p$ se pueden construir cuerpos finitos más grandes adjuntando raíces de polinomios irreducibles. Sea $f(x) \in \mathbb{F}_p[x]$ irreducible de grado n (siempre

existen). Se tiene que $F = \mathbb{F}_p[x]/\langle f(x)\rangle$ es un cuerpo. Si α es raíz del polinomio $f(x)$ y $m_\alpha(x)$ es el polinomio minimal de α (mónico de menor grado que se anula en α), entonces,

$$\langle f(x)\rangle = \langle m_\alpha(x)\rangle \qquad \text{y} \qquad F = \mathbb{F}_p(\alpha) \simeq \frac{\mathbb{F}_p[x]}{\langle f(x)\rangle},$$

donde $\mathbb{F}_p(\alpha)$ es el menor cuerpo de característica p que contiene a α. Se tiene

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(F) = \mathrm{gr}(m_\alpha) = n.$$

El cuerpo F tiene grado n y se lo denota por $\mathbb{F}_{p^n}$.

Ejemplo 1.1. Consideramos $p = 2$ y el polinomio irreducible $x^2 + x + 1$. Luego, tenemos el cuerpo finito de cuatro elementos,

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \frac{\mathbb{F}_2[x]}{\langle x^2 + x + 1\rangle} = \{0, 1, \alpha, \alpha^2\},$$

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

Lema 1.2. *Si F es un cuerpo finito de q elementos, entonces $\alpha^q = \alpha$ para todo $\alpha \in F$. O sea, todo elemento de F es raíz de*

$$f(x) = x^q - x.$$

Demostración. Tenemos que $F^* = F \setminus \{0\}$ es un grupo de $q-1$ elementos, entonces todo $\alpha \in F^*$ cumple que $\alpha^{q-1} = 1$, es decir

$$\alpha^q = \alpha.$$

Luego, todo elemento de F^* es raíz de f. Además, el cero también cumple esta propiedad y vale el lema. □

Recordemos que el cuerpo de descomposición de un polinomio $f \in K[x]$ en una clausura algebraica fija, denotado $SF(f(x))_K$, es la menor extensión de cuerpos F/K tal que f se descompone completamente en factores lineales sobre $F[x]$, es decir

$$f(x) = a(x - \alpha_1)\cdots(x - \alpha_n), \qquad a, \alpha_1, \ldots, \alpha_n \in F.$$

Equivalentemente, $F = K(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de adjunción de todas las raíces de f, o sea F es el menor cuerpo que contiene a todas las raíces de f.

Teorema 1.3. *Para cada primo p y cada $n \in \mathbb{N}$, existe un cuerpo finito de p^n elementos. Tal cuerpo es único salvo isomorfismos. En particular, todo cuerpo finito de $q = p^n$ elementos es isomorfo al cuerpo de descomposición $\mathbb{F}_q = SF(x^q - x)_{\mathbb{F}_p}$.*

Demostración. Sean $\mathbb{F}_p$ el cuerpo de p elementos y consideremos el polinomio

$$f_q(x) = x^q - x$$

definido sobre este cuerpo. Sea R el conjunto de las q raíces de $f_q(x)$ en una cierta clausura algebraica de $\mathbb{F}_p$. Es claro que tales raíces son distintas pues el polinomio $f_q(x)$ no tiene raíces múltiples ya que su derivada es coprima con f_q:

$$f_q'(x) = qX^{q-1} - 1 = -1 \pmod{p}.$$

Entonces, R tiene cardinal q.

Ahora bien, R es un cuerpo. Sean $\alpha, \beta \in R$, es decir, $\alpha^q = \alpha$, $\beta^q = \beta$. Obviamente, tenemos

$$(\alpha\beta)^q = \alpha\beta \tag{1.1}$$

y (suponiendo $\beta \neq 0$) $(\frac{\alpha}{\beta})^q = \frac{\alpha}{\beta}$. Pero teniendo en cuenta que en $\mathbb{F}_p$ se tiene $q \equiv 0 \bmod p$, también vale

$$(\alpha \pm \beta)^q = \alpha \pm \beta \tag{1.2}$$

(pues todos los demás miembros del desarrollo de $(\alpha \pm \beta)^q$ son múltiplos de p). Luego la suma, diferencia, producto y cociente de elementos de R están en R.

Veamos ahora la unicidad. Sea K otro cuerpo con q elementos. Entonces, por el lema anterior, los q elementos de K son raíces de $x^q - x$ y, por lo tanto, K puede identificarse con R. □

La función traza

Sean q una potencia de un primo y n un número positivo. Vamos a definir una función muy importante asociada a extensiones de cuerpos $\mathbb{F}_{q^n}/\mathbb{F}_q$. El mapa σ de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ dado por

$$\sigma(\alpha) = \alpha^q,$$

es llamado el *automorfismo de Frobenius*. Notar que σ es un automorfismo de cuerpos por (1.1) y (1.2).

Definición 1.4. Sea α un elemento de $\mathbb{F}_{q^n}$. Definimos su *traza relativa* en $\mathbb{F}_q$ como:

$$\mathrm{Tr}_{q^n/q}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

Cuando la extensión esté sobreentendida escribiremos simplemente $\mathrm{Tr}(\alpha)$.

Resumimos las propiedades básicas de esta función.

Lema 1.5 (Propiedades de la traza)**.** *Sean α, $\beta \in \mathbb{F}_{q^n}$, $a \in \mathbb{F}_q$, entonces:*

(*a*) $\mathrm{Tr}(\alpha) \in \mathbb{F}_q$.

(*b*) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.

(*c*) $\mathrm{Tr}(a\alpha) = a\mathrm{Tr}(\alpha)$. *En particular,* $\mathrm{Tr}(a) = na$.

(*d*) $\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$.

Demostración. (a) La traza de α es una raíz de $x^q - x$, pues

$$\begin{aligned} \mathrm{Tr}(\alpha)^q &= \sigma(\mathrm{Tr}(\alpha)) = \sigma(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)) \\ &= \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha) + \alpha = \mathrm{Tr}(\alpha), \end{aligned}$$

y por lo tanto $\mathrm{Tr}(\alpha) \in \mathbb{F}_q$.

(b) Por definición la traza de $\alpha + \beta$ es

$$\mathrm{Tr}(\alpha + \beta) = (\alpha + \beta) + \sigma(\alpha + \beta) + \cdots + \sigma^{n-1}(\alpha + \beta) \ .$$

Notemos que σ^i es automorfismo en $\mathbb{F}_{q^n}$ para todo i. Entonces

$$\begin{aligned} \mathrm{Tr}(\alpha + \beta) &= \alpha + \beta + \sigma(\alpha) + \sigma(\beta) + \cdots + \sigma^{n-1}(\alpha) + \sigma^{n-1}(\beta) \\ &= \big(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)\big) + \big(\beta + \sigma(\beta) + \cdots + \sigma^{n-1}(\beta)\big) \\ &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta), \end{aligned}$$

como queríamos ver.

(c) Calculamos la traza de la multiplicación de α por un escalar $a \in \mathbb{F}_q$.

$$\begin{aligned} \mathrm{Tr}(a\alpha) &= a\alpha + \sigma(a\alpha) + \cdots + \sigma^{n-1}(a\alpha) = a\alpha + \sigma(a)\sigma(\alpha) + \cdots + \sigma^{n-1}(a)\sigma^{n-1}(\alpha) \\ &= a\alpha + a^q\alpha^q + \cdots + a^{q^{n-1}}\alpha^{q^{n-1}} = a\alpha + a\alpha^q + \cdots + a\alpha^{q^{n-1}} \\ &= a(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)) = a\mathrm{Tr}(\alpha). \end{aligned}$$

En particular, $\mathrm{Tr}(1) = n$, entonces $\mathrm{Tr}(a) = na$, y queda demostrado (c).

(d) Como $\sigma^n(\alpha) = \alpha^{q^n} = \alpha$ para todo $\alpha \in \mathbb{F}_{q^n}$, entonces tenemos que

$$\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\sigma(\alpha)) = \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha) + \alpha = \mathrm{Tr}(\alpha),$$

que es lo que queríamos ver. □

Teorema 1.6. *El mapa* $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *es sobreyectivo. Para* $\alpha \in \mathbb{F}_{q^n}$, $\mathrm{Tr}(\alpha) = 0$ *si y sólo si existe un elemento* $\beta \in \mathbb{F}_{q^n}$ *tal que* $\alpha = \beta^q - \beta$.

Demostración. Estudiemos primero el núcleo de la traza.

($\Leftarrow$) Sea $\alpha \in \mathbb{F}_{q^n}$ de la forma $\alpha = \beta^q - \beta$, para algún $\beta \in \mathbb{F}_{q^n}$. Luego, se cumple que

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta^q - \beta) = \mathrm{Tr}(\beta^q) - \mathrm{Tr}(\beta) = 0$$

por (b) y (d) en Lema 1.5, como queríamos ver.

($\Rightarrow$) Sea $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}(\alpha) = 0$. Consideremos el polinomio $x^q - x + \alpha \in \mathbb{F}_{q^n}[x]$. Sea $p(x)$ un factor irreducible de $x^q - x + \alpha$ sobre $\mathbb{F}_{q^n}$.

Denotamos la clase residual de $x \pmod{p(x)}$ por β. Luego, se tiene

$$\beta^q - \beta = \alpha.$$

Entonces:

$$\begin{aligned} 0 &= \mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \\ &= (\beta^q - \beta) + \cdots + (\beta^q - \beta)^{q^{n-1}} \\ &= \beta^q - \beta + \beta^{q^2} - \beta^q + \cdots + \beta^{q^n} - \beta^{q^{n-1}} \\ &= \beta^{q^n} - \beta, \end{aligned}$$

lo que prueba que $\beta \in \mathbb{F}_{q^n}$, por el Lema 1.2.

Para ver la sobreyectividad de la traza, es suficiente ver que hay un elemento $\gamma \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}(\gamma) \neq 0$, puesto que para cualquier $a \in \mathbb{F}_q$ tenemos que

$$a = a\mathrm{Tr}(\gamma)^{-1}\mathrm{Tr}(\gamma) = \mathrm{Tr}(a\mathrm{Tr}(\gamma)^{-1}\gamma).$$

Sea K el conjunto de elementos de $\mathbb{F}_{q^n}$ de traza cero. Luego,

$$K = \{\beta^q - \beta \,:\, \beta \in \mathbb{F}_{q^n}\}.$$

Claramente, $\beta^q - \beta = (\beta')^q - (\beta')$ para $\beta, \beta' \in \mathbb{F}_{q^n}$ si y sólo si

$$(\beta - \beta')^q = \beta^q - (\beta')^q = \beta - \beta'$$

o sea, si $\beta - \beta' \in \mathbb{F}_q$. Se sigue que $|K| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = q^{n-1}$. Entonces, hay elementos $\gamma \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}(\gamma) \neq 0$. □

1.2 Curvas elípticas

En esta sección primero recordamos algunas curvas algebraicas especiales como las curvas superelípticas (que incluyen a las elípticas e hiperelípticas) y las de Artin-Schreier; y damos fórmulas generales y estimaciones para el número de puntos racionales de dichas curvas. Esto será de gran utilidad al calcular espectros de códigos cíclicos generales. Luego, nos concentramos en las curvas elípticas (no-singulares y supersingulares) y sus propiedades básicas, que serán centrales en el cálculo de la distribución de pesos de los códigos BCH, Melas y Zetterberg.

1.2.1 Curvas superelípticas y de Artin-Schreier

Dada una curva algebraica E con ecuación

$$E: \quad f(X,Y) = 0, \qquad f \in \overline{\mathbb{F}}_p[X,Y],$$

los puntos $(x,y) \in \mathbb{F}_q^2$ que satisfacen la ecuación, es decir $f(x,y) = 0$, se dicen puntos $\mathbb{F}_q$-racionales de E. El conjunto de puntos $\mathbb{F}_q$-racionales de la curva E se denota por $E(\mathbb{F}_q)$. Se tiene la siguiente cota muy conocida.

Teorema 1.7 (Hasse-Weil). *Sea E una curva irreducible no singular de género g definida sobre $\mathbb{F}_q$. Entonces, el número de puntos $\mathbb{F}_q$-racionales en E es $q+1+t$, donde $|t| \leq 2g\sqrt{q}$. Es decir,*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{1.3}$$

Consideremos un polinomio $f \in \mathbb{F}_q[X]$ con q potencia de un primo p. Curvas de la forma

$$A_f : \qquad Y^q - Y = f(X) \tag{1.4}$$

reciben el nombre de *curvas de Artin-Schreier*. Por otra parte, si s es un divisor de $q-1$, la curva

$$E_{f,s} : \qquad Y^s = f(X) \tag{1.5}$$

se llama *curva superelíptica* definida sobre $\mathbb{F}_q$. Para $s = 2$, se dice que es una *curva hiperelíptica*. Si además $\mathrm{gr}(f) = 3$, tenemos una *curva elíptica*. Estudiaremos curvas elípticas más generales en la siguiente subsección.

Los resultados que siguen sobre el número de soluciones de las ecuaciones (1.4) y (1.5) se pueden encontrar con demostraciones en [41, Chap. 1] (también en §6.3.3 de [34], sin demostraciones).

El siguiente enunciado nos da el número de soluciones de las ecuaciones correspondientes a las curvas que definimos más arriba.

Proposición 1.8 (Stepanov, [41]). *Sea $f \in \mathbb{F}_q[X]$, $s \mid q-1$ y $r \in \mathbb{N}$.*

(*a*) *El número de soluciones $(x,y) \in \mathbb{F}_{q^r}^2$ de la ecuación de la curva superelíptica $E_{f,s}$ es*

$$\#(E_{f,s}(\mathbb{F}_{q^r})) = \sum_{ord(\chi) \mid s} \sum_{x \in \mathbb{F}_{q^r}} \chi(f(x)),$$

donde la suma exterior es sobre todos los caracteres multiplicativos χ de $\mathbb{F}_{q^r}$ tal que χ^s es trivial.

(*b*) *El número de soluciones $(x,y) \in \mathbb{F}_{q^r}^2$ de la ecuación de la curva de Artin-Schreier A_f está dada por*

$$\#(A_f(\mathbb{F}_{q^r})) = \sum_{\psi} \sum_{x \in \mathbb{F}_{q^r}} \psi(\mathrm{Tr}_{q^r/q}(f(x)),$$

donde la suma exterior es sobre todos los caracteres aditivos ψ de $\mathbb{F}_{q^r}$.

En las notaciones previas, tenemos las siguientes estimaciones para los números de soluciones de las curvas superelípticas y de Artin-Schreier que se conocen como cotas de Weil.

Teorema 1.9 (Stepanov, [41]). *Sea $f \in \mathbb{F}_q[X]$ de grado n y $s \mid q-1$.*

(a) *Si* $(n, s) = 1$ *y* f *tiene* $d > 0$ *ceros distintos en* $\overline{\mathbb{F}}_q$, *entonces el número de puntos* $\mathbb{F}_{q^r}$*-racionales de la curva superelíptica* $E_{f,s}$ *satisface*

$$|\#E_{f,s}(\mathbb{F}_{q^r}) - q^r| \leq (s-1)(d-1)\sqrt{q^r}.$$

(b) *Si* $(n, q) = 1$ *entonces el número de puntos* $\mathbb{F}_{q^r}$*-racionales de la curva Artin-Schreier* A_f *satisface*

$$|\#A_f(\mathbb{F}_{q^r}) - q^r| \leq (n-1)(q-1)\sqrt{q^r}.$$

1.2.2 Curvas elípticas

Aquí nos ocupamos en más detalle de las curvas elípticas. Mostramos que en dichas curvas se puede definir una suma tal que el conjunto de puntos de la curva resulta un grupo, y el conjunto de puntos racionales un subgrupo de éste. Por último, estimamos la cantidad de puntos en el subgrupo, lo que está estrictamente relacionado, como veremos más adelante, con la distribución de pesos de los códigos cíclicos.

Forma de Weierstrass y j-invariante

Una *curva elíptica* es una curva algebraica no singular de género 1. Tiene una ecuación de la forma

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.6}$$

Esta ecuación es llamada *ecuación de Weierstrass* para E.

Si los coeficientes pueden ser todos elegidos en un cuerpo K, entonces decimos que E está definida sobre el cuerpo K. Nosotros sólo consideramos cuerpos finitos $K = \mathbb{F}_q$. Si $\mathrm{char}(\mathbb{F}_q) \neq 2$, entonces el cambio de variables

$$(x, y) \mapsto \left(x, y - \tfrac{1}{2}a_1x - \tfrac{1}{2}a_3\right)$$

transforma a E en la curva

$$E': \qquad y^2 = x^3 + b_2x^2 + b_4x + b_6.$$

Si $\mathrm{char}(K) \neq 2, 3$, entonces el cambio de variables

$$(x, y) \mapsto \left(\tfrac{1}{36}(x - 3b_2), \tfrac{1}{216}y\right)$$

transforma a E' en la curva

$$E'': \qquad y^2 = x^3 + ax + b. \tag{1.7}$$

Vamos a introducir un invariante muy importante de una curva elíptica E dada por la ecuación de Weierstrass (1.6). Primero definimos las siguientes cantidades

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1a_2, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \end{aligned}$$

y a partir de éstas también

$$c_4 = d_2^2 - 24d_4,$$
$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6.$$

Δ es llamado el *discriminante* de E. Ahora, el *j-invariante* de E está dado por

$$j(E) = \frac{c_4^3}{\Delta}. \tag{1.8}$$

Luego, el j-invariante sólo depende de la clase de isomorfismo de la curva. La condición $\Delta \neq 0$ es equivalente a la no singularidad de E.

Característica par. En el caso en que el cuerpo K es de característica 2, tenemos algunas simplificaciones. Notar que si $K = \mathbb{F}_{2^m}$ para algún m, entonces se tiene

$$j(E) = \frac{a_1^{12}}{\Delta}.$$

- Si $j(E) \neq 0$, el cambio de variables

$$(x, y) \mapsto \left(a_1^2 x + \tfrac{a_3}{a_1}, a_1^3 y + \tfrac{a_1^2 a_4 + a_3^2}{a_1^3}\right) \tag{1.9}$$

tranforma a E en la curva

$$E_1 : \qquad y^2 + xy = x^3 + a_2 x^2 + a_6. \tag{1.10}$$

Para E_1, se tiene $\Delta = a_6$ y $j(E_1) = \frac{1}{a_6}$.

- Si $j(E) = 0$, entonces el cambio de variables

$$(x, y) \mapsto (x + a_2, y)$$

tranforma a E en la curva

$$E_2 : \qquad y^2 + a_3 y = x^3 + a_4 x + a_6. \tag{1.11}$$

Para E_2, se tiene $\Delta = a_3^4$ y $j(E_2) = 0$.

Notemos que las curvas E y E_1 (resp. E y E_2) son isomorfas y, por lo tanto, $j(E) = j(E_1)$ (resp. $j(E) = j(E_2)$).

Curvas elípticas supersingulares

Una curva elíptica E se dice *supersingular* si $p \mid t$, donde $\#E(\mathbb{F}_q) = q + 1 - t$. Si no, la llamamos *no supersingular*. Si $p = 2, 3$ vimos que E es no supersingular si y sólo si $j(E) \neq 0$.

La ley de grupo

Sea E una curva elíptica dada por la ecuación de Weierstrass, definida sobre el cuerpo K. Un punto en E es una solución de esta ecuación con coordenadas en alguna extensión L/K, o el punto único en E en el infinito en el plano proyectivo sobre K. El punto en el infinito lo denotaremos por $\mathcal{O}$.

Estos puntos en E forman un grupo abeliano $(E, +)$ con la suma $+$ que se define a continuación.

- El elemento neutro es el punto $\mathcal{O}$ en el infinito.
- Si $\mathcal{P} = (x_1, y_1) \neq 0$, entonces $-\mathcal{P} = (x_1, -y_1 - a_1x_1 - a_3)$.
- Si $\mathcal{P} \neq 0$, $\mathcal{Q} \neq 0$, $\mathcal{P} \neq -\mathcal{Q}$, entonces $\mathcal{P} + \mathcal{Q} = -\mathcal{R}$, donde $\mathcal{R}$ es el tercer punto de intersección de la recta $\overline{\mathcal{P}\mathcal{Q}}$ si $\mathcal{P} \neq \mathcal{Q}$, o de la recta tangente a la curva en $\mathcal{P}$, si $\mathcal{P} = \mathcal{Q}$, con la curva.

Sea E definida sobre K y sea L una extensión de K. El conjunto de puntos *L-racionales* de E, denotado por $E(L)$, es el conjunto de puntos de E cuyas coordenadas se encuentran en L, junto con el punto $\mathcal{O}$. Entonces, $E(L)$ es un subgrupo de $(E, +)$.

La fórmula explícita de las coordenadas de $\mathcal{P} + \mathcal{Q}$ en términos de las coordenadas de $\mathcal{P}$ y $\mathcal{Q}$ es fácil de encontrar. Sean

$$\mathcal{P} = (x_1, y_1), \quad \mathcal{Q} = (x_2, y_2) \quad \text{y} \quad \mathcal{P} + \mathcal{Q} = (x_3, y_3).$$

Sea ℓ la recta que pasa por $\mathcal{P}$ y $\mathcal{Q}$, si $\mathcal{P} \neq \mathcal{Q}$, o la recta tangente a la curva en $\mathcal{P}$ en el caso $\mathcal{P} = \mathcal{Q}$. La pendiente de ℓ es

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_2 + a_3}, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

Si $\beta = y_1 - \lambda x_1$, entonces la ecuación que define a ℓ es $y = \lambda x + \beta$. Luego, el tercer punto de intersección de ℓ con la curva tiene coordenadas

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad \text{y} \qquad y_3 = -(\lambda + a_1)x_3 - \beta - a_3.$$

Fórmula de adición en el caso char$(K) \neq 2, 3$

Sea E'' la curva dada en (1.7). Si $\mathcal{P} = (x_1, y_1) \in E''$, entonces $-\mathcal{P} = (x_1, -y_1)$. Si $\mathcal{Q} = (x_2, y_2) \in E''$, $\mathcal{Q} \neq -\mathcal{P}$, entonces $\mathcal{P} + \mathcal{Q} = (x_3, y_3)$, donde

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1,$$

y

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

Fórmula de adición en el caso char$(K) = 2$

En el caso de característica 2 tenemos lo siguiente. Sean E_1 y E_2 las curvas dadas en (1.10) y (1.11), respectivamente.

- Caso $j(E) \neq 0$. Sea $\mathcal{P} = (x_1, y_1) \in E_1$. Entonces,

$$-\mathcal{P} = (x_1, y_1 + x_1).$$

Si $\mathcal{Q} = (x_2, y_2) \in E_1$, $\mathcal{Q} \neq -\mathcal{P}$, entonces $\mathcal{P} + \mathcal{Q} = (x_3, y_3)$, donde

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ x_1^2 + \dfrac{a_6}{x_1^2}, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

$$y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ x_1^2 + \left(x_1 + \dfrac{y_1}{x_1}\right)x_3 + x_3, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

- Caso $j(E) = 0$. Sea $\mathcal{P} = (x_1, y_1) \in E_2$. Luego,

$$-\mathcal{P} = (x_1, y_1 + a_3)$$

y si $\mathcal{Q} = (x_2, y_2) \in E_2$, $\mathcal{Q} \neq -\mathcal{P}$, entonces $\mathcal{P} + \mathcal{Q} = (x_3, y_3)$, donde

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ \dfrac{x_1^4 + a_4^2}{a_3^2}, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

$$y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + a_3, & \text{si } \mathcal{P} \neq \mathcal{Q}, \\ \left(\dfrac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3, & \text{si } \mathcal{P} = \mathcal{Q}. \end{cases}$$

1.3 Formas modulares y operadores de Hecke

Aquí introducimos los subgrupos modulares y de congruencias, formas modulares y cuspidales y por último los operadores de Hecke asociados y el teorema de Eichler-Selberg que da la traza de dichos operadores en el subgrupo de Hecke.

1.3.1 $\mathrm{SL}_2(\mathbb{Z})$ y sus subgrupos de congruencia

El *grupo modular completo* es

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,:\, a, b, c, d \in \mathbb{Z},\, ad - bc = 1 \right\}.$$

Sea N un entero positivo, el *subgrupo de congruencia de nivel* N, denotado por $\Gamma(N)$, se define como

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,:\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Como $\Gamma(N)$ es el núcleo del mapa natural

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}),$$

entonces $\Gamma(N)$ es un subgrupo normal de índice finito en $\mathrm{SL}_2(\mathbb{Z})$.

El *subgrupo de Hecke de nivel* N se denota por $\Gamma_0(N)$ y está definido por

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,:\, N \mid c \right\}.$$

El grupo $\Gamma_1(N)$ consiste de todas las matrices $\gamma \in \Gamma$ que satisfacen

$$\gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}.$$

Definición 1.10. Un *subgrupo de congruencia* de Γ es un subgrupo que contiene a $\Gamma(N)$ para algún N.

Ejemplos de subgrupos de congruencias son $\Gamma_0(N)$ y $\Gamma_1(N)$ ya que

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma.$$

El semiplano superior

Sea $\mathfrak{h}$ el semiplano superior

$$\mathfrak{h} = \{z = x + iy \,:\, x, y \in \mathbb{R}, y > 0\} \subset \mathbb{C}.$$

Sea $\mathrm{GL}_2^+(\mathbb{R})$ el grupo de matrices 2×2 con entradas reales y determinante positivo. El grupo $\mathrm{GL}_2^+(\mathbb{R})$ actúa sobre $\mathfrak{h}$ como grupo de automorfismos holomorfos, por

$$\gamma : z \to \frac{az + b}{cz + d} \qquad \text{para } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R}).$$

Denotamos $\mathfrak{h}^*$ a la unión de $\mathfrak{h}, \mathbb{Q}$ y el símbolo ∞. La acción de Γ sobre $\mathfrak{h}$ puede ser extendida a $\mathfrak{h}^*$ definiendo:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c} \qquad (c \neq 0),$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \infty = \infty,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{r}{s} = \frac{ar + bs}{cr + ds} \qquad (\tfrac{r}{s} \in \mathbb{Q} \text{ con } (r, s) = 1).$$

Los números racionales junto con ∞ son llamados cúspides.

1.3.2 Formas modulares y formas cuspidales

Sea f una función holomorfa sobre $\mathfrak{h}$ y k un entero positivo. Para

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$$

y $z \in \mathbb{C}$ definimos

$$(f|_k\gamma)(z) = (\det \gamma)^{\frac{k}{2}} (cz + d)^{-k} f\Big(\frac{az + b}{cz + d}\Big).$$

Para k fijo, el mapeo

$$\gamma : f \to f|_k\gamma$$

define una acción de $\mathrm{GL}_2^+(\mathbb{R})$ sobre el espacio de funciones holomorfas sobre $\mathfrak{h}$.

Sea G un subgrupo de índice finito en Γ. Sea f una función holomorfa sobre $\mathfrak{h}$ tal que

$$f|_k\gamma = f \qquad \text{para todo } \gamma \in G.$$

Como G tiene índice finito en Γ,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^M = \begin{pmatrix} 1 & M \\ 0 & 1 \end{pmatrix} \in G$$

para algún entero positivo M. Por lo tanto,

$$f(z + M) = f(z)$$

para todo $z \in \mathfrak{h}$. Entonces, tiene una expansión de Fourier en el infinito, dada por

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q_M^n, \quad \text{con} \quad q_M = e^{\frac{2\pi i z}{M}}.$$

Decimos que f es holomorfa en el infinito, si $a_n = 0$ para todo $n < 0$, y decimos que se anula en el infinito si $a_n = 0$ para todo $n \leq 0$.

Sea $\sigma \in \Gamma$. Entonces $\sigma^{-1}G\sigma$ también tiene índice finito en Γ y $(f|_k\sigma)|_k\gamma = f|_k\sigma$ para toda $\gamma \in \sigma^{-1}G\sigma$. Entonces, para cualquier $\sigma \in \Gamma$, $f|_k\sigma$ también tiene una expansión de Fourier en el infinito. Decimos que f es holomorfa en las cúspides, si $f|_k\sigma$ es holomorfa en el infinito para todo $\sigma \in \Gamma$.

Definición 1.11. Sea N un entero positivo y χ un carácter de Dirichlet módulo N. Una *forma modular* para $\Gamma_0(N)$ de tipo (k, χ) es una función holomorfa f sobre $\mathfrak{h}$ tal que

(i) $f|_k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \chi(d)f$ para toda $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,

(ii) f es holomorfa en las cúspides.

(Notar que (i) implica que $f|_k\gamma = f$ para toda $\gamma \in \Gamma_1(N)$).

La expansión de Fourier de tal forma f es:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

El entero k es llamado el *peso* de f. Una forma modular de este tipo es llamada una *forma cuspidal* si se anula en las cúspides.

Las formas modulares sobre $\Gamma_0(N)$ de tipo (k, χ) forman el espacio lineal complejo $M_k(\Gamma_0(N), \chi)$, y este tiene como subespacio al conjunto $S_k(\Gamma_0(N), \chi)$ de todas las formas cuspidales. Este subespacio tiene un subespacio complementario canónico $\mathcal{E}_k$ generado por las llamadas series de Eisenstein. Luego tenemos

$$M_k(\Gamma_0(N), \chi) = \mathcal{E}_k(\Gamma_0(N), \chi) \oplus S_k(\Gamma_0(N), \chi).$$

1.3.3 Operadores de Hecke

Los resultados que siguen son clásicos, su exposición se basa en la dada en el trabajo de Schoof y van der Vlugt [39]. Sea p un número primo y

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \qquad (q = e^{2\pi i z}),$$

una forma modular sobre $\Gamma_0(N)$ de tipo (k, χ). Los operadores de Hecke T_p y U_p están definidos por

$$f|_k T_p(z) = \sum_{n=0}^{\infty} a_{np}\, q^n + \chi(p)\, p^{k-1} \sum_{n=0}^{\infty} a_n q^{np}, \qquad \text{si } p \nmid N,$$

$$f|_k U_p(z) = \sum_{n=0}^{\infty} a_{np}\, q^n, \qquad \text{si } p \mid N.$$

Es fácil ver que $f_{|_k}T_p$ y $f_{|_k}U_p$ también son formas modulares sobre $\Gamma_0(N)$ de tipo (k, χ), y son formas cuspidales si f es una forma cuspidal.

Se sabe que el espacio $S_k(\Gamma_1(N), 1)$ se descompone según los caracteres de Dirichlet módulo N, que son los caracteres de $\Gamma_0(N)/\Gamma_1(N)$, es decir

$$S_k(\Gamma_1(N)) = S_k(\Gamma_1(N), 1) = \bigoplus_{\chi} S_k(\Gamma_0(N), \chi). \tag{1.12}$$

Los operadores de Hecke de $S_k(\Gamma_1(N))$ respetan esta descomposición.

Se tiene la siguiente definición unificada de los operadores de Hecke T_m para todo $m \in \mathbb{N}$ definida por

$$f|_k T_m(z) = \sum_{n=1}^{\infty} b_n\, q^n, \qquad \text{con} \qquad b_n = \sum_{d\,|\,(m,n)} \chi(d)\, d^{k-1}\, a_{mn/d^2}, \tag{1.13}$$

donde ponemos $\chi(d) = 0$ si $(d, N) > 1$.

El siguiente resultado, debido a Cohen [5], da las trazas de los operadores de Hecke.

Teorema 1.12. *Sea $k \geq 2$ un entero tal que $\chi(-1) = (-1)^k$ y sea N_χ el conductor de χ, un carácter de Dirichlet módulo N. Para cada entero $n \geq 1$, la traza del operador de Hecke T_n actuando sobre el espacio de formas cuspidales $S_k(\Gamma_0(N), \chi)$ está dada por:*

$$\mathrm{Tr}(T_n) = A_1 + A_2 + A_3 + A_4$$

donde A_1,A_2,A_3 y A_4 están definidos como sigue:

$$A_1 = \tfrac{1}{12} n^{\frac{k}{2}-1}\, \chi(\sqrt{n})\, (k-1)\, \psi(N),$$

donde $\chi(\sqrt{n}) = 0$ cuando $\sqrt{n} \notin \mathbb{Z}$ y

$$\psi(N) = N \prod_{p|N} \Big(1 + \tfrac{1}{p}\Big).$$

El número A_2 es

$$A_2 = -\tfrac{1}{2} \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4n}} \tfrac{\rho^{k-1} - \rho^{-k-1}}{1-\overline{\rho}} \sum_{f \in D} h_w\big(\tfrac{t^2-4n}{f^2}\big)\, \mu(t, f, n),$$

donde $D = \{f \mid t^2 - 4n : f > 0 \;\; y \;\; \frac{t^2-4n}{f^2} \equiv 0, 1 \pmod 4\}$, ρ y $\overline{\rho}$ denotan las raíces del polinomio $x^2 - tx + n$, y

$$h_w(-3) = \tfrac{1}{3}, \qquad h_w(-4) = \tfrac{1}{2}, \qquad h_w(\Delta) = h(\Delta) \quad \textit{para } \Delta < -4$$

donde $h(\Delta)$ es el número de clase de Δ (ver próxima sección). Además,

$$\mu(t, f, n) = \frac{\psi(N)}{\psi(\frac{N}{(N,f)})} \sum_{\substack{x \pmod N \\ x^2 - tx + n \equiv 0 \pmod N}} \chi(x).$$

Por otra parte,

$$A_3 = -\sum_{\substack{d|N \\ 0 < d \leq \sqrt{n}}}{}' d^{k-1} \sum_{\substack{c|N \\ (c, N/c)\,|\,(N/N_\chi, \frac{n}{d} - d)}} \varphi\big((c, \tfrac{N}{c})\big)\, \chi(z)$$

donde φ denota la función de Euler, la $'$ en la primer sumatoria indica que la contribución del término $d = \sqrt{n}$, si ocurre, debe ser multiplicada por $\frac{1}{2}$, y el número z está definido módulo $N/(c, \frac{N}{c})$ por

$$z \equiv d \pmod{c} \qquad y \qquad z \equiv \tfrac{n}{d} \pmod{\tfrac{N}{d}}.$$

Por último tenemos

$$A_4 = \sum_{\substack{0<t|n \\ (N,n/t)=1}} t$$

si $k = 2$ y $\chi = id$ y $A_4 = 0$ en caso contrario.

1.4 Número de clase de Kronecker

Aquí recordamos la definición del número de clase de formas cuadráticas de Kronecker y lo relacionamos con el número de clase de extensiones cuadráticas. Los resultados de esta sección se pueden ver en el trabajo de Schoof y van der Vlugt [39].

Si Δ es un entero positivo congruente a 0 o a 1 módulo 4. se definen los conjuntos

$$B(\Delta) = \{ax^2 + bxy + cy^2 \,:\, a, b, c \in \mathbb{Z}, a > 0, b^2 - 4ac = \Delta\},$$
$$b(\Delta) = \{ax^2 + bxy + cy^2 \in B(\Delta) \,:\, \mathrm{mcd}(a, b, c) = 1\}.$$

Los elementos de $B(\Delta)$ son llamados *formas cuadráticas binarias definidas positivas con discriminante* Δ. Las que pertenecen a $b(\Delta)$ se dicen *primitivas*.

El grupo $\mathrm{SL}_2(\mathbb{Z})$ actúa sobre $B(\Delta)$ por

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot f(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$$

para $f(x, y) \in B(\Delta)$. El subconjunto $b(\Delta)$ se preserva bajo esta acción. Luego, el número de órbitas de $b(\Delta)$ es llamado el *número de clase de* Δ y se denota $h(\Delta)$.

El *número de clase de Kronecker de* Δ se denota por $H(\Delta)$ y está definido como el número de órbitas en $B(\Delta)$, pero uno debería contar las formas ax^2+ay^2 y $ax^2+axy+ay^2$, si hubiera en $B(\Delta)$, con multiplicidad $\frac{1}{2}$ y $\frac{1}{3}$, respectivamente.

La relación entre el número de clase de Kronecker $H(\Delta)$ y el número de clase $h_w(\Delta)$ del cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{\Delta})$ está dada por (ver Proposition 2.1 en [39])

$$H(\Delta) = \sum_{\substack{f|\Delta,\, f>0 \\ \frac{\Delta}{f^2} \equiv 0,1 \pmod 4}} h_w(\tfrac{\Delta}{f^2}), \tag{1.14}$$

donde h_w está definido por:

$$h_w(-3) = \tfrac{1}{3}, \qquad h_w(-4) = \tfrac{1}{2} \qquad \text{y} \qquad h_w(\Delta) = h(\Delta) \quad \text{si } \Delta < -4.$$

Para d pequeño, obtenemos las siguientes tablas de valores:

$-d$	$H(d)$
3	1
4	1
7	1
8	1
11	1
12	2
15	2
16	2

$-d$	$H(d)$
19	1
20	2
23	3
14	2
27	2
28	2
31	3
32	3

$-d$	$H(d)$
35	2
36	3
39	4
40	2
43	1
44	4
47	5
48	4

$-d$	$H(d)$
51	2
52	2
55	4
56	4
59	3
60	4
63	5
64	4

1.5 Sumas exponenciales

En esta sección definimos las sumas de Gauss, de Jacobi, de Kloosterman y de Weil, y damos varias de sus propiedades más conocidas.

Recordemos que un *carácter multiplicativo* χ en $\mathbb{F}_q^*$ es un mapa desde el grupo cíclico $\mathbb{F}_q^*$ en el grupo de las raíces de la unidad complejas, tal que

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

para todo $\alpha, \beta \in \mathbb{F}_q^*$. Extendemos χ a una función en $\mathbb{F}_q$ definiendo $\chi(0) = 0$. El *carácter trivial* χ_0 satisface $\chi_0(\alpha) = 1$ para cada $\alpha \in \mathbb{F}_q^*$.

Algunos de los resultados pueden cambiar según como se defina el cáracter trivial en cero. A veces se define $\chi_0(0) = 1$ y otras veces, $\chi_0(0) = 0$, como en este caso.

1.5.1 Sumas de Gauss

De aquí en adelante, si p es un primo, denotaremos por

$$\omega_p = e^{\frac{2\pi i}{p}}$$

a la raíz primitiva p-ésima de la unidad en $\mathbb{C}$. Para un carácter χ de orden k en $\mathbb{F}_q$ y para $\beta \in \mathbb{F}_q$, la *suma de Gauss* $G(\beta, \chi)$ de orden k sobre $\mathbb{F}_q$ se define por

$$G(\beta, \chi) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\, \omega_p^{\mathrm{Tr}(\alpha\beta)}.$$

Cuando $\beta = 1$ ó $\chi = \chi_0$ escribiremos simplemente $G(\chi) = G(1, \chi)$ ó $G(\beta) = G(\beta, \chi_0)$, respectivamente.

Teorema 1.13. *Sea χ un carácter sobre $\mathbb{F}_q$ y $\beta \in \mathbb{F}_q$. Entonces vale*

$$G(\beta, \chi) = \begin{cases} q - 1, & \text{si } \beta = 0, \chi = \chi_0, \\ \overline{\chi}(\beta)\, G(\chi), & \text{caso contrario.} \end{cases}$$

En particular, $G(\overline{\chi}) = \chi(-1)\overline{G(\chi)}$. *Además se tiene que*

(*a*) $|G(\chi)| = \sqrt{q}$ *si* $\chi \neq \chi_0$ *y* $G(\chi_0) = 0$.

(*b*) $G(\beta, \chi^p) = G(\beta^p, \chi)$ *donde* p *es la característica de* $\mathbb{F}_q$.

Definición 1.14. Sea $\beta \in \mathbb{F}_q^*$ y supongamos que $q = kf + 1$ para algún entero positivo k. Los *períodos gaussianos f-nomiales* (reducidos) $g(\beta, k)$ se definen por

$$g(\beta, k) = \sum_{\alpha \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(\beta\alpha^k)}. \tag{1.15}$$

Cuando $\beta = 1$, denotamos $g(k) = g(1, k)$. Los períodos $g(\beta, k)$ son también llamados sumas de Gauss.

Existe una estrecha relación entre sumas y períodos de Gauss.

Teorema 1.15. *Sea* $\beta \in \mathbb{F}_q^*$. *Si* χ *es un carácter sobre* $\mathbb{F}_q$ *de orden* k, *entonces*

$$g(\beta, k) = \sum_{j=1}^{k-1} G(\beta, \chi^j).$$

En particular, $|g(\beta, k)| \leq (k-1)\sqrt{q}$.

1.5.2 Sumas de Jacobi

Sean χ, ψ caracteres multiplicativos en $\mathbb{F}_q$. La *suma de Jacobi* $J(\chi, \psi)$ sobre $\mathbb{F}_q$ se define por

$$J(\chi, \psi) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\psi(1-\alpha).$$

Decimos que la suma de Jacobi tiene orden k si k es el mínimo común múltiplo de los órdenes de sus argumentos.

Teorema 1.16. *Sean* χ, ψ *caracteres en* $\mathbb{F}_q$. *Entonces se tiene*

(*a*)

$$J(\chi, \psi) = \begin{cases} q-2, & \text{si } \chi, \psi \text{ son triviales,} \\ -1, & \text{si exactamente uno de los dos es trivial,} \\ -\chi(-1), & \text{si } \chi\psi \text{ es trivial con } \chi \text{ no trivial.} \end{cases}$$

(*b*) *Si* $\chi\psi$ *es no trivial, entonces*

$$J(\chi, \psi) = \frac{G(\chi)G(\psi)}{G(\chi\psi)}.$$

(c) *Si χ es no trivial, entonces*

$$J(\chi,\psi)=\frac{\psi(-1)G(\psi)G(\overline{\chi\psi})}{G(\overline{\chi})}.$$

(d) *Si χ es de orden $k>1$, entonces*

$$G(\chi)^k=q\chi(-1)\prod_{j=1}^{k-2}J(\chi,\chi^j).$$

Definición 1.17. Sean $\chi_1,\ldots,\chi_t$ caracteres sobre $\mathbb{F}_q$. Se define la *suma múltiple de Jacobi* como

$$J(\chi_1,\ldots,\chi_t)=\sum_{\substack{\alpha_1,\ldots,\alpha_t\in\mathbb{F}_q\\ \alpha_1+\cdots+\alpha_t=1}}\chi_1(\alpha_1)\cdots\chi_t(\alpha_t).$$

Similarmente definimos:

$$J_0(\chi_1,\ldots,\chi_t)=\sum_{\substack{\alpha_1,\ldots,\alpha_t\in\mathbb{F}_q\\ \alpha_1+\cdots+\alpha_t=0}}\chi_1(\alpha_1)\ldots\chi_t(\alpha_t).$$

1.5.3 Sumas de Kloosterman

Para $u,v\in\mathbb{F}_q$ y un carácter multiplicativo χ sobre $\mathbb{F}_q$, se define la *suma de Kloosterman* $\kappa(v,u,\chi)$ sobre $\mathbb{F}_q$, como

$$\kappa(v,u,\chi)=\sum_{\alpha\in\mathbb{F}_q^*}\chi(\alpha)\,\omega_p^{\mathrm{Tr}(v\alpha+\frac{u}{\alpha})}. \tag{1.16}$$

Notar que $\kappa(0,0;\chi)=G(\chi)$. Cuando $\chi=\chi_0$ es trivial, denotamos $\kappa(v,u)=\kappa(v,u,\chi_0)$ y cuando $v=1$, $\kappa(u,\chi)=\kappa(1,u,\chi)$. Así, ponemos $\kappa(u)=\kappa(1,u,\chi_0)$.

Para q impar y χ trivial, estas sumas se pueden poner en términos sólo del carácter cuadrático.

Proposición 1.18. *Para q impar y $u\in\mathbb{F}_q$,*

$$\kappa(u)=\sum_{y\in\mathbb{F}_q}\rho(y^2-4u)\,\omega_p^{\mathrm{Tr}(y)},$$

donde ρ es el carácter cuadrático sobre $\mathbb{F}_q$.

En el caso general, Conrad ([6]) probó la siguiente.

Teorema 1.19. *Sea u en $\mathbb{F}_q$ y ρ el carácter cuadráctico en $\mathbb{F}_q$. Entonces, para cualquier carácter χ de $\mathbb{F}_q$ se tiene*

$$\kappa(u,\chi)=\frac{G(\rho)\bar{\chi}(4)}{G(\chi\rho)}\sum_{y\in\mathbb{F}_q}(\chi\rho)(y^2-4u)\,\omega_p^{\mathrm{Tr}(y)}.$$

Estas sumas pueden ser generalizadas de la siguiente manera. Para $u \in \mathbb{F}_q$ y caracteres $\chi_1, \ldots, \chi_m$ sobre $\mathbb{F}_q$, se define la *suma de Kloosterman múltiple* sobre $\mathbb{F}_q$ como

$$\kappa(u, \chi_1, \ldots, \chi_m) = \sum_{\substack{\alpha_0, \ldots, \alpha_m \in \mathbb{F}_q \\ \alpha_0 \cdots \alpha_m = u}} \chi_1(\alpha_1) \cdots \chi_m(\alpha_m)\, \omega_p^{\mathrm{Tr}(\alpha_0 + \cdots + \alpha_m)}.$$

Es también llamada una *hipersuma de Kloosterman*.

Katz ([21]) dió la siguiente expresión para las hipersumas de Kloosterman en términos de sumas de Gauss.

Teorema 1.20. *Para $u \in \mathbb{F}_q^*$ y caracteres $\chi_1, \ldots, \chi_m$ en $\mathbb{F}_q$ se tiene*

$$\kappa(u, \chi_1, \ldots, \chi_m) = \tfrac{1}{q-1} \sum_{\chi} \bar{\chi}(u) \prod_{i=0}^{m} G(\chi\chi_i)$$

donde χ_0 es el carácter trivial y y la suma es sobre todos los caracteres χ de $\mathbb{F}_q$.

1.5.4 Sumas de Weil

Todos los resultados de esta subsección y sus respectivas demostraciones se pueden encontrar en los tres trabajos de Coulter de 1998-1999 ([7], [8] y [9]).

Sean p un número primo y $q = p^m$ para algún entero m. Una *suma de Weil* es una suma exponencial de la forma

$$W(\chi, f) = \sum_{x \in \mathbb{F}_q} \chi(f(x)), \tag{1.17}$$

donde χ es un carácter aditivo no trivial de $\mathbb{F}_q$ y $f \in \mathbb{F}_q[x]$.

Estas sumas son muy generales y sólo se conocen para ciertos f. Nosotros estamos interesados en el caso particular en que f es de la forma

$$f_\alpha^{a,b}(x) = ax^{p^\alpha + 1} + bx, \tag{1.18}$$

donde $a, b \in \mathbb{F}_q$ y α es un número natural.

El carácter aditivo canónico de $\mathbb{F}_q$, denotado por χ_1, está dado por

$$\chi_1(x) = e^{\frac{2\pi i \mathrm{Tr}(x)}{p}} = \omega_p^{\mathrm{Tr}(x)}, \tag{1.19}$$

para todo $x \in \mathbb{F}_q$. Notemos que $\chi_1(x^p) = \chi_1(x)$ y $\chi_1(-x) = \overline{\chi_1(x)}$ para todo $x \in \mathbb{F}_q$. Además, cualquier carácter aditivo χ_a sobre $\mathbb{F}_q$ puede ser obtenido a partir de χ_1 por

$$\chi_a(x) = \chi_1(ax),$$

para todo $x \in \mathbb{F}_q$. Luego, solo hace falta encontrar el valor de las sumas de Weil en el caso $\chi = \chi_1$.

Denotamos por $S_\alpha(a,b)$ a la suma de Weil $W(\chi_1, f_\alpha^{a,b})$, es decir,

$$S_\alpha(a,b) = \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx) \tag{1.20}$$

donde $a, b \in \mathbb{F}_q$ y $\alpha \in \mathbb{N}$. El caso $(a,b) = (0,0)$ es trivial, ya que

$$S_\alpha(0,0) = \sum_{x\in\mathbb{F}_q} \chi_1(0) = q.$$

Notar que si $a = 0$ y $b \neq 0$ o bien $a \neq 0$ y $b = 0$ se obtienen sumas de Gauss o períodos de Gauss, respectivamente. En efecto,

$$\begin{aligned} S_\alpha(0,b) &= \sum_{x\in\mathbb{F}_q} \chi_1(bx) = \sum_{x\in\mathbb{F}_q} \omega_p^{\mathrm{Tr}(bx)} = G(b,\chi_0), \\ S_\alpha(a,0) &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) = \sum_{x\in\mathbb{F}_q} \omega_p^{\mathrm{Tr}(ax^{p^\alpha+1})} = g(a,p^\alpha+1). \end{aligned} \tag{1.21}$$

Además, por Teorema 1.13,

$$S_\alpha(0,b) = \bar{\chi}_0(b)G(\chi_0) = 0.$$

Coulter estudió en detalle las sumas en (1.20) con $a \neq 0$, en característica par e impar. Sólo daremos los valores explícitos en el caso $p = 2$, que es el que necesitaremos más adelante al estudiar el espectro de los códigos BCH binarios.

Característica 2

Consideramos ahora $p = 2$ y $q = 2^m$ para algún m. Sea $d = (\alpha, m)$. Queremos calcular las sumas

$$S_\alpha(a,b) = \sum_{x\in\mathbb{F}_{2^m}} \chi_1(ax^{2^\alpha+1} + bx). \tag{1.22}$$

Tenemos ahora dos casos, dependiendo si $\frac{m}{d}$ es par o impar. Los resultados que siguen fueron obtenidos en [9]. Los resultados para el caso p impar son muy similares en el caso $\frac{m}{d}$ par, muy distintos para $\frac{m}{d}$ impar, y pueden encontrarse en los trabajos [7] y [8].

Caso $\frac{m}{d}$ impar

Damos primero los valores para $S_\alpha(a,0)$.

Teorema 1.21. *Sea χ un carácter aditivo no trivial de $\mathbb{F}_q$. Si $\frac{m}{d}$ es impar entonces*

$$S_\alpha(a,0) = \sum_{x\in\mathbb{F}_q} \chi_1(ax^{2^\alpha+1}) = \begin{cases} q, & \text{si } a = 0, \\ 0, & \text{caso contrario.} \end{cases}$$

Veamos ahora el valor de $S_\alpha(a,b)$ para $b \neq 0$. Sea t un entero que divide a m. Denotamos por Tr_t a la función traza de $\mathbb{F}_q = \mathbb{F}_{p^m}$ en $\mathbb{F}_{p^t}$, es decir,

$$\mathrm{Tr}_t(x) = x + x^{p^t} + \cdots + x^{p^{t(\frac{m}{t}-1)}},$$

para todo $x \in \mathbb{F}_q$. A Tr_1 la denotamos simplemente por Tr.

Teorema 1.22. *Sea $b \in \mathbb{F}_q^*$ y supongamos $\frac{m}{d}$ es impar. Entonces*

$$S_\alpha(a,b) = S_\alpha(1, bc^{-1}),$$

donde $c \in \mathbb{F}_q^*$ es el único elemento que satisface $c^{2^\alpha+1} = a$. Además, $S_\alpha(1,b) = 0$ si $\mathrm{Tr}_d(b) \neq 1$ y $S_\alpha(1,b) = \pm 2^{\frac{m+d}{2}}$ si $\mathrm{Tr}_d(b) = 1$.

En el Teorema 1.22 falta determinar el signo de $S_\alpha(1,b)$ cuando $\mathrm{Tr}_d(b) = 1$. El siguiente lema reduce esto a encontrar el signo de $S_\alpha(1,1)$.

Lema 1.23. *Sea $b \in \mathbb{F}_q^*$ tal que $\mathrm{Tr}_d(b) = 1$ y supongamos $\frac{e}{d}$ es impar. Entonces*

$$S_\alpha(1,b) = \chi_1(c^{2^\alpha+1} + c)\, S_\alpha(1,1),$$

donde $b = c^{2^{2^\alpha}} + c + 1$ para algún $c \in \mathbb{F}_q$.

Finalmente damos el valor de $S_\alpha(1,1)$ con el signo dado en términos del símbolo de Jacobi.

Teorema 1.24. *Sea $\frac{m}{d}$ impar, entonces*

$$S_\alpha(1,1) = (\tfrac{2}{m/d})^d\, 2^{\frac{m+d}{2}},$$

donde $(\frac{2}{m/d})$ es el símbolo de Jacobi.

Esto completa la determinación de las sumas de Weil $S_\alpha(a,b)$ en el caso $\frac{m}{d}$ impar.

Caso $\frac{m}{d}$ par

Nuevamente, primero se calcula el valor para las sumas con $b = 0$. Denotamos por β a un elemento primitivo de $\mathbb{F}_q$.

Teorema 1.25. *Sea $\frac{m}{d}$ par y $m = 2r$ para algún entero r. Entonces,*

$$S_\alpha(a,0) = \begin{cases} (-1)^{\frac{r}{d}}\, 2^r, & \text{si } a \neq \beta^{t(2^d+1)} \text{ para cualquier entero } t, \\ -(-1)^{\frac{r}{d}}\, 2^{r+d}, & \text{si } a = \beta^{t(2^d+1)} \text{ para algún entero } t. \end{cases}$$

Para dar el valor de las sumas $S_\alpha(a,b)$ en el caso de b general necesitaremos recordar que un polinomio $f \in \mathbb{F}_q[x]$ se dice un *polinomio de permutación* si induce una permutación sobre $\mathbb{F}_q$.

Teorema 1.26. *Sea $b \in \mathbb{F}_q^*$ y supongamos $\frac{m}{d}$ es par, luego $m = 2r$ para algún entero r. Sea $f(x) = a^{2^\alpha} x^{2^{2\alpha}} + ax$. Hay dos casos.*

(a) *Si $a \neq \beta^{t(2^d+1)}$ para algún entero t entonces f es un polinomio de permutación. Sea $x_0 \in \mathbb{F}_q$ el único elemento que satisface $f(x_0) = b^{2^\alpha}$. Entonces*

$$S_\alpha(a,b) = (-1)^{\frac{r}{d}}\, 2^r\, \chi_1(a x_0^{2^\alpha+1}).$$

(b) *Si $a = \beta^{t(2^d+1)}$ entonces $S_\alpha(a,b) = 0$ a menos que la ecuación $f(x) = b^{2^\alpha}$ tenga solución. Si la ecuación tiene solución, digamos x_0, entonces*

$$S_\alpha(a,b) = \begin{cases} (-1)^{\frac{r}{d}+1}\, 2^{r+d}\, \chi_1(a x_0^{2^\alpha+1}), & si\ \mathrm{Tr}_d(a) = 0, \\ (-1)^{\frac{r}{d}}\, 2^r\, \chi_1(a x_0^{2^\alpha+1}), & si\ \mathrm{Tr}_d(a) \neq 0. \end{cases}$$

Capítulo 2

Códigos autocorrectores

En este capítulo daremos definiciones básicas de la teoría de códigos y sus propiedades más importantes. Luego, introduciremos los códigos cíclicos y enunciaremos dos teoremas que utilizaremos más adelante, la Identidad de MacWilliams y el Teorema de Delsarte. Por último, veremos algunos ejemplos de los códigos más conocidos.

2.1 Generalidades

Un *alfabeto* es un conjunto finito $A = \{a_1, \ldots, a_q\}$. A los elementos de A se los llama *símbolos*. Una *n-cadena* o palabra de longitud n sobre A es una sucesión de n elementos de A. Denotamos por A^n el conjunto de todas las n-cadenas y por A^* el conjunto de todas las palabras sobre A.

Definición 2.1. Si $A = \{a_1, \ldots, a_q\}$ es un alfabeto, un *código q-ario* sobre A es un subconjunto $\mathcal{C}$ de A^*. Los elementos de $\mathcal{C}$ se llaman *palabras código*. El número $M = |\mathcal{C}|$ se llama el *tamaño* del código.

Si todas las palabras código tienen longitud fija n, decimos que $\mathcal{C}$ es un código de *bloque* con parámetros (n, M) o que $\mathcal{C}$ es un (n, M)-código. Si $\mathcal{C}$ no es de bloque, decimos que $\mathcal{C}$ es de longitud variable.

Ejemplo 2.2. $\mathcal{C} = \{0, 10, 101, 1110, 11111\}$ es un código de longitud variable. El ejemplo más famoso de este tipo de códigos es el código Morse.

De ahora en más, siempre $\mathcal{C}$ será un código de bloque.

Definición 2.3. Sean x e y dos palabras sobre el mismo alfabeto A. La *distancia de Hamming* entre x e y, denotada por $d(x, y)$, se define como el número de coordenadas en que x e y difieren, es decir, $d : A^n \times A^n \to [0, n] \subset \mathbb{N}$, donde

$$d(x, y) = \#\{1 \leq i \leq n \, : \, x_i \neq y_i\}.$$

Definición 2.4. Dado un código $\mathcal{C}$ se define la *distancia mínima* de $\mathcal{C}$, y se la denota $d(\mathcal{C})$ ó $d_{\mathcal{C}}$, como la menor distancia no nula entre sus palabras código, es decir,

$$d = d_{\mathcal{C}} = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} d(x, y).$$

Ahora decimos que $\mathcal{C}$ es un (n, M, d)-código.

Definición 2.5. Dado $x \in \mathbb{F}_q^n$ se define el *peso* de x, denotado por $w(x)$, como el número de coordenadas no nulas de x, es decir,

$$w(x) = \#\{1 \leq i \leq n \,:\, x_i \neq 0\}.$$

Si $\mathcal{C}$ es un código, el peso de $\mathcal{C}$ se define por

$$w_{\mathcal{C}} = \min_{\substack{x \in \mathcal{C} \\ x \neq 0}} w(x).$$

2.2 Códigos lineales

Definición 2.6. Un *código lineal* q-ario de longitud n y rango 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. Si $\mathcal{C}$ tiene distancia mínima d entonces $\mathcal{C}$ es un $[n, k, d]_q$-código.

Notemos que el tamaño de un $[n, k]_q$-código es $M = q^k$.

Ejemplo 2.7. El código de repetición q-ario

$$Rep(n) = \{\underbrace{0 \cdots 0}_{n}, \underbrace{1 \cdots 1}_{n}, \ldots, \underbrace{(q-1) \cdots (q-1)}_{n}\}$$

es un $[n, 1, n]_q$-código lineal.

Proposición 2.8. *Si $\mathcal{C}$ es un código lineal entonces $d(\mathcal{C}) = w(\mathcal{C})$.*

Demostración. Como $\mathcal{C}$ es lineal, tenemos que

$$d(\mathcal{C}) = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} d(x, y) = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} w(x - y) = \min_{\substack{x \in \mathcal{C} \\ x \neq 0}} w(x) = w(\mathcal{C}),$$

ya que $x - y$ recorre todas las palabras código de C cuando x e y recorren todo $\mathcal{C}$. □

Definición 2.9. Sea $\mathcal{C}$ un $[n, k]_q$-código. Una *matriz generadora* de $\mathcal{C}$ es una matriz $G \in \mathbb{F}_q^{k \times n}$ cuyas filas forman una base de $\mathcal{C}$.

Observemos que G siempre existe y tiene rango k. Además, G genera $\mathcal{C}$, es decir,

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

Esto nos dice que dado un código $\mathcal{C}$, encontrando una base, podemos obtener una matriz generadora; y dada una matriz G, tenemos un código $\mathcal{C} = \mathbb{F}_q^k G$.

2.3 Código dual

Definición 2.10. Si $\mathcal{C}$ es un $[n,k]_q$-código, el conjunto

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \,:\, x \cdot c = 0 \quad \text{para todo } c \in \mathcal{C}\}$$

es el *código dual* de $\mathcal{C}$, donde $\cdot$ es el producto interno usual de $\mathbb{F}_q^n$. Una matriz H se dice *matriz de paridad* de $\mathcal{C}$ si es una matriz generadora de $\mathcal{C}^\perp$.

A continuación damos los parámetros y propiedades básicas del código dual $\mathcal{C}^\perp$ de un código lineal $\mathcal{C}$ dado.

Teorema 2.11. *Sea $\mathcal{C}$ un $[n,k]_q$-código.*

(*a*) *Si G es una matriz generadora de $\mathcal{C}$, entonces*

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \,:\, xG^T = 0\} = \{x \in \mathbb{F}_q^n \,:\, Gx^T = 0\}.$$

(*b*) *$\mathcal{C}^\perp$ es un $[n, n-k]_q$-código.*

(*c*) *$\mathcal{C}^{\perp\perp} = \mathcal{C}$.*

Demostración. (*a*) Por definición, $x \in \mathcal{C}^\perp$ si y sólo si $x \cdot c = 0$ para todo $c \in \mathcal{C}$. Se tiene que

$$0 = x \cdot c = x \cdot c^T = x \cdot (uG)^T = (xG^T) \cdot u^T,$$

para algún $u \in \mathbb{F}_q^k$.

($\supseteq$) Si $xG^T = 0$, entonces $x \cdot c = 0$. Luego, $x \in \mathcal{C}^\perp$. Por lo tanto,

$$\{x \in \mathbb{F}_q^n \,:\, xG^T = 0\} \subseteq \mathcal{C}^\perp.$$

($\subseteq$) Si $x \in \mathcal{C}^\perp$, entonces $(x \cdot G^T) \cdot u^T = 0$ para todo $u \in \mathbb{F}_q^k$. En particular, para $u = e_1, \ldots, e_k$, los vectores de la base canónica.

Luego, $0 = (x \cdot G^T) \cdot e_i^T = (x \cdot G^T)^i$ para $1 \leq i \leq k$. Por lo tanto, $u \cdot G^T = 0$. Entonces,

$$\mathcal{C}^\perp \subseteq \{x \in \mathbb{F}_q^n \,:\, x \cdot G^T = 0\}.$$

(*b*) Es claro que $\mathcal{C}^\perp$ es subespacio de $\mathbb{F}_q^n$. Por (*a*),

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \,:\, G \cdot x^T = 0\},$$

o sea, $\mathcal{C}^\perp$ es el espacio solución de k ecuaciones con n incógnitas. Luego, como G tiene rango k, hay $n-k$ variables libres, por lo tanto, $\dim \mathcal{C}^\perp = n-k$.

(*c*) Notar que

$$\mathcal{C} \subset \mathcal{C}^{\perp\perp} = \{x \in \mathbb{F}_q^n \,:\, x \cdot c' = 0 \quad \text{para todo} \quad c' \in \mathcal{C}^\perp\}.$$

Pero $\dim \mathcal{C}^{\perp\perp} = n - (n-k) = k = \dim \mathcal{C}$. Luego, $\mathcal{C} = \mathcal{C}^{\perp\perp}$. □

2.4 La identidad de MacWilliams

Aquí definimos el espectro o distribución de pesos de un código, que es el objeto matemático que nos interesa estudiar más adelante para códigos cíclicos. Luego damos un resultado muy importante, conocido como identidad de MacWilliams ([29]), que relaciona el polinomio enumerador de pesos de un código con el de su dual.

Definición 2.12. Si $\mathcal{C}$ es un (n, M)-código, denotamos con A_i al número de palabras código de peso i, es decir,

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

Los números $A_0, A_1, \ldots, A_n$ se conocen como la *distribución de pesos o espectro* de $\mathcal{C}$ y la suma formal

$$W_{\mathcal{C}}(x) = \sum_{i=0}^{n} A_i x^i \tag{2.1}$$

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

A continuación damos la identidad de MacWilliams para códigos lineales binarios.

Teorema 2.13 (Identidad de MacWilliams para códigos binarios)**.** *Si $\mathcal{C}$ es un $[n, k]$-código binario, el enumerador de pesos del código dual $\mathcal{C}^\perp$ es*

$$W_{\mathcal{C}^\perp}(x) = \tfrac{1}{2^k}(1+x)^n W_{\mathcal{C}}(\tfrac{1-x}{1+x}) = \tfrac{1}{2^k}\sum_{i=0}^{n} A_i (1-x)^i (1+x)^{n-i}. \tag{2.2}$$

Antes de probar el teorema, enunciamos algunos lemas auxiliares.

Lema 2.14. *Sea $\mathcal{C}$ un $[n, k]$-código binario e $y \in \mathbb{F}_2^n \setminus \mathcal{C}^\perp$. Entonces, el producto interno $x \cdot y = 0$ ó $x \cdot y = 1$, con la misma frecuencia cuando x recorre las palabras código de $\mathcal{C}$.*

Demostración. Sean

$$A = \{x \in \mathcal{C} \,:\, x \cdot y = 0\} \quad \text{y} \quad B = \{x \in \mathcal{C} \,:\, x \cdot y = 1\}.$$

Como $y \notin \mathcal{C}^\perp$, entonces existe $u \in B$. Luego, $u + A \subseteq B$, pues si $x \in A$, entonces

$$(u + x) \cdot y = u \cdot y + x \cdot y = 1 + 0 = 1.$$

Luego, $u + x \in B$. Por lo tanto, $u + A \subset B$.

Similarmente, $u + B \subseteq A$. Entonces,

$$|A| = |u + A| \leq |B| = |u + B| \leq |A|.$$

Por lo tanto, $|A| = |B|$. □

Lema 2.15. *Sean $\mathcal{C}$ un $[n, k]$-código binario lineal, $y \in \mathbb{F}_2^n$. Entonces*

$$\sum_{x \in \mathcal{C}} (-1)^{x \cdot y} = \begin{cases} 2^k, & \text{si } y \in \mathcal{C}^\perp, \\ 0, & \text{si } y \notin \mathcal{C}^\perp. \end{cases}$$

Demostración. Si $y \in \mathcal{C}^\perp$, entonces $x \cdot y = 0$ para todo $x \in \mathcal{C}$. Luego,

$$\sum_{x\in\mathcal{C}}(-1)^{x\cdot y} = |\mathcal{C}| = 2^k.$$

Si $y \notin \mathcal{C}^\perp$, por el lema anterior, $(-1)^{x\cdot y}$ es 1 y -1 con la misma frecuencia, por lo tanto,

$$\sum_{x\in\mathcal{C}}(-1)^{x\cdot y} = 0.$$

Entonces, se cumple lo que queríamos ver. □

Lema 2.16. *Para cualquier $x \in \mathbb{F}_2^n$ se cumple la siguiente identidad en $\mathbb{F}_2[z]$,*

$$\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot y}\, z^{w(y)} = (1-z)^{w(x)}(1+z)^{n-w(x)}.$$

Demostración. Si $x \in \mathbb{F}_2^n$ se tiene

$$\begin{aligned}\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot y}\, z^{w(y)} &= \sum_{y_1=0}^{1}\cdots\sum_{y_n=0}^{1} z^{y_1+\cdots+y_n}(-1)^{x_1y_1+\cdots+x_ny_n}\\ &= \sum_{y_1=0}^{1}\cdots\sum_{y_n=0}^{1}\Big(\prod_{i=1}^{n}(-1)^{x_iy_i}\, z^{y_i}\Big)\\ &= \prod_{i=1}^{n}\Big(\sum_{j=0}^{1}(-1)^{jx_i}\, z^j\Big) = (1-z)^{w(x)}(1+z)^{n-w(x)}.\end{aligned}$$

Hemos usado que

$$\sum_{j=0}^{1}(-1)^{jx_i}\, z^j = \begin{cases}1+z, & \text{si } x_i = 0,\\ 1-z, & \text{si } x_i = 1,\end{cases}$$

y esto concluye la prueba. □

Demostración del teorema. Escribiremos el polinomio

$$f(x) = \sum_{u\in\mathcal{C}}\Big(\sum_{v\in\mathbb{F}_2^n}(-1)^{u\cdot v}x^{w(v)}\Big)$$

de dos formas. Por un lado, usando el Lema 2.16, tenemos que

$$f(x) = \sum_{u\in\mathcal{C}}(1-x)^{w(u)}(1+x)^{n-w(u)} = \sum_{i=0}^{n}A_i(1-x)^i(1+x)^{n-i}.$$

Por otro lado, cambiando el orden de la suma y usando el Lema 2.15

$$f(x) = \sum_{v\in\mathbb{F}_2^n}x^{w(v)}\Big(\sum_{u\in\mathcal{C}}(-1)^{u\cdot v}\Big) = \sum_{v\in\mathcal{C}^\perp}x^{w(v)}2^k = 2^kW_{\mathcal{C}^\perp}(x).$$

Luego, se tiene que

$$W_{\mathcal{C}^\perp}(x) = \tfrac{1}{2^k} f(x) = \tfrac{1}{2^k} \sum_{i=0}^{n} A_i (1-x)^i (1+x)^{n-i}.$$

De esta expresión se obtiene (2.2) lo que completa la prueba. □

Enunciamos ahora una versión más general de este teorema sin demostración (no es difícil, utiliza caracteres de grupos abelianos).

Teorema 2.17 (Identidad de MacWilliams generalizada)**.** *Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal, $\mathcal{C}^\perp$ su dual y $W_{\mathcal{C}}(x)$ y $W_{\mathcal{C}^\perp}(x)$ los enumeradores de peso de $\mathcal{C}$ y $\mathcal{C}^\perp$, respectivamente. Entonces*

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

Notar que para $q = 2$ se recupera (2.2).

2.5 Polinomios de Krawtchouk

Introducimos aquí una familia de polinomios ortogonales discretos llamados polinomios de Krawtchouk, que es muy ubicua en problemas de combinatoria. Muchos problemas combinatorios tienen solución dependiendo de la existencia o no de ceros enteros de estos polinomios. Por ejemplo: transformada de Radon discreta, códigos perfectos, cubrimientos perfectos, reconstrucción de grafos, etc ([11], [22]). Para un estudio de los ceros enteros de estos polinomimos consultar los trabajos de Chihara-Stanton, Habsieger y Krasikov-Litsyn ([4], [13], [14], [15], [22], [26]). Incluso, han sido usados en problemas de geometría espectral para producir pares de variedades compactas planas isospectrales (ver los trabajos de Miatello, Podestá y Rossetti [31], [32], [33]). Un excelente survey de este tema es [23].

Sean q (no necesariamente primo) y n enteros positivos. El *polinomio de Krawtchouk q-ario de orden n y grado k*, con $0 \le k \le n$, se define como

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

Notar que $K_k^{n,q}(\ell) \in \mathbb{Z}$ para todo $\ell \in \mathbb{Z}$ entero. Cuando esté claro el valor de n y q, escribiremos simplemente $K_k(x)$. Por ejemplo, cuando $q = 2$ se dicen polinomios binarios de Krawtchouk y se omite el 2 de la notación. Usaremos estos polinomios binarios para el cálculo de espectro de códigos binarios.

Estos polinomios tienen la siguiente función generatriz

$$\sum_{k=0}^{\infty} K_k^{n,q}(x)\, z^k = \big(1+(q-1)z\big)^{n-x}(1-z)^x. \tag{2.3}$$

Además, satisfacen varias relaciones de recurrencia.

Teorema 2.18. *Los polinomios de Krawtchouk satisfacen la siguiente recurrencia*

$$(k+1)K_{k+1}^{n,q}(x) = ((n-k)(q-1)+k-qx)K_k^{n,q}(x) - (q-1)(n-k+1)K_{k-1}^{n,q}(x),$$

para $k = 1, 2, \ldots, n-1$, *con valores iniciales* $K_0(x) = 1$, $K_1(x) = n - 2x$.

Demostración. Se puede encontrar en [30]. □

Veamos ahora cuál es la relación entre estos polinomios y la distribución de pesos de un código. Sea $\mathcal{C}$ un $[n,k,d]_q$-código y $\mathcal{C}^\perp$ el $[n,n-k,d^\perp]_q$-código dual. La distribución de pesos de $\mathcal{C}$ es $A_0, A_1, \ldots, A_n$, y el enumerador de peso de $\mathcal{C}$ es el polinomio dado en (2.1). Por la identidad de MacWilliams y usando la función generatriz de estos polinomios dada en (2.3), tenemos que

$$\begin{aligned}
\sum_{i=0}^{n} A_i^\perp x^i = W_{\mathcal{C}}^\perp(x) &= \frac{1}{|\mathcal{C}|}(1+(q-1)x)^n\, W_{\mathcal{C}}\Big(\tfrac{1-x}{q+(q-1)x}\Big) \\
&= \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} A_i(1-x)^i(1+(q-1)x)^{n-i} \\
&= \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} A_i\Big(\sum_{j=0}^{\infty} K_j^{n,q}(i)x^j\Big) \\
&= \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n}\Big(\sum_{j=0}^{n} A_j K_i^{n,q}(j)\Big)x^i.
\end{aligned}$$

Esto nos dice que podemos escribir los números $A_i^\perp$ del código dual en términos de los A_i y de los polinomios de Krawtchouk de la siguiente manera

$$A_i^\perp = \sum_{j=0}^{n} A_j\, K_i^{n,q}(j). \tag{2.4}$$

2.6 Códigos cíclicos

Dentro de la familia de códigos lineales se destaca la clase de códigos cíclicos. Estos códigos son cerrados por permutaciones cíclicas y son algunos de los más usados por sus buenos parámetros y por poseer algoritmos eficientes de codificación y decodificación. Entre ellos se destacan los códigos de Golay binarios y ternarios, los códigos de Reed-Solomon, BCH y Reed-Muller y los códigos de residuos cuadráticos, entre otros.

Definición 2.19. Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es *cíclico* si se cumple que si $c_0c_1\cdots c_{n-1} \in \mathcal{C}$, entonces $c_{n-1}c_0\cdots c_{n-2} \in \mathcal{C}$.

Notemos que, por definición, un código lineal $\mathcal{C}$ es cíclico si es cerrado por el desplazamiento cíclico

$$c_0c_1\cdots c_{n-1} \mapsto c_k\cdots c_{n-1}c_0\cdots c_{k-1}.$$

O sea, si denotamos por $s : \mathbb{F}_q^n \to \mathbb{F}_q^n$ al desplazamiento cíclico

$$s(x_0x_1\cdots x_{n-1}) = x_{n-1}x_0\cdots x_{n-2},$$

entonces $\mathcal{C}$ es cíclico si y sólo si dado $c \in \mathcal{C}$ vale que

$$s^k(c) \in \mathcal{C} \qquad \text{para todo } \ k = 1, \ldots, n.$$

Notar que $s \in End(\mathbb{F}_q^n)$. Más aún, s es un automorfismo, ya que como $s^n = id$, entonces $s^{-1} = s^{n-1}$. De esta manera, tenemos que $\mathcal{C}$ es un código cíclico si y sólo si $s(\mathcal{C}) \subseteq \mathcal{C}$, y esto pasa si y sólo si $s \in Aut(\mathcal{C})$.

Ejemplo 2.20. Consideramos el $[7, 4, 3]$-código de Hamming binario.

$$\mathcal{C} = H_2(3) = \left\{ \begin{array}{ll} 0000000, & 1111111 \\ 1101000, & 0010111 \\ 0110100, & 1001011 \\ 0011010, & 1100101 \\ 0001101, & 1110010 \\ 1000110, & 0111001 \\ 0100011, & 1011100 \\ 1010001, & 0101110 \end{array} \right\}$$

Es inmediato ver que $\mathcal{C}$ es lineal.

Como $\mathcal{C}$ está formado por las palabras $0 = 0000000$, $1 = 1111111$ y los desplazamientos cíclicos de $c = 1101000$ y de su complemento $\overline{c} = 0010111$, se ve que $\mathcal{C}$ es un código cíclico.

Si $\mathcal{C}$ es un código en $\mathbb{F}_q^n$, a cada palabra código c podemos asignarle, de manera natural, un polinomio $c(x)$ mediante la aplicación

$$\Phi : \mathcal{C} \longrightarrow \mathbb{F}_q[x],$$

definida por

$$c = c_0c_1\cdots c_{n-1} \quad \mapsto \quad \Phi(c) = c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

Notar que Φ es inyectiva y por lo tanto una biyección entre $\mathbb{F}_q^n$ y el conjunto $(\mathbb{F}_q[x])_n$ de polinomios de grado menor que n.

Veamos ahora como expresar los desplazamientos cíclicos en términos de polinomios. Consideremos el ideal principal generado por $x^n - 1$ en el anillo de polinomios $\mathbb{F}_q[x]$, es decir

$$\langle x^n - 1\rangle = \{f(x)(x^n - 1) : \ f(x) \in \mathbb{F}_q[x]\}.$$

Recordemos que si R es un anillo conmutativo, un subanillo $I \subset R$ es un ideal si $xr = rx \in I$ para todo $x \in I$, $r \in R$. El cociente

$$R_{q,n} = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} = \{f(x) + \langle x^n - 1\rangle : \ f(x) \in (\mathbb{F}_q[x])_n\}$$

es el álgebra de polinomios de grado menor que n, con la suma usual de polinomios y el producto de polinomios módulo $x^n - 1$. Un elemento en $R_{q,n}$ es de la forma

$$f(x) + \langle x^n - 1\rangle \qquad \text{ó} \qquad \overline{f(x)} \pmod{(x^n - 1)},$$

pero lo denotamos simplemente por $f(x)$.

Proposición 2.21. *Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es cíclico si y sólo si $\Phi(\mathcal{C}) \subset R_{q,n}$ es un ideal.*

Demostración. $\Phi(\mathcal{C})$ es un ideal en $R_{q,n}$ si dados $p(x) = p_0 + p_1 x + \cdots + p_r x^r \in R_{q,n}$ y $c = c_0 c_1 \cdots c_{n-1} \in \mathcal{C}$ se tiene que

$$p(x)c(x) \in \Phi(\mathcal{C})$$

con $c(x) = \Phi(c)$. Por linealidad de $\Phi(c)$, esto resulta equivalente a $xc(x) \in \Phi(C)$. En $R_{q,n}$ se tiene que

$$\begin{aligned} x(c_0 + c_1 x + \cdots + c_{n-1}) &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &\equiv c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} \pmod{(x^n - 1)}. \end{aligned}$$

Es decir, $xc(x) = s(c)(x)$. De aquí, el resultado sigue claramente. □

A partir de ahora pensaremos, como es habitual, a las palabras código directamente como polinomios.

Teorema 2.22. *Sea $\mathcal{C}$ un ideal en $\frac{\mathbb{F}_q^n[x]}{\langle x^n - 1\rangle}$. Entonces:*

(a) *Existe un único polinomio mónico $g(x)$ de grado mínimo en $\mathcal{C}$. Además, $\mathcal{C} = \langle g(x)\rangle$.*

(b) *$g(x) \mid x^n - 1$.*

(c) *Si $gr(g(x)) = r$ entonces $\mathcal{C} = \langle g(x)\rangle = \{r(x)g(x) \ : \ gr(r(x)) < n - r\}$.*

(d) *$\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ es una base de $\mathcal{C}$ y $\dim(\mathcal{C}) = k = n - r$.*

Demostración. (a) Supongamos que $\mathcal{C}$ contiene 2 polinomios mónicos distintos, $g_1(x)$ y $g_2(x)$, de grado mínimo. Entonces, $g_1(x) - g_2(x)$ es un polinomio no nulo de grado menor que r, lo cuál es absurdo. Luego, existe un único polinomio mónico de grado mínimo r en $\mathcal{C}$. Lo llamamos $g(x)$.

Veamos que $\mathcal{C} = \langle g(x)\rangle$. Como $g(x) \in \mathcal{C}$, y $\mathcal{C}$ es un ideal, tenemos que $\langle g(x)\rangle \subset \mathcal{C}$. Por otra parte, supongamos que $p(x) \in \mathcal{C}$. Existen únicos $q(x)$, $r(x)$ tales que

$$p(x) = q(x)g(x) + r(x),$$

con $\mathrm{gr}(r(x)) < r$ ó $r(x) = 0$.

Luego, como $r(x) = p(x) - q(x)g(x) \in \mathcal{C}$ y tiene grado menor que r, necesariamente $r(x) = 0$. Así, $p(x) \in \langle g(x) \rangle$ y $\mathcal{C} \subset \langle g(x) \rangle$. Por lo tanto,

$$\mathcal{C} = \langle g(x) \rangle.$$

(b) Existen únicos $q(x)$, $r(x)$ tal que

$$x^n - 1 = q(x)g(x) + r(x)$$

con $r(x)$ de grado menor que r o $r(x) = 0$. Como $x^n - 1 = 0 \in \mathcal{C}$ en $R_{q,n}$, entonces $r(x) = -q(x)g(x) \in \mathcal{C}$ y por lo tanto $r(x) = 0$, de donde

$$g(x) \mid x^n - 1,$$

que es lo que queríamos ver.

(c) Sabemos que $\mathcal{C} = \langle g(x) \rangle = \{f(x)g(x) : f(x) \in R_{q,n}\}$. Queremos ver que basta restringirse a $f(x)$ con $\mathrm{gr}(f(x)) < n - r$. Se tiene que

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

para algún polinomio $h(x)$ de grado $n - r$. Dividiendo, tenemos, $f(x) = q(x)h(x) + r(x)$ con $\mathrm{gr}(r(x)) < n - r$ o $r(x) = 0$. Entonces,

$$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x),$$

y así,

$$f(x)g(x) = r(x)g(x) \text{ en } R_{q,n}.$$

Luego, se cumple (c).

(d) Por (c), $\mathcal{C}$ está generado por $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$. Como este es un conjunto linealmente independiente, pues son todos polinomios de grado distinto, resulta una base de $\mathcal{C}$ y, por lo tanto, $\dim(\mathcal{C}) = n - r$. □

Definición 2.23. Al polinomio $g(x)$ del Teorema 2.22, se lo llama *polinomio generador* o *generador polinomial* de $\mathcal{C}$.

Como el polinomio generador $g(x)$ de un $[n, n-r]$-código cíclico en $R_{n,q}$ divide a $x^n - 1$ tenemos que

$$x^n - 1 = g(x)h(x),$$

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

Teorema 2.24. *Sea $h(x)$ el polinomio de chequeo de un código cíclico $\mathcal{C}$ en $R_{q,n}$.*

(a) *El código $\mathcal{C}$ puede describirse como*

$$\mathcal{C} = \{p(x) \in R_{q,n} : p(x)h(x) \equiv 0\}.$$

(*b*) *Si* $h(x) = h_0 + h_1x + \cdots + h_{n-r}x^{n-r}$, *entonces la matriz de paridad de* $\mathcal{C}$ *está dada por*

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

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

$$h^\perp(x) = h_0^{-1}x^{n-r}h(x^{-1}) = h_0^{-1}(h_0x^{n-r} + h_1x^{n-r-1} + \cdots + h_{n-r}).$$

Demostración. (*a*) Sea $\mathcal{C} = \langle g(x)\rangle$. Si $p(x) \in \mathcal{C}$, entonces $p(x) = f(x)g(x)$ para algún $f(x) \in R_{q,n}$. Luego

$$p(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv 0.$$

Recíprocamente, sea $p(x) \in R_{q,n}$ tal que $p(x)h(x) \equiv 0$. Dividiendo, se tiene que $p(x) = q(x)g(x) + r(x)$ con $\mathrm{gr}r(x) < r$ ó $r(x) = 0$. Entonces,

$$0 \equiv p(x)h(x) = q(x)g(x)h(x) + r(x)h(x) \equiv r(x)h(x).$$

Sin embargo, gr $r(x)h(x) < r + (n - r) = n$, por lo que $r(x)h(x) = 0$. Luego, $r(x) = 0$ y $p(x) = q(x)g(x) \in \mathcal{C}$.

(*b*) Si $c(x) \in \mathcal{C}$, entonces $c(x)h(x) \equiv 0$. Ahora, como $\mathrm{gr}c(x)h(x) < 2n - r$, reduciendo módulo x^n-1, vemos que los coeficientes de $x^{n-r}, x^{n-r+1}, \ldots, x^{n-1}$ en el producto $c(x)h(x)$ son cero, es decir, tenemos el siguiente sistema de ecuaciones

$$\begin{aligned} c_0h_{n-r} + c_1h_{n-r-1} + \cdots + c_{n-r}h_0 &= 0 \\ c_1h_{n-r} + c_2h_{n-r-1} + \cdots + c_{n-r+1}h_0 &= 0 \\ &\vdots \\ c_{r-1}h_{n-r} + c_rh_{n-r-1} + \cdots + c_{n-1}h_0 &= 0. \end{aligned}$$

Pero esto es equivalente a $(c_0c_1 \ldots c_{n-1})H^T = 0$, y así H genera un código $\mathcal{C}'$ que es ortogonal a $\mathcal{C}$, o sea, $\mathcal{C}' \subseteq \mathcal{C}^\perp$. Commo $h_{n-r} \neq 0$, sigue que $\dim\mathcal{C}' = r$ y por lo tanto $\mathcal{C}' = \mathcal{C}^\perp$.

(*c*) Notar que $h_0 \neq 0$. Como $h(x)g(x) = x^n - 1$ entonces $h(x^{-1})g(x^{-1}) = x^{-n} - 1$ o sea

$$x^{n-r}h(x^{-1})x^rg(x^{-1}) = 1 - x^n$$

de donde sale que el polinomio mónico $g(x)^\perp = h_0^{-1}x^{n-r}h(x^{-1})$ divide a $x^n - 1$. Luego, el código cíclico generado por $g(x)^\perp$ tiene una matriz generadora H, y por lo tanto, $\langle g(h)^\perp\rangle = \mathcal{C}^\perp$. □

Códigos cíclicos irreducibles

Se dice que $\mathcal{C}$ es un *código irreducible* si $h(x)$ es irreducible sobre $\mathbb{F}_q$. De lo contrario, $\mathcal{C}$ se dice reducible. Estos códigos son conocidos también como códigos minimales, que se definen de la siguiente manera.

Supongamos que

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

es la factorización de $x^n - 1$ en polinomios irreducibles sobre $\mathbb{F}_q$. Los códigos cíclicos $M_i = \langle m_i(x) \rangle$ se dicen maximales. Similarmente, si tenemos

$$\overline{m_i}(x) = \frac{x^n - 1}{m_i(x)},$$

entonces los códigos cíclicos $\overline{M_i} = \langle \overline{m_i}(x) \rangle$ son minimales.

El siguiente teorema nos da una caracterización de los códigos cíclicos irreducibles como códigos traza.

Teorema 2.25. *Sea $g(x)$ un factor irreducible de $x^n - 1$ sobre $\mathbb{F}_q$. Supongamos que $g(x)$ tiene grado s, y sea $\gamma \in \mathbb{F}_{q^s}$ una raíz de $g(x)$. Sea $\mathrm{Tr}_s : \mathbb{F}_{q^s} \mapsto \mathbb{F}_q$ la función traza. Entonces*

$$\mathcal{C}_\gamma = \Big\{ \sum_{i=0}^{n-1} \mathrm{Tr}_s(\xi \gamma^i)\, x^i \ : \ \xi \in \mathbb{F}_{q^s} \Big\}$$

es un $[n, s]$-código cíclico irreducible cuyos no-ceros son $\{\gamma^{-q^i} : 0 \leq i < s\}$.

Demostracion. Por Lema 1.5, $\mathcal{C}_\gamma$ es un código lineal sobre $\mathbb{F}_q$. Si

$$c_\xi(x) = \sum_{i=0}^{n-1} \mathrm{Tr}_s(\xi \gamma^i)\, x^i,$$

entonces $c_{\xi\gamma^{-1}}(x) = c_\xi(x)x$ en $R_{q,n}$, lo que implica que $\mathcal{C}_\gamma$ es cíclico. Sea $g(x) = \sum_{i=0}^{n-1} g_i x^i$. Por el Lema 1.5, como $g_i \in \mathbb{F}_q$ y $g(\gamma) = 0$, tenemos

$$g \cdot c_\xi = \sum_{i=0}^{n-1} g_i \mathrm{Tr}_s(\xi \gamma^i) = \mathrm{Tr}_s\Big(\xi \sum_{i=0}^{n-1} g_i \gamma^i \Big) = \mathrm{Tr}_s(0) = 0.$$

Entonces, $\langle g(x) \rangle \subseteq \mathcal{C}_\gamma^\perp$.

Además, $\mathcal{C}_\gamma^\perp$ es un código cíclico distinto de $R_{q,n}$. Como $g(x)$ es irreducible sobre $\mathbb{F}_q$, no hay códigos cíclicos propios entre $\langle g(x) \rangle$ y $R_{q,n}$. Entonces, $\langle g(x) \rangle = \mathcal{C}_\gamma^\perp$. Luego, $\mathcal{C}_\gamma$ es un código cíclico irreducible. □

2.7 Teorema de Delsarte

En esta sección damos un resultado muy importante, el Teorema de Delsarte, que combinado con las identidades de MacWilliams nos permitirá hallar distribuciones de peso de

códigos cíclicos siguiendo una estrategia general.

Dada una extensión de cuerpos $\mathbb{F}_{q^m}/\mathbb{F}_q$ y un código q^m-ario $\mathcal{C}$, existen dos formas canónicas de asociarle códigos con palabras en el cuerpo más pequeño, restringiendo o traceando.

Definición 2.26. Sea $\mathcal{C}$ un $[n,k]$-código lineal sobre $\mathbb{F}_{q^m}$. El *código restricción* de $\mathcal{C}$ respecto a $\mathbb{F}_q$ es

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

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

Otra forma 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, que definimos en la sección de cuerpos finitos del capítulo anterior.

Dado un vector $c = (c_1, \ldots, c_n) \in \mathbb{F}_{q^m}^n$ podemos definir su traza por

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

Definición 2.27. 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

$$\mathrm{Tr}(\mathcal{C}) = \{\mathrm{Tr}_{q^m/q}(c) \,:\, c \in \mathcal{C}\}.$$

Notemos que si $\mathcal{C}$ es un código cíclico sobre $\mathbb{F}_{q^m}$, entonces tanto $\mathrm{Res}(\mathcal{C})$ como $\mathrm{Tr}(\mathcal{C})$ resultan cíclicos.

Veamos ahora el famoso Teorema de Delsarte ([10]) que relaciona las trazas de los duales con las restricciones.

Teorema 2.28. *Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_{q^m}$. Entonces tenemos que*

$$(\mathrm{Res}(\mathcal{C}))^\perp = \mathrm{Tr}(\mathcal{C}^\perp),$$

Demostración. Primero veamos que $(\mathrm{Res}(\mathcal{C}))^\perp \supseteq \mathrm{Tr}(\mathcal{C}^\perp)$.

Sean $c = (c_1, \ldots, c_n) \in \mathcal{C}^\perp$ y $b = (b_1, \ldots, b_n) \in \mathrm{Res}(\mathcal{C})$. Por la linealidad de la traza, se tiene que

$$\mathrm{Tr}(c) \cdot b = \sum_{i=1}^{n} \mathrm{Tr}(c_i) b_i = \mathrm{Tr}\Big(\sum_{i=1}^{n} c_i b_i\Big) = \mathrm{Tr}(c \cdot b) = \mathrm{Tr}(0) = 0.$$

Luego, $\mathrm{Tr}(c) \in \mathrm{Res}(\mathcal{C})^\perp$.

Ahora veamos que $(\mathrm{Tr}(\mathcal{C}^\perp))^\perp \subseteq \mathrm{Res}(\mathcal{C})$. Sea $a = (a_1, \ldots, a_n) \in (\mathrm{Tr}(\mathcal{C}^\perp))^\perp$. Como $a_i \in \mathbb{F}_q$ para $1 \leq i \leq n$, solo hace falta ver que $a \in \mathcal{C}$. Para $b = (b_1, \ldots, b_n) \in \mathcal{C}^\perp$ se tiene que $\beta b \in \mathcal{C}^\perp$ para todo $\beta \in \mathbb{F}_{q^m}$, y entonces

$$0 = a(\mathrm{Tr}(\beta b)) = \sum_{i=1}^{n} a_i \mathrm{Tr}(\beta b_i) = \mathrm{Tr}\Big(\beta \sum_{i=1}^{n} a_i b_i\Big) = \mathrm{Tr}(\beta(a \cdot b)).$$

Entonces, $a \cdot b = 0$ y $a \in \mathcal{C}$. Luego, $(\mathrm{Tr}(\mathcal{C}^{\perp}))^{\perp} \subseteq \mathrm{Res}(\mathcal{C})$.

Por lo tanto,

$$\mathrm{Tr}(\mathcal{C}^{\perp}) \subseteq (\mathrm{Res}(\mathcal{C}))^{\perp},$$

y se cumple lo que queríamos. □

El teorema afirma que se cumple el siguiente diagrama

$$\begin{array}{ccc} \mathcal{C} & \overset{\text{dual}}{\longleftrightarrow} & \mathcal{C}^{\perp} \\ \mathrm{Res}\downarrow & & \downarrow \mathrm{Tr} \\ \mathrm{Res}(\mathcal{C}) & \overset{\text{dual}}{\longleftrightarrow} & \mathrm{Res}(\mathcal{C})^{\perp} \end{array}$$

Consecuencia para códigos cíclicos irreducibles

Sean $q = p^m$, α un generador de $\mathbb{F}_p^*$ y

$$h(x) = h_1(x) \cdots h_t(x) \in \mathbb{F}_p[x],$$

donde $h_j(x)$ son polinomios irreducibles distintos sobre $\mathbb{F}_p$. Para cada $1 \leq j \leq t$, sea

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

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

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

Por lo tanto, $\mathrm{gr}(h_j(x)) = m_j$ para todo $j = 1, \ldots, t$.

Pongamos

$$n = \tfrac{q-1}{\delta} \qquad \text{con} \quad \delta = \mathrm{mcd}(q-1, s_1, \ldots, s_t)$$

y definamos el código

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

donde

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

Por el Teorema de Delsarte, $\mathcal{C}$ es un $[n,k]$-código cíclico con polinomio de chequeo $h(x)$ y $k = m_1 + \cdots + m_t$, por lo tanto todo código cíclico puede ser definido dando solamente los ceros del polinomio de chequeo vía esta contrucción. Una consecuencia de esto último es que todo código cíclico irreducible es un código traza, lo cuál resulta muy importante para los fines de este trabajo.

2.8 Códigos más conocidos

Introduciremos la definición de algunos de los códigos lineales y cíclicos más importantes, y de los que hablaremos en los próximos capítulos: Hamming, BCH y Reed-Muller. Por cuestiones de espacio, hemos dejado afuera de esta lista a los códigos de Golay, de Reed-Solomon, de residuos cuadráticos y de Goppa racionales, que son igualmente útiles y famosos.

2.8.1 Códigos de Hamming

Los códigos de Hamming binarios son los códigos más antiguos que se conocen y fueron introducidos por Richard Hamming en 1950 en [16]. En esa época las 'computadoras' funcionaban con tarjetas perforadas. Richard dejaba a las máquinas calculando toda la noche y al llegar a la mañana recibía el desagradable mensaje 'parity check error'. Cansado de lidiar con esto inventó los códigos que llevan su nombre y que corrigen 1 error.

Si formamos la matriz H cuyas columnas son las 2^r-1 palabras no nulas de $\mathbb{F}_2^r$, tenemos una matriz $r \times n$, con $n = 2^r - 1$, en donde cualquier par de columnas son linealmente independientes, pero hay tres columnas linealmente dependientes. Luego, H es la matriz de paridad de un código lineal, denotado por $H_2(r)$, con parámetros

$$n = 2^r - 1, \qquad k = n - r, \qquad d = 3.$$

Este es el llamado *código de Hamming binario de orden* r.

Los códigos Hamming binarios pueden generalizarse a cualquier alfabeto $\mathbb{F}_q$. Para cada r fijo, construimos la matriz $H_{q,r}$ de la siguiente manera. Elegimos cualquier columna no nula $c_1 \in V_1 = \mathbb{F}_q^r$. Luego, elegimos cualquier columna no nula

$$c_2 \in V_2 = V_1 \setminus \{\alpha c_1 \,:\, \alpha \in \mathbb{F}_q^*\}.$$

Continuamos eligiendo columnas no nulas de esta forma y descartamos los múltiplos escalares de las columnas elegidas hasta agotar todas las columnas de $\mathbb{F}_q^r$. Como cada columna $c \in \mathbb{F}_q^r$ tiene $q-1$ múltiplos escalares no nulos αc, $\alpha \in \mathbb{F}_q$, vemos que la matriz $H_{q,r}$ formada por las columnas c_i tiene $\frac{q^r-1}{q-1}$ columnas.

La matriz $H_{q,r} \in M_{r\times n}(\mathbb{F}_q)$ con $n = \frac{q^r-1}{q-1}$ se llama de Hamming de orden r y es la matriz de paridad de un código lineal q-ario con parámetros

$$n = \frac{q^r-1}{q-1}, \qquad k = n - r, \qquad d = 3,$$

denotado por $H_q(r)$ y llamada *código de Hamming q-ario de orden r*.

Cuando $(n, q-1) = 1$, $H_q(r)$ puede ser visto como un código cíclico. Por ejemplo, los códigos Hamming binarios son cíclicos, al igual que los ternarios de longitud impar. 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 $H_q(r)$ es

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

Notar que su polinomio generador es

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

Códigos simplex

Los duales de los códigos Hamming son llamados *códigos simplex*. Son $[\frac{q^r-1}{q-1}, r]_q$-códigos. El peso de las palabras de este código tiene una propiedad interesante.

Teorema 2.29. *Las palabras no nulas del $[\frac{q^r-1}{q-1}, r]_q$-código simplex sobre $\mathbb{F}_q$ tienen todas peso $q^r - 1$. En particular, la distancia mínima es $d = q^r - 1$.*

Para códigos simplex binarios veamos una construcción recursiva y una prueba para el teorema. Sea G_2 la matriz

$$G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Para $r \geq 3$, definimos G_r por inducción como

$$G_r = \begin{pmatrix} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ & & & 0 & & & \\ & G_{r-1} & & \vdots & & G_{r-1} & \\ & & & 0 & & & \end{pmatrix}$$

Afirmamos que el código $S_2(r)$ generado por G_r es el dual de $H_2(r)$. Claramente, G_r tiene una fila más que G_{r-1} y, como G_2 tiene dos filas, G_r tiene r filas. Si llamamos n_r al número de columnas de G_r, tenemos que $n_2 = 2^2 - 1$ y $n_r = 2n_{r-1} + 1$; entonces, por inducción, $n_r = 2^r - 1$. Las columnas de G_2 son distintas de cero y distintas entre ellas, luego, por construcción, las columnas de G_r son distintas de cero y distintas entre ellas. Entonces, G_r tiene $2^r - 1$ columnas distintas de longitud r. Pero hay solo $2^r - 1$ r-uplas distintas, éstas son las expansiones binarias de $1, 2, \ldots, 2^r - 1$. Entonces,

$$S_2(r) = H_2(r)^\perp.$$

Las palabras no nulas de $S_2(2)$ tienen peso 2. Asumimos que las palabras distintas de cero de $S_2(r-1)$ tienen peso 2^{r-2}. Entonces, las palabras no nulas del subcódigo generado por las últimas $r - 1$ filas de G_r tienen la forma $(a, 0, b)$, donde $a, b \in S_2(r-1)$. Luego, estas palabras tienen peso $2 \cdot 2^{r-2} = 2^{r-1}$.

También la primer fila de G_r tiene peso $1 + 2^{r-1} + 1 = 2^{r-1}$. El resto de las filas de $S_2(r)$ tienen la forma $(a, 1, b + 1)$, donde $a, b \in S_2(r-1)$. Como $w(b+1) = 2^{r-2} - 1$, entonces

$$w(a, 1, b + 1) = 2^{r-2} + 1 + 2^{r-2} - 1 = 2^{r-1}.$$

Luego, por inducción, todas las palabras distintas de cero de $S_2(r)$ tienen peso 2^{r-1}.

2.8.2 Códigos BCH

Ahora veremos los códigos BCH, que llevan ese nombre pues fueron introducidos y estudiados en 1959-1960 por Bose y Ray-Chadhuri y por Hocquenghem en los trabajos [1], [2] y [18].

El *código cíclico* $BCH_{n,q}(\delta)$ de longitud n y distancia diseñada δ, con δ un entero tal que $2 \leq \delta \leq n$, es el código cíclico cuyo polinomio generador es de la forma

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

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 $\mathbb{F}_q$.

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

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

Ésta 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 que satisface

$$d \geq \delta.$$

Más aún, como las entradas de H están en $\mathbb{F}_{q^m}$, éstas 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

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

En el caso particular que $q = 2$, $a = 1$ y $\delta = 4$, nos referimos a $BCH_{n,q}(\delta)$ como el código BCH binario de longitud $2^m - 1$. 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 $i = 1, 3$.

2.8.3 Códigos Reed-Muller

Los siguientes códigos que veremos fueron originalmente introducidos en 1954 por Muller en [35]. El mismo año, Reed dió un método de decodificación ([36]). Hoy se los conoce como códigos de Reed-Muller. Daremos una descripción recursiva alternativa. Estos

códigos generalizan a los códigos de Reed-Solomon.

Para $0 \leq r \leq m$, el *código de Reed-Muller* de orden r y longitud 2^m, denotado por $RM(r,m)$ se define recursivamente de la siguiente manera.

- $RM(0,m) = Rep_2(2m) = \{0,1\}$,
- $RM(m,m) = \mathbb{Z}_2^{2^m}$,
- $RM(r,m) = RM(r,m-1) \oplus RM(r-1,m-1), \quad \text{si} \quad 0 < r < m.$

Es decir,

$$RM(r,m) = \big\{(u, u+v) \in \mathbb{Z}_2^{2^m} \,:\, u \in RM(r,m-1),\, v \in RM(r-1,m-1)\big\}.$$

Este código tiene parámetros

$$n = 2^m, \qquad k = \sum_{i=0}^{r} \binom{m}{i}, \qquad d = 2^{m-r}.$$

Enuciamos a continuación, sin demostración, algunas propiedades importantes de estos códigos.

Teorema 2.30. *Sea* $0 \leq r \leq m$.

(*a*) $R(r,m)$ *tiene matriz generadora*

$$G_{0,m} = \underbrace{(11\cdots1)}_{(m+1)-veces}, \quad G_{m,m} = \begin{pmatrix} G_{m-1,m} \\ 0\cdots01 \end{pmatrix},$$

$$G_{r,m} = \begin{pmatrix} G_{r,m-1} & G_{r,m-1} \\ 0 & G_{r-1,m-1} \end{pmatrix} \qquad si \quad 0 < r < m.$$

(*b*) $RM(r-1,m) \subset R(r,m)$ *para* $r > 0$. *Es decir,*

$$RM(0,m) \subset RM(1,m) \subset \cdots \subset RM(r-1,m) \subset RM(r,m).$$

(*c*) *Todas las palabras en* $RM(1,m)$, *salvo* $\mathbf{0} = (0,\ldots,0)$ *y* $\mathbf{1} = (1,\ldots,1)$, *tienen peso* 2^{m-1}.

(*d*) $RM^{\perp}(r,m) = RM(m-1-r,m)$ *con* $r < m$.

Capítulo 3

Distribución de pesos de códigos lineales

En este capítulo nos dedicamos a la distribución de pesos de códigos lineales y cíclicos a partir de diferentes estrategias. En primer lugar, definimos el género de un código y vemos el enumerador de pesos como un polinomio en $x-1$, lo que nos lleva a un teorema que nos da algunas desigualdades para los coeficientes del enumerador en esta representación, los cuáles tienen cierta relación con los números A_i que buscamos. A continuación analizamos qué nos dice este teorema en el caso de los códigos MDS y, en particular, en códigos de Hamming. En la siguiente sección mostramos algunos resultados sobre la relación entre la distribución de pesos de códigos cíclicos irreducibles y el número de soluciones de ciertas ecuaciones diagonales.

3.1 Códigos lineales y enumeradores de peso

Sea $\mathcal{C}$ un $[n,k,d]_q$-código. Recordamos que A_i es el número de palabras de peso i en $\mathcal{C}$. Notemos que se cumple que

$$\sum_{i=0}^{n} A_i = q^k.$$

Homogeneizando el polinomio enumerador de peso del código $\mathcal{C}$, definido en (2.1), obtenemos

$$W_{\mathcal{C}}(x,y) = \sum_{c\in\mathcal{C}} x^{|c|}y^{n-|c|} = \sum_{i=0}^{n} A_i\, x^i\, y^{n-i}, \tag{3.1}$$

donde $|c|$ es el soporte de la $c=(c_1,\ldots,c_n)$, es decir,

$$|c| = \#\{1\le i\le n \,:\, c_i\neq 0\}.$$

A veces es conveniente considerar el polinomio no homogéneo. A partir del polinomio enumerador de pesos homogéneo en (3.1) podemos recuperar el polinomio enumerador de

pesos no homogéneo de la siguiente manera

$$W_{\mathcal{C}}(x,1) = W_{\mathcal{C}}(x) = \sum_{i=0}^{n} A_i x^i.$$

El código $\mathcal{C}$ tiene exactamente una palabra código de peso 0 y no tiene otras palabras de peso menor a d. Entonces, tenemos que

$$A_0 = 1, \qquad A_1 = \cdots = A_{d-1} = 0, \qquad A_d \neq 0,$$

y esto nos dice que podemos escribir

$$W_{\mathcal{C}}(x,y) = y^n + x^d \sum_{i=0}^{n-d} A_{d+i}\, x^i\, y^{n-d-i}.$$

Como en muchos casos no sabemos el valor exacto de d, pero conocemos alguna cota, es más conveniente escribirlo de la siguiente forma. Sea a un entero tal que $d \geq n - a$, entonces

$$W_{\mathcal{C}}(x) = 1 + \sum_{i=0}^{a} A_{d+i}\, x^i. \tag{3.2}$$

Luego, podemos ver fácilmente que si $d > n - a$, entonces tenemos una representación del polinomio enumerador de pesos dada por

$$W_{\mathcal{C}}(x) = x^n + \sum_{i=0}^{a} B_i (x-1)^i, \tag{3.3}$$

donde, si comparamos las expresiones (3.2) y (3.3), tenemos que los números A_i y B_i están relacionados por

$$B_i = \sum_{j=n-a}^{n-i} \tbinom{n-j}{i} A_j \qquad \text{y} \qquad A_i = \sum_{j=n-i}^{a} (-1)^{n+i+j} \tbinom{j}{n-i} B_j. \tag{3.4}$$

A partir de la identidad de MacWilliams, y homogeneizando los polinomios $W_{\mathcal{C}}(x)$ y $W_{\mathcal{C}^\perp}(x)$, obtenemos la expresión homogénea de las identidades de MacWilliams

$$W_{\mathcal{C}^\perp}(x,y) = \tfrac{1}{q^k} W_{\mathcal{C}}\big(x + (q-1)y, x - y\big). \tag{3.5}$$

3.1.1 Un resultado general

Existen muchas cotas que involucran los paramétros de un código, como por ejemplo las cotas de Hamming, de Gilbert-Varshamov, de Griesmer, etc. Recordamos ahora la más simple de todas.

Proposición 3.1 (Cota de Singleton)**.** *Si $\mathcal{C}$ es un $[n,k,d]_q$-código lineal entonces*

$$d \leq n - k + 1.$$

Los códigos cuyos parámetros alcanzan la igualdad en la cota de Singleton se llaman *códigos MDS* (por 'maximum distance separable'), ya que son los que tienen la mayor distancia posible entre todos los códigos con longitud y tamaño fijos.

Esto motiva la siguiente definición.

Definición 3.2. Sea g un entero no negativo. Un código $\mathcal{C}$ es llamado de *género a lo sumo* g si g es el mínimo entero tal que se cumplen las siguientes relaciones

$$k + d \geq n + 1 - g \qquad \text{y} \qquad (n-k) + d^{\perp} \geq n + 1 - g.$$

En este caso, $\mathcal{C}^{\perp}$ también resulta un código de género a lo sumo g. Notemos que los códigos MDS que definimos antes son de género a lo sumo cero.

Definimos el número

$$a = k + g - 1 \tag{3.6}$$

que será de gran utilidad en lo que resta de la sección.

El siguiente resultado para códigos lineales generales es muy importante ya que determina una parte del espectro y da cotas para la otra parte. Esto en combinación con otras propiedades conocidas, resulta muy útil en ciertos casos a la hora de calcular la distribución de pesos de un código.

Teorema 3.3. *Sea $\mathcal{C}$ un $[n,k,d]_q$-código de género a lo sumo g y $a = k+g-1$. Entonces los coeficientes B_i en la representación de $W_{\mathcal{C}}(x)$ dada por* (3.3) *satisfacen*

$$B_i = \tbinom{n}{i}(q^{a-i-g+1} - 1),$$

para $i \leq a - 2g + 1$ y las desigualdades

$$\max\left\{0, \tbinom{n}{i}(q^{a-i-g+1} - 1)\right\} \leq B_i \leq \tbinom{n}{i}(q^{a-i+1} - 1),$$

para $a - 2g + 2 \leq i \leq a$.

Demostración. En primer lugar, aplicaremos la identidad de MacWilliams al caso homogéneo y, luego, lo escribiremos a partir de la representación del polinomio enumerador de pesos dada en (3.3).

$$W_{\mathcal{C}^{\perp}}(x,y) = \tfrac{1}{q^k}\left\{(x + (q-1)y)^n + \sum_{i=0}^{a} B_i (qy)^i (x-y)^{n-i}\right\}. \tag{3.7}$$

Pasamos ahora a coordenadas no homogéneas. Para el código $\mathcal{C}^{\perp}$ tenemos que

$$W_{\mathcal{C}^{\perp}}(x) = x^n + \sum_{i=0}^{a^{\perp}} B_i^{\perp} (x-1)^i, \tag{3.8}$$

donde los $B_i^{\perp}$ son los números B_i en (3.3) cuando reemplazamos $\mathcal{C}$ por $\mathcal{C}^{\perp}$ y

$$a^{\perp} = n - k + g - 1.$$

A partir de (3.7) tomando $y = 1$ obtenemos que

$$x^n + \sum_{i=0}^{a^\perp} B_i^\perp (x-1)^i = q^{-k}\big\{(x+q-1)^n + \sum_{i=0}^{a} B_i q^i (x-1)^{n-i}\big\}.$$

Luego, expandiendo en potencias de $z = x - 1$ se tiene que

$$\sum_{i=0}^{a^\perp} \big(B_i^\perp + \tbinom{n}{i}\big) z^i + \sum_{i=a^\perp+1}^{n} \tbinom{n}{i} z^i = \sum_{i=0}^{n-a-1} \tbinom{n}{i} q^{n-k-i} z^i + \sum_{i=n-a}^{n} \big(B_{n-i} + \tbinom{n}{i}\big) q^{n-k-i} z^i.$$

De aquí podemos ver que, para $n - a \leq i \leq n$, se tiene

$$B_{n-i} = \begin{cases} \binom{n}{i}(q^{-n+k+i} - 1), & \text{si } i \geq a^\perp + 1, \\ \binom{n}{i}(q^{-n+k+i} - 1) + B_i^\perp q^{-n+k+i}, & \text{si } i \leq a^\perp. \end{cases}$$

Haciendo la sustitución $j = n - i$ y teniendo en cuenta que

$$k = a - g + 1,$$

$$a^\perp = n - k + g - 1 = n - a + 2g - 2.$$

se tiene que

$$B_j = \begin{cases} \binom{n}{j}(q^{a-j-g+1} - 1), & \text{si } j \leq a - 2g + 1, \\ \binom{n}{j}(q^{a-j-g+1} - 1) + B_{n-j}^\perp q^{a-j-g+1}, & \text{si } a - 2g + 2 \leq j. \end{cases}$$

Esto prueba la igualdad deseada y la desigualdad inferior. La desigualdad restante se puede calcular de manera similar. □

3.1.2 Espectro de códigos MDS

El teorema anterior permite conocer parcialmente la distribución de pesos de códigos lineales. Veamos que para los códigos MDS dicho teorema es suficiente. Como ya notamos, estos códigos tienen género a lo sumo cero, luego $g = 0$ y $a = k - 1$. Así, el polinomio enumerador de pesos está representado por

$$W_{\mathcal{C}}(x) = x^n + \sum_{i=0}^{k-1} B_i (x-1)^i.$$

Entonces, el Teorema 3.3 nos dice que

$$B_i = \tbinom{n}{i}(q^{k-i} - 1) \qquad \text{para} \quad i \leq k.$$

En este caso, tenemos todas igualdades, es decir, conocemos todos los números B_i. Tenemos entonces que

$$A_0 = 1, \qquad A_1 = A_2 = \cdots = A_{n-k} = 0,$$

$$A_i = \sum_{j=n-i}^{k-1} (-1)^{n+i+j} \tbinom{j}{n-i} B_j \qquad \text{para} \quad i \geq n - k + 1.$$

En conclusión, considerando un código MDS, a partir del Teorema 3.3, podemos encontrar su distribución de pesos completa. Veamos un ejemplo.

Ejemplo 3.4. Consideremos el $[8, 7, 2]_2$-código Reed-Muller $RM(2, 3)$. Notemos que

$$k + d = 7 + 2 = 9 = n + 1,$$

por lo tanto, este es un código de género a lo sumo cero. Luego, $a = k - 1 = 6$ y tenemos que

$$B_i = \tbinom{8}{i}(2^{7-i} - 1) \qquad \text{para} \quad i \leq 7.$$

Entonces, se tiene

$$\begin{aligned}
B_0 &= \tbinom{8}{0}(2^7 - 1) = 127,\\
B_1 &= \tbinom{8}{1}(2^6 - 1) = 504,\\
B_2 &= \tbinom{8}{2}(2^5 - 1) = 868,\\
B_3 &= \tbinom{8}{3}(2^4 - 1) = 840,\\
B_4 &= \tbinom{8}{4}(2^3 - 1) = 490,\\
B_5 &= \tbinom{8}{5}(2^2 - 1) = 168,\\
B_6 &= \tbinom{8}{6}(2^1 - 1) = 28,\\
B_7 &= \tbinom{8}{7}(2^0 - 1) = 0.
\end{aligned}$$

Luego, la distribución de pesos del código es

$$\begin{aligned}
A_0 &= 1,\\
A_1 &= 0,\\
A_2 &= B_6 = 28,\\
A_3 &= B_5 - 6B_6 = 0,\\
A_4 &= B_4 - 5B_5 + 15B_6 = 70,\\
A_5 &= B_3 - 4B_4 + 10B_5 - 20B_6 = 0,\\
A_6 &= B_2 - 3B_3 + 6B_4 - 10B_5 + 15B_6 = 28,\\
A_7 &= B_1 - 2B_2 + 3B_3 - 4B_4 + 5B_5 - 6B_6 = 0,\\
A_8 &= B_0 - B_1 + B_2 - B_3 + B_4 - B_5 + B_6 = 1.
\end{aligned}$$

Es decir, el espectro es simétrico y su enumerador de pesos queda

$$W_{RM(2,3)}(x) = x + 28x^2 + 70x^4 + 28x^6 + x^8.$$

Es directo chequear que la suma de los pesos $A_0 + \cdots + A_8 = 128$ es igual al número de palabras del código, como tiene que ser.

3.1.3 Espectro de códigos de Hamming

Sea $H_q(r)$ el $[n, n - r, 3]_q$-código de Hamming. Veamos qué nos dice el Teorema 3.3 en este caso. Encontremos primero el género. Tenemos que

$$n - r + 3 = k + d \geq n + 1 - g$$

y esto pasa si y sólo si,

$$g \geq r - 2.$$

Por lo tanto, el código $H_q(r)$ es de género a lo sumo $r-2$. Representamos al polinomio enumerador de pesos como en (3.3), con

$$a = k + g - 1 = n - 3.$$

Entonces, por el Teorema 3.3, tenemos que

$$B_i = \tbinom{n}{i}(q^{n-r-i} - 1)$$

para $i \leq a - 2g + 1 = n - 2r + 2$, y

$$\max\left\{0, \tbinom{n}{i}(q^{n-r-i} - 1)\right\} \leq B_i \leq \tbinom{n}{i}(q^{n-2-i})$$

para $n - 2r + 3 \leq i \leq n - 3$.

Conocemos exactamente los primeros $n - 2r + 3$ números B_i y tenemos cotas para los siguientes $2r - 5$ números B_i.

Luego, la distribución de pesos de $H_q(r)$ es

$$A_0 = 1, \quad A_1 = A_2 = 0,$$

$$A_i = \sum_{j=n-i}^{n-3} (-1)^{n+i+j} \tbinom{j}{n-i} B_j \qquad \text{para} \quad 3 \leq i \leq n.$$

Desconocemos el valor exacto de cada A_i, pero los tenemos escritos en términos de los $2r-5$ B_i's, para los que sólo tenemos una cota. En el caso binario, para encontrar el espectro de manera explícita puede ayudarnos el hecho de que la distribución de pesos de los códigos de Hamming binarios es simétrica, pues contiene a la palabra $\mathbf{1} = (1 \ldots 1)$ y esto es una condición suficiente, como se puede ver en [19]. En general, los códigos de Hamming q-arios con $q \neq 2$ no son simétricos. Esto se puede ver a partir del resultado en [24], que da los valores explícitos de A_i para $1 \leq i \leq 10$ para cualquier $H_q(r)$. Por ejemplo si $q = 3$ y $r = 3$, tenemos que $A_3 \neq A_{10}$.

Sin embargo, encontrar la distribución de pesos de este código es fácil. Conocemos el espectro del código simplex $H_q(r)^\perp$, que está dado por

$$A_0 = 1, \qquad A_{q^{r-1}} = q^r - 1,$$

y $A_i = 0$ para todos los demás índices i.

Entonces, por (2.4), se tiene que

$$A_i = \frac{1}{|H_q(r)^\perp|} \sum_{j=0}^{n} A_j^\perp K_i^{n,q}(j) = \tfrac{1}{q^r}\left\{K_i^{n,q}(0) + (q^r - 1)K_i^{n,q}(q^{r-1})\right\}.$$

Por la definición de los polinomios de Krawtchouk (otra forma de calcular estos polinomios es usando la recurrencia vista en el Teorema 2.18) concluimos que

$$A_i = \tfrac{1}{q^r}\left\{(q-1)^i \tbinom{n}{i} + (q^r - 1)\sum_{j=0}^{q^{r-1}} (-1)^j (q-1)^{i-j} \tbinom{q^{r-1}}{j} \tbinom{n-q^{r-1}}{i-j}\right\}.$$

obteniendo una fórmula cerrada para la distribución de pesos de códigos de Hamming q-arios.

3.2 Códigos cíclicos y ecuaciones diagonales

En esta sección damos la definición de una ecuación diagonal y algunos resultados que nos permiten encontrar el número N de soluciones de dicha ecuación, en algunos casos. Luego, vemos cuál es la relación entre el número N y la distribución de pesos de un código cíclico irreducible.

3.2.1 Ecuaciones diagonales sobre cuerpos finitos

Sea $\mathbb{F}_q$ con $q = p^r$ y p primo. Consideremos una ecuación polinomial del tipo

$$a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} = b, \tag{3.9}$$

donde $s \geq 2$, $d_1, \ldots, d_s$ son enteros positivos, $b \in \mathbb{F}_q$ y $a_1, \ldots, a_s \in \mathbb{F}_q^*$. Tal ecuación es llamada una *ecuación diagonal* sobre el cuerpo $\mathbb{F}_q$. El número N de soluciones de esta ecuación en $\mathbb{F}_q^s$ es el número de s-uplas $(\gamma_1, \ldots, \gamma_s) \in \mathbb{F}_q^s$ para las cuáles

$$a_1 \gamma_1^{d_1} + \cdots + a_s \gamma_s^{d_s} = b.$$

El siguiente teorema nos ayudará a encontrar el número de soluciones de la ecuación diagonal (3.9) en el caso particular en que $d_1 = \cdots = d_s = d$, es decir

$$a_1 x_1^d + \cdots + a_s x_s^d = b. \tag{3.10}$$

Para cada $a \in \mathbb{F}_q$, necesitaremos considerar el carácter aditivo de $\mathbb{F}_q$ definido por

$$\chi_a(x) = \omega_p^{\mathrm{Tr}(ax)}$$

donde $\omega_p = e^{\frac{2\pi i}{p}}$ es la raíz p-ésima de la unidad en $\mathbb{C}$.

Teorema 3.5. *El número N de soluciones de la ecuación* (3.10) *es*

$$N = q^{-1} \sum_{a \in \mathbb{F}_q} \chi_a(-b) \prod_{i=1}^{s} S_{aa_i},$$

donde

$$S_u = \sum_{x \in \mathbb{F}_q} \chi_u(x^d).$$

Demostración. Definimos

$$F(x_1, \ldots, x_s) = a_1 x_1^d + \cdots + a_s x_s^d - b,$$

y

$$S = \sum_{x=(x_1,\ldots,x_s) \in \mathbb{F}_q^s} \sum_{a \in \mathbb{F}_q} \chi_a(F(x_1, \ldots, x_s)).$$

Tenemos que

$$\sum_{a\in\mathbb{F}_q}\chi_a(F(x_1,\ldots,x_s)) = \begin{cases} q, & \text{si } F(x_1,\ldots,x_s)=0,\\ 0, & \text{caso contrario.}\end{cases}$$

Entonces, usando esto e intercambiando las sumas, se sigue que

$$qN = S = \sum_{a\in\mathbb{F}_q}\sum_{(x_1,\ldots,x_s)\in\mathbb{F}_q^s}\chi_a(F(x_1,\ldots,x_s)).$$

Como χ_a es un morfismo, la suma interior es igual al producto de $\chi_a(-b)$ por

$$\sum_{(x_1,\ldots,x_s)\in\mathbb{F}_q^s}\Big(\prod_{i=1}^{s}\chi_a(a_ix_i^d)\Big),$$

que es también igual a

$$\prod_{i=1}^{s}\Big(\sum_{a\in\mathbb{F}_q}\chi_a(a_ix^d)\Big).$$

De aquí, sale lo que queríamos. □

Corolario 3.6. *El número N de soluciones de la ecuación diagonal $x_1^d+\cdots+x_s^d=0$ está dado por*

$$N=\tfrac{1}{p^r}\sum_{a\in\mathbb{F}_q}(S_a)^s \qquad \textit{donde} \qquad S_a=\sum_{x\in\mathbb{F}_q}\omega_p^{\mathrm{Tr}(ax^d)}.$$

Notemos que $S_a = g(\alpha,d)$ en el caso que $k\equiv 1 \pmod d$, donde $g(\alpha,d)$ es el período de Gauss.

3.2.2 Número de soluciones y espectro de códigos cíclicos

Sea $m(x)$ un divisor mónico irreducible de x^n-1 sobre $\mathbb{F}_p$. Entonces, $(m(x))$ es un ideal maximal, y el código cíclico generado por $\frac{x^n-1}{m(x)}$ es llamado, como vimos, un código cíclico irreducible. Tenemos que $m(x)=m_\alpha(x)$, el polinomio minimal de α sobre $\mathbb{F}_p$, donde α es una raíz primitiva n-ésima de la unidad. Denotamos a este código por $\mathcal{C}(\alpha)$.

Sea L el cuerpo de descomposición de x^n-1 sobre $\mathbb{F}_p$. Sabemos que $\mathcal{C}(\alpha)$ es la imagen de L por el mapa inyectivo $\mu: L\to\mathbb{F}_p^n$ definido por

$$\mu(c)=\big(\mathrm{Tr}(c),\mathrm{Tr}(c\alpha),\ldots,\mathrm{Tr}(c\alpha^{n-1})\big)=\sum_{i=0}^{n-1}\mathrm{Tr}(c\alpha^i)\,x^i.$$

Es decir, $L=\mathbb{F}_{p^e}$ con $e=\mathrm{gr}\ m_\alpha(x)$ y

$$\mathcal{C}(\alpha)=\big\{\big(\mathrm{Tr}_{p^e/p}(c\alpha^i)\big)_{i=0}^{n-1} : c\in\mathbb{F}_{p^d}\big\}.$$

Proposición 3.7. *Sea $a \in \mathbb{F}_q$, $q = p^r$ y supongamos $p^r - 1 = nd$ y $p - 1 \mid n$. Entonces, la suma S_a del Corolario 3.6 está dada por*

$$S_a = p^r - \frac{dp}{p-1}\, w(\mu(c)), \tag{3.11}$$

donde $c = \mathrm{Tr}(a)$ y $w(\mu(c))$ es el peso de la palabra $\mu(c)$ en el código $\mathcal{C}(\alpha)$.

Demostración. Consideremos la ecuación

$$\mathrm{Tr}(ax^d) = \lambda, \tag{3.12}$$

con $\lambda \in \mathbb{F}_p$ y sea N_λ el número de soluciones $x \in \mathbb{F}_q$ de (3.12). Si $\lambda \neq 0$, entonces la ecuación es equivalente a

$$\mathrm{Tr}(\lambda^{-1} a x^d) = 1.$$

Como $p - 1 \mid n$ se sigue que $\mathbb{F}_p^*$ está contenido en el subgrupo multiplicativo G de orden n de $\mathbb{F}_q^*$. Entonces, existe algún x_λ en $\mathbb{F}_q^*$ tal que $\lambda^{-1} = x_\lambda^d$. Si definimos $y = x_\lambda x$, entonces, la ecuación (3.12) se convierte en

$$\mathrm{Tr}(ay^d) = 1.$$

Por lo tanto, $N_\lambda = N_1$ para $\lambda \neq 0$. Esto es

$$S_a = \sum_{\lambda \in \mathbb{F}_p} N_\lambda\, w_p^\lambda = N_0 + N_1 \sum_{\lambda \neq 0} w_p^\lambda = N_0 + N_1\big(-1 + \sum_{\lambda=0}^{p-1} \omega_p^\lambda\big).$$

Como $\sum_{\lambda=0}^{p-1} \omega_p^\lambda = 0$, tenemos que

$$S_a = N_0 - N_1. \tag{3.13}$$

Por otro lado, se tiene que

$$\mathrm{Tr}_{q/p}(a\alpha^i) = \mathrm{Tr}_{L/\mathbb{F}_p}\left(\mathrm{Tr}_{\mathbb{F}_q/L}(a\alpha^i)\right) = \mathrm{Tr}_{L/\mathbb{F}_p}\left(\alpha^i \mathrm{Tr}_{\mathbb{F}_q/L}(a)\right) = \mathrm{Tr}_{L/\mathbb{F}_p}(c\alpha^i).$$

Entonces,

$$n - w(\mu(c)) = \#\{0 \leq i \leq n-1 \,:\, \mathrm{Tr}_{q/p}(a\alpha^i) = 0\}.$$

Como $nd = p^r - 1$, la ecuación $x^d = \alpha^i$ tiene exactamente d soluciones en $\mathbb{F}_q^*$. Entonces

$$N_0 = 1 + d\{n - w(\mu(c))\}. \tag{3.14}$$

Además,

$$|\mathbb{F}_q| = \sum_{\lambda \in \mathbb{F}_p} N_\lambda,$$

lo que significa que

$$p^r = N_0 + (p-1)N_1. \tag{3.15}$$

Luego, de (3.13), (3.14) y (3.15) se obtiene (3.11), como queríamos. □

El siguiente resultado relaciona las soluciones de ecuaciones diagonales con el espectro de ciertos códigos cíclicos asociados.

Teorema 3.8 (Wolfmann)**.** *Sea $a \in \mathbb{F}_q$, $q = p^r$ y supongamos $p^r - 1 = nd$ y $p-1 \mid n$. Sean $A_0, \ldots, A_n$ la distribución de pesos del código asociado $\mathcal{C}(\alpha)$ y N el número de soluciones $(x_1, \ldots, x_s)$ de $x_1^d + \cdots + x_s^d = 0$ en $\mathbb{F}_q^s$. Entonces*

$$N = \frac{p^{s-\nu}}{(p-1)^s} \sum_{i=0}^{n} A_i \left\{(p-1)p^{r-1} - di\right\}^s, \tag{3.16}$$

donde ν es el orden multiplicativo de p módulo n.

Demostración. Por el corolario 3.6 y la proposición 3.7, N está dado por

$$N = \frac{p^{s-r}}{(p-1)^s} \sum_{a \in \mathbb{F}_q} \left((p-1)p^{r-1} - dw(\mu(\mathrm{Tr}(a)))\right)^s.$$

El orden multiplicativo ν de p módulo n es un divisor de r, y el cuerpo de descomposición L de $x^n - 1$ sobre $\mathbb{F}_p$ es $\mathbb{F}_{p^\nu}$.

Para cualquier $c \in L$, el número de elementos $a \in \mathbb{F}_q$ tal que $c = \mathrm{Tr}(a)$ es

$$(p^\nu)^{\frac{r}{\nu}-1} = p^{r-\nu}.$$

Entonces tenemos

$$\sum_{a \in \mathbb{F}_q} \left((p-1)p^{r-1} - dw(\mu(\mathrm{Tr}(a)))\right)^s = p^{r-\nu} \sum_{c \in L} \left((p-1)p^{r-1} - dw(\mu(c))\right)^s.$$

Luego,

$$N = \frac{p^{s-\nu}}{(p-1)^s} \sum_{c \in L} \left((p-1)p^{r-1} - dw(\mu(c))\right)^s.$$

El mapa μ es inyectivo y así el número de elementos $c \in L$ tal que $w(\mu(c)) = i$ es el número A_i de palabras código en $\mathcal{C}(\alpha)$ de peso i. Esto nos da la fórmula para N que queríamos. □

El teorema nos dice que, bajo la condición de que d divide a $\frac{p^r-1}{p-1}$, podemos calcular el número de soluciones de $x_1^d + \cdots + x_s^d = 0$ si conocemos la distribución de pesos del código cíclico irreducible asociado.

Ejemplo 3.9. Sean $p = 2$, $d = 7$, $r = 6$ y $n = 9$. El número N de soluciones de

$$x_1^7 + \cdots + x_s^7 = 0$$

sobre $\mathbb{F}_{2^6}$ está dado por

$$N = 2^{2s-6}(16^s + 9^{s+1} + 27 \cdot 2^s + 27 \cdot (-5)^s).$$

Veamos una demostración de esto.

Primero notemos que la descomposición de $x^9 - 1$ en factores irreducibles es

$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

donde hemos usado propiedades de los polinomios ciclotómicos. En efecto, $x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)$ y $\Phi_9(x) = \Phi_3(x^3)$. Es fácil chequear que estos polinomios son irreducibles sobre $\mathbb{F}_2$.

Luego, $x^6 + x^3 + 1$ es el polinomio minimal de α sobre $\mathbb{F}_2$, donde α es una raíz novena de la unidad sobre $\mathbb{F}_2$. Entonces, el generador de $\mathcal{C}(\alpha)$ está dado por

$$g(x) = \frac{(x^9 - 1)}{(x^3 - 1)} = x^6 + x^3 + 1.$$

Luego la matriz generadora de $\mathcal{C}(\alpha)$ es

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Las palabras código de $\mathcal{C}(\alpha)$ son combinaciones lineales sobre $\mathbb{F}_2$ de las filas de G. Luego, la distribución de pesos de $\mathcal{C}(\alpha)$ está dada por

$$A_0 = 1, \qquad A_1 = 0, \qquad A_2 = 9, \qquad A_3 = 0, \qquad A_4 = 27,$$
$$A_5 = 0, \qquad A_6 = 27, \qquad A_7 = A_8 = A_9 = 0.$$

Luego, tenemos que

$$\begin{aligned} N &= 2^{s-6}\{2^{5s} + 9(2^5 - 14)^s + 27(2^5 - 28)^s + 27(2^5 - 42)^s\} \\ &= 2^{2s-6}\{2^{4s} + 9^{s+1} + 27 \cdot 2^s + 27 \cdot (-5)^s\}, \end{aligned}$$

que es lo queríamos ver.

Por ejemplo, veamos que pasa en los casos mas chicos $s = 2, 3$. La ecuación

$$x_1^7 + x_2^7 = 0$$

tiene

$$N = 2^{-2}\{2^8 + 9^3 + 27 \cdot 2^2 + 27 \cdot (-5)^2\} = 442$$

soluciones mientras que la ecuación

$$x_1^7 + x_2^7 + x_3^7 = 0$$

tiene exactamente

$$N = 2^0\{2^{12} + 9^4 + 27 \cdot 2^3 + 27 \cdot (-5)^3\} = 7498$$

soluciones.

Capítulo 4

Distribución de pesos de códigos cíclicos

Aquí consideramos códigos cíclicos y planteamos una estrategia muy útil para encontrar su distribución de pesos utilizando el Teorema de Desarte y la Identidad de MacWilliams. El resto del trabajo se basa en usar esta estrategia para distintos códigos, aunque nos concentraremos principalmente en los códigos de Melas y los códigos relacionados de Zetterberg.

Sea C un código cíclico de longitud n sobre $\mathbb{F}_p$ con p primo. Consideramos $\mathcal{C}$ el código cíclico en $\mathbb{F}_{q=p^r}$ tal que $\mathrm{Res}(\mathcal{C}) = C$, donde $\mathrm{Res}(\mathcal{C}) = \mathcal{C} \cap \mathbb{F}_p^n$ es la restricción de $\mathcal{C}$ sobre $\mathbb{F}_p$. Luego, por el Teorema de Delsarte, se tiene que

$$\mathrm{Res}(\mathcal{C})^\perp = \mathrm{Tr}(\mathcal{C}^\perp).$$

Es decir, tenemos el siguiente diagrama

$$\begin{array}{ccc} \overline{\mathcal{C}} & \overset{\text{dual}}{\longleftrightarrow} & \overline{\mathcal{C}}^\perp \\ \mathrm{Res}\downarrow & & \downarrow \mathrm{Tr} \\ C & \overset{\text{dual}}{\longleftrightarrow} & C^\perp \end{array}$$

Para conocer la distribución de pesos de $C^\perp$, pensamos entonces en este código como un código traza. Sea

$$v = (v_1, \ldots, v_n) = (\mathrm{Tr}(v_1), \ldots, \mathrm{Tr}(v_n)) \in C^\perp$$

una palabra en el código dual. Para conocer su peso es suficiente entonces conocer el número $\#\{1 \leq i \leq n : \mathrm{Tr}(v_i) \neq 0\}$. Equivalentemente, tenemos

$$w(c) = n - \#\{1 \leq i \leq n \, : \, \mathrm{Tr}(v_i) = 0\}. \tag{4.1}$$

El número $\#\{1 \leq i \leq n : \mathrm{Tr}(v_i) = 0\}$ está naturalmente asociado a ciertas sumas exponenciales o a la cantidad de puntos racionales de curvas algebraicas.

Por Teorema 1.6 sabemos que $\mathrm{Tr}(f(x)) = 0$ si y sólo si existe un $y \in \mathbb{F}_{q^m}$ tal que $y^q - y = f(x)$. Entonces, el peso $w(c)$ está estrictamente relacionado con el número de puntos racionales de la curva de Artin-Schreier

$$Y^q - Y = f(X). \tag{4.2}$$

Por otro lado, si $\omega_q = e^{\frac{2\pi i}{q}}$ tenemos que

$$\sum_{s\in\mathbb{F}_q} \omega_q^{s\mathrm{Tr}(f(x))} = \begin{cases} q, & \text{si } \mathrm{Tr}(f(x)) = 0, \\ 0, & \text{si } \mathrm{Tr}(f(x)) \neq 0. \end{cases} \tag{4.3}$$

Luego, de (4.1) y (4.3) obtenemos que

$$w(c) = n - \tfrac{1}{q}\Big(q^m - 1 + \sum_{s\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}^*} \omega_q^{\mathrm{Tr}(sf(x))}\Big),$$

donde la suma interior es una suma exponencial, que según como sea $f(x)$ tomará eventualmente la forma de alguna suma conocida como las sumas de Gauss, de Kloosterman o de Weil.

Una vez que tenemos la distribución de pesos del código dual, usamos la Identidad de MacWilliams para obtener la distribución de pesos del código $\mathcal{C}$. Recordemos que si el código $\mathcal{C}$ es un código cíclico irreducible, entonces puede ser visto como un código traza y podemos trabajar directamente con las curvas algebraicas o las sumas exponenciales.

Usaremos esta estrategia para encontrar la distribución de pesos de los códigos cíclicos clásicos de Hamming y BCH en este capítulo, y los menos conocidos Melas y Zetterberg en los capítulos siguientes.

4.1 Códigos de Hamming

Si bien el espectro de estos códigos lo hemos calculado de forma tradicional en el capítulo anterior, veamos aquí cómo se aplica la estrategia general mencionada al comienzo del capítulo al caso de códigos de Hamming cíclicos.

Sean p un número primo, $m \geq 2$ y $q = p^m$. Comenzamos recordando dos resultados clásicos sobre ciclicidad de los códigos de Hamming (ver por ejemplo Sección 7.4 en [37]):

- Todo código de Hamming binario $H_2(m)$ es equivalente a un código cíclico (o sea es cíclico salvo permutación de coordenadas).
- Si $(m, q-1) = 1$ entonces el código de Hamming q-ario $H_p(m)$ es equivalente a un código cíclico.

Consideremos códigos de Hamming $H_p(m)$ cíclicos (o sea m coprimo con $p-1$ si p es impar y con las coordenadas ya correctamente ordenadas). El código $H_p(m)$ de longitud $q-1$ es el ideal generado por $m_\alpha(T)$ en $\frac{\mathbb{F}_p[T]}{\langle T^{q-1}-1\rangle}$, donde $m_\alpha(T)$ es el polinomio minimal de α, donde α es un generador de $\mathbb{F}_q^*$.

Notemos que la dimensión de $H_p(m)$ es $q-1-m$ y la distancia mínima es 3, como ya habíamos mencionado.

Podemos relacionar la distribución de pesos de este $H_p(m)$ tanto con una curva algebraica como con ciertas sumas de Gauss. Primero, vemos a $H_p(m)$ como la restricción a $\frac{\mathbb{F}_p[T]}{\langle T^{q-1}-1\rangle}$ del código $\mathcal{H}_p(m)$ definido por el ideal

$$(T-\alpha)$$

en $\frac{\mathbb{F}_q[T]}{\langle T^{q-1}-1\rangle}$.

Los polinomios en $\mathcal{H}_p(m)$ son los vectores $(a_0, a_1, \ldots, a_{q-2})$ que son ortogonales a los vectores $(1, \alpha, \alpha^2, \ldots, \alpha^{q-2})$. Como α genera $\mathbb{F}_q^*$, el último vector tiene precisamente todos los elementos $x \in \mathbb{F}_q^*$ como sus coordenadas. Entonces, el dual de $\mathcal{H}_p(m)$ en $\mathbb{F}_q$ está dado por

$$\mathcal{H}_p(m)^\perp = \{(\lambda x)_{x\in\mathbb{F}_q^*} \,:\, \lambda \in \mathbb{F}_q\}.$$

Luego, por el Teorema de Delsarte, tenemos que

$$\begin{array}{ccc} \mathcal{H}_p(m) & \overset{\text{dual}}{\longleftrightarrow} & \mathcal{H}_p(m)^\perp \\ \text{Res}\downarrow & & \downarrow \text{Tr} \\ H_p(m) & \overset{\text{dual}}{\longleftrightarrow} & H_p(m)^\perp \end{array}$$

Por lo tanto,

$$H_p(m)^\perp = \{\text{Tr}(\lambda x)_{x\in\mathbb{F}_q^*} \,:\, \lambda \in \mathbb{F}_q\}.$$

Si tenemos una palabra $v \in H_p(m)^\perp$, entonces

$$\begin{aligned} w(v) = \#\{i \,:\, v_i \neq 0\} &= q-1-\#\{i \,:\, v_i = 0\} \\ &= q-1-\#\{x \in \mathbb{F}_q^* \,:\, \text{Tr}(\lambda x) = 0\}. \end{aligned}$$

Veamos todo esto en un ejemplo simple. Consideremos el código binario $H_2(3)$, dado por el ideal generado por el polinomio $f(x) = x^3 + x + 1$, que es irreducible en $\mathbb{F}_2$. Buscamos un código $\mathcal{H}_2(3)$ en $\mathbb{F}_8$ tal que $\text{Res}(\mathcal{H}_2(3)) = H_2(3)$. Observemos que $f(x)$ no es irreducible en $\mathbb{F}_8$, y tenemos que

$$x^3 + x + 1 = (x-\alpha)(x-\alpha^2)(x-\alpha^4),$$

con α una raíz séptima de la unidad de $\mathbb{F}_8^*$.

Entonces, el código $\mathcal{H}_2(3)$ dado por el ideal generado por $x-\alpha$ es tal que $\text{Res}(\mathcal{H}_2(3)) = H_2(3)$, y se tiene que

$$\begin{array}{ccc} \mathcal{H}_2(3) & \overset{\text{dual}}{\longleftrightarrow} & \mathcal{H}_2(3)^\perp \\ \text{Res}\downarrow & & \downarrow \text{Tr} \\ H_2(3) & \overset{\text{dual}}{\longleftrightarrow} & H_2(3)^\perp \end{array}$$

A continuación calcularemos el espectro de $H_2(m)$ siguiendo dos caminos diferentes. Primero, a partir de curvas algebraicas y, luego, utilizando sumas exponenciales.

Por curvas

El Teorema 1.6 nos dice que

$$\mathrm{Tr}(\lambda x) = 0$$

si y sólo si existe $y \in \mathbb{F}_q$ tal que

$$y^p - y = \lambda x,$$

entonces, el peso de una palabra $v \in H_p(m)^\perp$ está relacionado con la cantidad de puntos racionales de la curva

$$E_\lambda : \qquad Y^p - Y = \lambda X.$$

No siempre es fácil encontrar los puntos racionales de esta curva.

Por sumas exponenciales

Sea $\omega_p = e^{\frac{2\pi i}{p}}$. Notemos que si $f(x) = \lambda x$, entonces

$$\sum_{s\in\mathbb{F}_p} \omega_p^{s\mathrm{Tr}(f(x))} = \begin{cases} p, & \text{si} \quad \mathrm{Tr}(f(x)) = 0, \\ 0, & \text{si} \quad \mathrm{Tr}(f(x)) \neq 0. \end{cases}$$

Además, se tiene que

$$\begin{aligned} \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(f(x)) = 0\} &= \sum_{x\in\mathbb{F}_q^*} \tfrac{1}{p} \sum_{s\in\mathbb{F}_p} \omega_p^{s\mathrm{Tr}(f(x))} \\ &= \tfrac{1}{p} \sum_{s\in\mathbb{F}_p} \sum_{x\in\mathbb{F}_q^*} \omega_p^{s\mathrm{Tr}(f(x))} \\ &= \tfrac{1}{p}\Big(q - 1 + \sum_{s\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q^*} \omega_p^{\mathrm{Tr}(sf(x))}\Big). \end{aligned}$$

Luego, para $v \in H_p(m)^\perp$,

$$\begin{aligned} w(v) &= q - 1 - \#\{x \in \mathbb{F}_p^* \,:\, \mathrm{Tr}(f(x)) = 0\} \\ &= \tfrac{1}{p}\big((q-1)(p-1) - \sum_{s\in\mathbb{F}_p^*} g(s\lambda; 1)\big), \end{aligned}$$

donde $g(s\lambda; 1)$ es el período de Gauss dado en (1.15).

Consideremos ahora el caso binario, tenemos el código $H_2(m)$. Vimos, entonces, que para $v \in H_2(m)^\perp$,

$$w(v) = \tfrac{1}{2}\big(q - 1 - \sum_{s\in\mathbb{F}_2^*} g(s\lambda; 1)\big) = \tfrac{1}{2}\big(q - 1 - g(\lambda; 1)\big),$$

donde

$$g(\lambda; 1) = \sum_{x\in\mathbb{F}_q} (-1)^{\mathrm{Tr}(\lambda x)}.$$

Conociendo esta suma, podríamos conocer la distribución de pesos del código $H_2(m)$.

4.2 Códigos BCH

Sean p un número primo, $m \geq 2$ y $q = p^m$. El código cíclico $BCH_p(m)$ de longitud $q-1$ es el ideal generado por

$$m_\alpha(T)\, m_{\alpha^3}(T)$$

en $\mathbb{F}_p[T]/\langle T^{q-1}-1\rangle$, donde $m_{\alpha^i}(T)$ es el polinomio minimal de α^i para $i = 1, 3$ y α es un generador de $\mathbb{F}_q^*$. De ahora en más, denotaremos a este código por $B_p(m)$.

Vemos al código $B_p(m)$ como la restricción del código $\mathcal{B}_p(m)$ dado por el ideal generado por

$$(T-\alpha)(T-\alpha^3)$$

en $\mathbb{F}_q[T]/\langle T^{q-1}-1\rangle$. Luego, por el Teorema de Delsarte, tenemos:

$$\begin{array}{ccc} \mathcal{B}_p(m) & \overset{\text{dual}}{\longleftrightarrow} & \mathcal{B}_p(m)^\perp \\ \text{Res}\downarrow & & \downarrow \text{Tr} \\ B_p(m) & \overset{\text{dual}}{\longleftrightarrow} & B_p(m)^\perp \end{array}$$

Los polinomios en $\mathcal{B}_p(m)$ son precisamente aquellos que se anulan en α y α^3, por lo tanto, tenemos que

$$\mathcal{B}_p(m)^\perp = \{(\lambda x + \mu x^3)_{x\in\mathbb{F}_q^*} \,:\, \lambda, \mu \in \mathbb{F}_q\}.$$

Entonces,

$$B_p(m)^\perp = \{(\text{Tr}(\lambda x + \mu x^3))_{x\in\mathbb{F}_q^*} \,:\, \lambda, \mu \in \mathbb{F}_q\}.$$

A partir de esto, podemos seguir de dos maneras diferentes: usando curvas elípticas o usando sumas exponenciales. Veremos los casos p impar y par por separado.

4.2.1 Caso general

Por sumas exponenciales

Si tenemos una palabra $v = (v_1, \ldots, v_n) \in B_p(m)^\perp$, entonces

$$w(v) = \#\{1 \leq i \leq n \,:\, v_i \neq 0\} = q - 1 - \#\{x \in \mathbb{F}_q \,:\, \text{Tr}(f(x)) = 0\}$$

donde

$$f(x) = \lambda x + \mu x^3.$$

Además, notemos que si $\omega_p = e^{\frac{2\pi i}{p}}$, entonces se tiene

$$\sum_{s\in\mathbb{F}_p} \omega_p^{s\text{Tr}(f(x))} = \begin{cases} p, & \text{si Tr}(f(x)) = 0, \\ 0, & \text{si Tr}(f(x)) \neq 0. \end{cases}$$

Por lo tanto,

$$\begin{aligned} w(v) &= q-1-\sum_{x\in\mathbb{F}_q^*}\tfrac{1}{p}\sum_{s\in\mathbb{F}_p}\omega_p^{s\mathrm{Tr}(f(x))} \\ &= q-1-\tfrac{1}{p}\sum_{s\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_q^*}\omega_p^{s\mathrm{Tr}(f(x))} \\ &= q-1-\tfrac{1}{p}\Big(q-1-\sum_{s\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q^*}\omega_p^{\mathrm{Tr}(sf(x))}\Big) \\ &= \tfrac{1}{p}\big\{(q-1)(p-1)-\sum_{s\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q^*}\omega_p^{\mathrm{Tr}(sf(x))}\big\}. \end{aligned}$$

Es decir,

$$w(v)=\tfrac{1}{p}\big\{(q-1)(p-1)-\sum_{s\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q^*}\omega_p^{\mathrm{Tr}(s(\mu x+\lambda x^3)}\big\}.$$

En el caso binario, las sumas interiores resultarán ser sumas de Weil y podremos resolverlas.

Por curvas elípticas

Sea

$$v_{\lambda,\mu}=(\mathrm{Tr}(\lambda x+\mu x^3))_{x\in\mathbb{F}_q^*}$$

una palabra en $B_p(m)^\perp$. Su peso está relacionado directamente con el número de puntos racionales de la curva

$$E_{\lambda,\mu}: \qquad Y^p-Y=\lambda X+\mu X^3.$$

Para $x\in\mathbb{F}_q$ se tiene que

$$\mathrm{Tr}(\lambda x+\mu x^3)=0 \quad\Longleftrightarrow\quad \text{existe } y\in\mathbb{F}_q: \quad y^p-y=\lambda x+\mu x^3.$$

Entonces, excepto para los puntos $(0,0)$, $(0,1)$ y el punto en el infinito, el peso de $v_{\lambda,\mu}$ es

$$w(v_{\lambda,\mu})=(q-1)-\tfrac{1}{2}(\#E_{\lambda,\mu}(\mathbb{F}_q)-3).$$

Habría que determinar el número de puntos racionales de la curva $E_{\lambda,\mu}$ para determinar los pesos, y cuántas veces se repiten para dar la distribución completa.

4.2.2 Caso binario

Consideramos ahora $p=2$ y $q=2^m$. De ahora en más, denotaremos al código $B_2(m)$ por B_m. Notemos que B_m tiene dimensión mayor o igual a $q-1-2m$ y distancia mínima $d=5$.

Por sumas exponenciales (de Weil)

Por lo visto en el caso general, se tiene que para $v \in B_2(m)^\perp$ el peso está dado por

$$w(v) = \tfrac{1}{2}\big\{q - 1 - \sum_{x\in\mathbb{F}_q^*} \omega_2^{\mathrm{Tr}(\lambda x+\mu x^3)}\big\} \ = \tfrac{1}{2}\big\{q - \sum_{x\in\mathbb{F}_q} (-1)^{\mathrm{Tr}(\lambda x+\mu x^3)}\big\}.$$

Como $3 = 2^1 + 1$, podemos usar sumas de Weil. En efecto,

$$w(v) = \tfrac{1}{2}\{q - S_1(\mu,\lambda)\}. \tag{4.4}$$

donde $S_1(\mu,\lambda)$ es la suma de Weil definida en (1.9), con $p = 2$ y $\alpha = 1$.

Conocemos el valor de estas sumas. En este caso $d = (1, m) = 1$. Luego, tenemos dos casos dependiendo si m es par o no.

• Veamos primero qué pasa cuando m es impar. Por el Teorema 1.21, cuando $\lambda = 0$, se tiene que $S_1(0,0) = q$ y $S_1(\mu,0) = 0$ para todo $\mu \neq 0$. Si $\mu = 0$ y $\lambda \neq 0$ tenemos que

$$S_1(0,\lambda) = g(\lambda,1),$$

donde $g(\lambda,1)$ es el período de Gauss dado en (1.15). Por otro lado, si $\lambda \neq 0$, el Teorema 1.22 dice que

$$S_1(\mu,\lambda) = S_1(1,\lambda c^{-1}),$$

con c el único elemento en $\mathbb{F}_q^*$ tal que $c^3 = \mu$. Además,

$$S_1(1,\lambda) = \begin{cases} 0, & \text{si } \mathrm{Tr}(\lambda) = 0, \\ \pm 2^{\frac{m+1}{2}}, & \text{si } \mathrm{Tr}(\lambda) = 1. \end{cases}$$

Nos falta conocer el signo de $S_1(1,\lambda)$ en el caso en que $\mathrm{Tr}(\lambda) \neq 0$. Para eso, por el Teorema 1.23 tenemos que

$$S_1(1,\lambda) = \chi_1(b^3+b)\, S_1(1,1),$$

donde $b^4 + b + 1 = \lambda$ y, por el Teorema 1.24,

$$S_1(1,1) = (\tfrac{2}{m})\, 2^{\frac{m+3}{2}},$$

y se sabe que $(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$.

Luego, para $v \in B_2(m)^\perp$ se tiene

$$\begin{aligned} w(v) &= \tfrac{1}{2}\{q - S_1(\mu,\lambda)\} = \tfrac{1}{2}\{q - S_1(1,\lambda c^{-1})\} \\ &= \tfrac{1}{2}\big\{q - \tfrac{1}{m}\,\chi_1(b^3+b)\, 2^{\frac{m+3}{2}}\big\}, \end{aligned}$$

donde $b^4 + b + 1 = \lambda c^{-1}$ y $c^3 = \lambda$.

• Nos interesa ahora el caso m par. Por ser par, m se puede escribir de la forma $m = 2r$ para algún r. Sea β un elemento primitivo de $\mathbb{F}_q$. Cuando $\lambda = 0$, por Teorema 1.25, se tiene que

$$S_1(\mu, 0) = \begin{cases} (-1)^r 2^r, & \text{si } \mu \neq \beta^{3t} \text{ para cualquier } t \in \mathbb{Z}, \\ -(-1)^r 2^{r+1}, & \text{si } \mu = \beta^{3t} \text{ para algún } t \in \mathbb{Z}. \end{cases}$$

Y en el caso $\lambda \neq 0$, el Teorema 1.26 nos dice que

$$S_1(\mu, \lambda) = \begin{cases} (-1)^r 2^r \chi_1(\mu x_0^3), & \text{si } \mu \neq \beta^{3t} \text{ para algún entero } t, \\ -(-1)^r 2^{r+1} \chi_1(\mu x_0^3), & \text{si } \mu = \beta^{3t} \text{ y } \mathrm{Tr}(\mu) = 0, \\ (-1)^r 2^r \chi_1(\mu x_0^3), & \text{si } \mu = \beta^{3t} \text{ y } \mathrm{Tr} \neq 0. \end{cases}$$

Aquí, x_0 es tal que $\mu^3 x_0^4 + \mu x_0 = \lambda^2$.

Por lo tanto, para $v \in B_2(m)^\perp$ tenemos

$$w(v) = \tfrac{1}{2}\{q - S_1(\mu, \lambda)\}$$

de donde

$$w(v) = \begin{cases} \frac{1}{2}\{q - (-1)^r 2^r\}, & \text{si } \lambda = 0,\ \mu \neq \beta^{3t} \text{ para todo } t \in \mathbb{Z}, \\ \frac{1}{2}\{q + (-1)^r 2^r\}, & \text{si } \lambda = 0,\ \mu = \beta^{3t} \text{ para algún } t \in \mathbb{Z}, \\ \frac{1}{2}\{q - (-1)^r 2^r \chi_1(\mu x_0^3))\}, & \text{si } \lambda \neq 0,\ \mu \neq \beta^{3t} \text{ para todo } t \in \mathbb{Z}, \\ \frac{1}{2}\{q - (-1)^r 2^r \chi_1(\mu x_0^3))\}, & \text{si } \lambda \neq 0, \mu = \beta^{3t} \text{ para algún } t \in \mathbb{Z} \text{ y } \mathrm{Tr}(\mu) \neq 0, \\ \frac{1}{2}\{q + (-1)^r 2^{r+1} \chi_1(\mu x_0^3)\}, & \text{si } \lambda \neq 0,\ \mu = \beta^{3t} \text{ para algún } t \in \mathbb{Z} \text{ y } \mathrm{Tr}(\mu) = 0. \end{cases}$$

Entonces, para cada palabra en el código dual, conocemos su peso.

Observemos que con un estudio más detallado de estas sumas podríamos obtener las distribuciones de peso, calculando la frecuencia con la que aparece cada uno de los pesos distintos que obtuvimos.

Por curvas elípticas

Como vimos, el peso de las palabras en $B_m^\perp$ está directamente relacionado con el número de puntos racionales de la curva

$$E_{\lambda,\mu}: \qquad Y^2 - Y = \lambda X + \mu X^3.$$

Si $v_{\lambda,\mu} \in B_m^\perp$, excepto para los puntos $(0,0)$, $(0,1)$ y el punto en el infinito, se tiene que:

$$w(v_{\lambda,\mu}) = (q-1) - \tfrac{1}{2}(\#E(\mathbb{F}_q) - 3).$$

Para $\lambda = \mu = 0$ obtenemos la palabra cero. Si $\mu = 0$ y $\lambda \neq 0$, la curva $E_{\lambda,\mu}$ es una cónica y se sabe que éstas tienen $q+1$ puntos racionales (se puede ver en [40], pág. 109), lo que da lugar a $q-1$ palabras de peso

$$q - 1 - \tfrac{1}{2}(q + 1 - 3) = \tfrac{q}{2}.$$

Cuando $\mu \neq 0$, la curva $E_{\lambda,\mu}$ tiene género 1, es una curva elíptica supersingular ya que $j(E_{\lambda,\mu}) = 0$. Además, si observamos la definición de curva elíptica supersingular en la Sección 1.2.2, como conocemos los pesos de las palabras del código y, por lo tanto, sabemos el valor de $\#E(\mathbb{F}_q)$ entonces podemos observar que $2 \mid t$ si $\#E(\mathbb{F}_q) = q+1-t$. Esto significa que no tiene puntos de orden 2 o, equivalentemente, que su anillo de $\overline{\mathbb{F}}_2$-endomorfismos no es conmutativo. Hay, salvo isomorfismos, solo una curva elíptica supersingular sobre $\overline{\mathbb{F}_2}$. Tiene ecuación

$$Y^2 + Y = X^3.$$

Sobre $\mathbb{F}_q$ hay más clases de isomorfismos.

Proposición 4.1. *Sea $\mathbb{F}_q$ una extensión de $\mathbb{F}_2$ de grado m. Si m es impar, hay, salvo isomorfismos, exactamente 3 curvas elípticas supersingulares sobre $\mathbb{F}_q$. Si m es par, hay, salvo isomorfismos, exactamente 7 curvas elípticas supersingulares sobre $\mathbb{F}_q$. En las siguientes tablas se ordenan según el número de puntos sobre $\mathbb{F}_q$. También damos la cardinalidad de sus grupos de automorfismos $\mathbb{F}_q$-racionales.*

Table 4.1: Clases de isomorfismo de curvas elípticas supersingulares, m impar

$\#E(\mathbb{F}_q)$	Frecuencia	$\#Aut_{\mathbb{F}_q}(E)$
$q+1-\sqrt{2q}$	1	4
$q+1$	1	2
$q+1+\sqrt{2q}$	1	4

Table 4.2: Clases de isomorfismo de curvas elípticas supersingulares, m par

$\#E(\mathbb{F}_q)$	Frecuencia	$\#Aut_{\mathbb{F}_q}(E)$
$q+1-\sqrt{2q}$	1	24
$q+1-\sqrt{q}$	2	6
$q+1$	1	4
$q+1+\sqrt{q}$	2	6
$q+1+\sqrt{2q}$	1	24

Demostración. Se puede encontrar en [47]. □

A partir de esto, podemos encontrar la cantidad de curvas en la familia que estamos considerando.

Proposición 4.2. *Sea E una curva elíptica supersingular sobre $\mathbb{F}_q$. El número de curvas en la familia*

$$Y^2 + Y = \lambda X + \mu X^3 \quad (\lambda \in \mathbb{F}_q, \mu \in \mathbb{F}_q^*)$$

que son isomorfas sobre $\mathbb{F}_q$ a E es igual a

$$\frac{(q-1)(\#E(\mathbb{F}_q)-1)}{\#Aut_{\mathbb{F}_q}(E)}.$$

Demostración. En la ecuación, reemplazamos X por $\mu^{-1}X$ e Y por $\mu^{-1}Y$ y luego sustituimos λ por $\lambda\mu^{-1}$. Así, nuestra familia de curvas elípticas supersingulares se convierte en

$$Y^2 + \mu Y = X^3 + \lambda X \, (\lambda \in \mathbb{F}_q, \mu \in \mathbb{F}_q^*).$$

Tomemos una de esas curvas E, una tranformación de la forma

$$Y \leftarrow u^3 Y + rX + s$$

$$X \leftarrow u^2 X + t,$$

con $r, s, t \in \mathbb{F}_q$, $u \in \mathbb{F}_q^*$, lleva a E a otra curva de la familia si y sólo si

$$s^2 + \mu s = t^3 + \lambda t \qquad \text{y} \qquad t = u^{-4} r^2.$$

Hay $(\#E(\mathbb{F}_q) - 1)(q-1)$ de estas transformaciones y todas las curvas correspondientes son isomorfas a E. Como todo $\mathbb{F}_q$-automorfismo de E es también de esta forma, el número de curvas en la familia isomorfas a E es

$$\frac{(q-1)(\#E(\mathbb{F}_q) - 1)}{\#Aut_{\mathbb{F}_q}(E)}.$$

Entonces, encontramos, usando la proposición anterior, exactamente $q(q-1)$ curvas, es decir, obtenemos todas las curvas de la familia. □

Usando ambas proposiciones obtenemos la distribución de pesos del código $B_m^\perp$ que damos en las siguientes tablas

Table 4.3: Espectro de $B_m^\perp$ para m impar

Peso	Frecuencia
0	1
$\frac{1}{2}(q + \sqrt{2q})$	$\frac{1}{4}(q-1)(q - \sqrt{2q})$
$\frac{1}{2}q$	$\frac{1}{2}(q-1)q + (q-1)$
$\frac{1}{2}(q - \sqrt{2q})$	$\frac{1}{4}(q-1)(q + \sqrt{2q})$

Table 4.4: Espectro de $B_m^\perp$ para m par

Peso	Frecuencia
0	1
$\frac{1}{2}(q + 2\sqrt{q})$	$\frac{1}{24}(q-1)(q - 2\sqrt{q})$
$\frac{1}{2}(q + \sqrt{q})$	$\frac{1}{3}(q-1)(q - \sqrt{q})$
$\frac{1}{2}q$	$\frac{1}{4}(q-1)q + (q-1)$
$\frac{1}{2}(q - \sqrt{q})$	$\frac{1}{3}(q-1)(q + \sqrt{q})$
$\frac{1}{2}(q - 2\sqrt{q})$	$\frac{1}{24}(q-1)(q + 2\sqrt{q})$

Finalmente usaremos identidades de MacWilliams para calcular la distribución de pesos del código B_m a partir de la de su dual. En efecto, teniendo en cuenta que se cumple (2.4), para los polinomios de Krawtchouk $K_k^{q-1,2}(x)$ que ya definimos, encontramos la distribución de pesos del código B_m. Se tiene que

$$\begin{aligned} q^2 A_k = {} & K_k^{q-1,2}(0) + \tfrac{q-1}{4}\big(q - \sqrt{2q}\big) K_k^{q-1,2}\big(\tfrac{q+\sqrt{2q}}{2}\big) + \big(\tfrac{q-1}{2}q + q - 1\big) K_k^{q-1,2}\big(\tfrac{q}{2}\big) \\ & + \tfrac{q-1}{4}\big(q + \sqrt{2q}\big) K_k^{q-1,2}\big(\tfrac{q-\sqrt{2q}}{2}\big), \end{aligned} \tag{4.5}$$

para m impar y que

$$\begin{aligned} q^2 A_k = {} & K_k^{q-1,2}(0) + \tfrac{q-1}{24}(q - 2\sqrt{q}) K_k^{q-1,2}\big(\tfrac{q+2\sqrt{q}}{2}\big) + \tfrac{q-1}{3}(q - \sqrt{q}) K_k^{q-1,2}\big(\tfrac{q+\sqrt{q}}{2}\big) \\ & + \big(\tfrac{q-1}{4}q + q - 1\big) K_k^{q-1,2}\big(\tfrac{q}{2}\big) + \tfrac{q-1}{3}(q + \sqrt{q}) K_k^{q-1,2}\big(\tfrac{q-\sqrt{q}}{2}\big) \\ & + \tfrac{q-1}{24}(q + 2\sqrt{q}) K_k^{q-1,2}\big(\tfrac{q-2\sqrt{q}}{2}\big), \end{aligned} \tag{4.6}$$

para m par.

Como ya dijimos, estos polinomios se pueden calcular por definición o usando la recurrencia que cumplen.

En el Apéndice calculamos la distribución de pesos de esta manera para algunos ejemplos.

Capítulo 5

Distribución de pesos de códigos de Melas

En este capítulo aplicamos la estrategia de la que hablamos en el capítulo anterior para encontrar la distribución de pesos de un código un poco menos conocido, el código de Melas. En particular, calculamos el espectro en los casos binario y ternario, a partir de curvas elípticas. Para este capítulo utilizamos [38] y [43].

Sean p un número primo, $m \geq 2$ y $q = p^m$. El código de Melas $M_p(m)$ es el código cíclico p-ario generado por el ideal generado por

$$m_\alpha(T)m_{\alpha^{-1}}(T),$$

en $\frac{\mathbb{F}_p[T]}{(T^{q-1}-1)}$, donde α es un generador de $\mathbb{F}_q^*$ y $m_\alpha(T)$ es el polinomio minimal de α.

Podemos ver a $M_p(m)$ como la restricción del código $\mathcal{M}_p(m)$ dado por el ideal generado por el polinomio

$$(T-\alpha)(T-\alpha^{-1}),$$

en $\frac{\mathbb{F}_q[T]}{(T^{q-1})}$, cuyo dual es el código

$$\mathcal{M}_p(m)^\perp = \{(\lambda x + \mu x^{-1})_{x\in\mathbb{F}_q^*} \,:\, \lambda, \mu \in \mathbb{F}_q\}.$$

En efecto, como $\mathcal{M}_p(m)$ tiene matriz de paridad

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(q-2)} \end{pmatrix},$$

entonces se tiene que

$$\begin{aligned} \mathcal{M}_p(m)^\perp &= \{cH \in \mathbb{F}_q^{q-1} \,:\, c \in \mathbb{F}_q^m\} \\ &= \{(\lambda+\mu, \lambda\alpha + \mu\alpha^{-1}, \ldots, \lambda\alpha^{q-2} + \mu\alpha^{-(q-2)}) \,:\, \lambda, \mu \in \mathbb{F}_q\}, \end{aligned}$$

Ahora, por el teorema de Delsarte tenemos

$$\begin{array}{ccc} \mathcal{M}_p(m) & \overset{dual}{\longleftrightarrow} & \mathcal{M}_p(m)^\perp \\ \mathrm{Res}\downarrow & & \downarrow\mathrm{Tr} \\ M_p(m) & \overset{dual}{\longleftrightarrow} & M_p(m)^\perp \end{array}$$

de donde deducimos que

$$M_p(m)^\perp = \{\phi(\lambda,\mu) = (\mathrm{Tr}(\lambda x + \mu x^{-1}))_{x\in\mathbb{F}_q^*} \,:\, \lambda,\mu \in \mathbb{F}_q\}. \tag{5.1}$$

Notemos que, por (5.1), sabemos que $M_p(m)^\perp$, y por lo tanto $M_p(m)$, no dependen de la elección del generador α.

Si $v \in M_p(m)^\perp$, $v = (v_1,\ldots,v_n) = (\mathrm{Tr}(\lambda x + \mu x^{-1}))_{x\in\mathbb{F}_q^*}$ entonces

$$\begin{aligned} w(v) &= n - \#\{1 \le i \le n \,:\, v_i = 0\} \\ &= n - \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(\lambda x + \mu x^{-1}) = 0\}. \end{aligned}$$

Por sumas exponenciales

La distribución de pesos del código Melas está relacionada, mediante la siguiente proposición, con ciertas sumas exponenciales, específicamente sumas de Kloosterman.

Proposición 5.1. *Los pesos de las palabras $\phi(\lambda,\mu)$ en $M_p(m)^\perp$ están dados por*

$$w(\phi(\lambda,\mu)) = \tfrac{1}{p}\{(p-1)(q-1) - \sum_{s\in\mathbb{F}_p^*} \kappa(s\lambda, s\mu)\}, \tag{5.2}$$

donde $\kappa(\lambda,\mu)$ es la suma de Kloosterman definida en (1.16) *con el carácter trivial.*

Demostración. Sea $f(x) = \lambda x + \mu x^{-1}$. Para cada $x \in \mathbb{F}_q$ tenemos:

$$\sum_{s\in\mathbb{F}_q} w_p^{s\mathrm{Tr}(f(x))} = \begin{cases} p, & \text{si } \mathrm{Tr}(f(x)) = 0, \\ 0, & \text{si } \mathrm{Tr}(f(x)) \neq 0. \end{cases}$$

Como ya vimos,

$$w(\phi(\lambda,\mu)) = q - 1 - \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(f(x)) = 0\}. \tag{5.3}$$

Entonces, tenemos que

$$\begin{aligned} \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(f(x)) = 0\} &= \sum_{x\in\mathbb{F}_q^*} \tfrac{1}{p} \sum_{s\in\mathbb{F}_p} w_p^{s\mathrm{Tr}(f(x))} = \tfrac{1}{p} \sum_{s\in\mathbb{F}_p} \sum_{x\in\mathbb{F}_q^*} w_p^{s\mathrm{Tr}(f(x))} \\ &= \tfrac{1}{p}\Big((q-1) + \sum_{s\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q^*} w_p^{s\mathrm{Tr}(f(x))}\Big). \end{aligned} \tag{5.4}$$

De (5.3) y (5.4) y usando (1.16) obtenemos (5.2), como queríamos ver. □

En general, estas sumas de Kloosterman no son conocidas, por lo tanto, no podemos encontrar la distribución de pesos del código de Melas binario de esta forma.

Por curvas

Como ya dijimos, para cada palabra código $v \in M_p(m)^\perp$ tenemos que

$$w(v) = n - \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(\lambda x + \mu x^{-1}) = 0\}.$$

Además, por el Teorema 1.6, se tiene que

$$\mathrm{Tr}(\lambda x + \mu x^{-1}) = 0$$

si y sólo si, existe $y \in \mathbb{F}_q$ tal que

$$y^p - y = \lambda x + \mu x^{-1}.$$

Por lo tanto, la distribución de pesos del código de Melas está estrictamente relacionada con el número de puntos racionales de la curva

$$E_{\lambda,\mu}: \qquad Y^p - Y = \lambda X + \mu X^{-1}.$$

Calcular el número de puntos racionales de esta curva es, en general, un problema difícil, sin embargo, para los casos $p = 2, 3$ lo podemos hacer.

5.1 Caso binario

Consideramos ahora el caso $p = 2$, o sea $q = 2^m$. El código cíclico $M_2(m)$ tiene dimensión $q - 1 - 2m$ y distancia mínima 3 ó 5, dependiendo si m es par o impar.

Por sumas exponenciales

Por la Proposición 5.1, considerando $p = 2$ tenemos que

$$w(\phi(\lambda, \mu)) = \tfrac{1}{2}\big\{q - 1 - \kappa(\lambda, \mu)\big\},$$

donde

$$\kappa(\lambda, \mu) = \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(\lambda x + \mu x^{-1})}.$$

Sin embargo, esta suma no es conocida.

Por curvas

Sabemos que si $v \in M_2(m)^\perp$ entonces

$$w(v) = n - \#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(\lambda x + \mu x^{-1}) = 0\}.$$

Si $\lambda = \mu = 0$ entonces v es la palabra cero.

En primer lugar, calcularemos la distribución de pesos de un código auxiliar, el subcódigo con $\mu \in \mathbb{F}_2$, definido por

$$\mathcal{C}_2(m) = \{c(\lambda, \mu) = (\mathrm{Tr}(\lambda x + \mu x^{-1})) \,:\, \lambda \in \mathbb{F}_q,\, \mu \in \mathbb{F}_2\}.$$

Teorema 5.2. *Los pesos de las palabras $c(\lambda, \mu)$ en $\mathcal{C}_2(m)$ están dados por:*

(a) $w(c(0,1)) = \frac{q}{2}$,

(b) $w(c(\lambda, 0)) = \frac{q}{2}$ *si* $\lambda \neq 0$,

(c) $w(c(\lambda, 1)) = q - \frac{1}{2}\#E_\lambda(\mathbb{F}_q)$, *para* $\lambda \neq 0$, *donde* E_λ *denota la curva elíptica*

$$E_\lambda : \quad y^2 + xy = x^3 + \lambda x.$$

Demostración. Los pesos de las palabras código $c(\lambda, \mu)$ son fácilmente determinados cuando $\lambda = 0$ ó $\mu = 0$. Sabemos que $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ es una forma lineal no trivial. Entonces el peso de

$$c(0,1) = (\mathrm{Tr}(x^{-1}))_{x \in \mathbb{F}_q^*}$$

es el cardinal del complemento del núcleo de esta forma lineal, que es igual a $\frac{q}{2}$.

De la misma manera, para $\lambda \neq 0$, tenemos que

$$w(c(\lambda, 0)) = w(c(1,0)) = w\big((\mathrm{Tr}(x))_{x \in \mathbb{F}_q^*}\big) = \frac{q}{2}.$$

En el caso restante, el peso está estrechamente relacionado con el número de puntos racionales en la curva

$$C_\lambda : \qquad y^2 + y = \lambda x + x^{-1}$$

sobre $\mathbb{F}_q$ (pues, por propiedades de la traza, $\mathrm{Tr}(\lambda x + \mu x^{-1}) = 0$ si y sólo si existe $y \in \mathbb{F}_q$ tal que $y^2 + y = \lambda x + \mu x^{-1}$, como $\mu \neq 0$, entonces $\mu = 1$). Para un $x \in \mathbb{F}_q^*$ dado, la ecuación cuadrática

$$y^2 + y = \lambda x + x^{-1}$$

tiene dos soluciones o ninguna, dependiendo si $\mathrm{Tr}(\lambda x + x^{-1}) = 0$ ó 1.

Sea $\gamma = \lambda x + x^{-1}$. Si $y^2 + y = \gamma$ tiene una solución $y \in \mathbb{F}_q$, entonces $y + 1$ es otra solución y, además, usando el Lema 1.5, tenemos que

$$\mathrm{Tr}(\gamma) = \mathrm{Tr}(y^2 + y) = \mathrm{Tr}(y^2) + \mathrm{Tr}(y) = \mathrm{Tr}(y) + \mathrm{Tr}(y) = 0.$$

Sea $T_0 = \{\gamma \in \mathbb{F}_q \,:\, \mathrm{Tr}(\gamma) = 0\}$. Como la traza $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ es sobreyectiva, entonces hay exactamente $\frac{q}{2}$ elementos en T_0.

Por otro lado, el mapa

$$y \mapsto y^2 + y$$

de $\mathbb{F}_q$ a T_0 tiene la propiedad de que cualquier $\gamma \in T_0$ tiene dos preimágenes distintas o ninguna en absoluto en $\mathbb{F}_q$, pues si y es una solución entonces $y + 1$ es también solución. Pero el último caso no puede ocurrir porque $|\mathbb{F}_q| = 2|T_0|$. Entonces el mapa es sobreyectivo, es decir, para cada $\gamma \in T_0$ la ecuación $y^2 + y = \gamma$ tiene dos soluciones $y \in \mathbb{F}_q$.

Luego,

$$\mathrm{Tr}(\lambda x + x^{-1}) = 1 - \tfrac{1}{2}\#\{y \in \mathbb{F}_q \,:\, y^2 + y = \lambda x + x^{-1}\},$$

entonces el peso de la palabra $c(\lambda, 1)$ es igual a

$$w(c(\lambda, 1)) = q - 1 - \tfrac{1}{2}\#C_{af}(\mathbb{F}_q),$$

donde $C_{af}(\mathbb{F}_q)$ denota el conjunto de puntos $\mathbb{F}_q$-racionales de la curva C_λ en el plano afín. Haremos un cambio de variables para pasar de la curva C_λ a una curva elíptica. En efecto, multiplicando la ecuación C_λ por $\lambda^2 x^2$ y reemplazando primero y por $x^{-1}y$ y luego x por $\lambda^{-1}x$, tenemos la ecuación de una curva elíptica

$$E_\lambda : \quad y^2 + xy = x^3 + \lambda x$$

Luego, C_λ y E_λ tienen el mismo número de puntos en el plano proyectivo sobre $\mathbb{F}_q$. Como C_λ tiene dos puntos en el infinito (los puntos $(0:0:1)$ y $(0:1:0)$), se sigue que

$$\#C_{af}(\mathbb{F}_q) = \#E_\lambda(\mathbb{F}_q) - 2.$$

Por lo tanto tenemos

$$w(c(\lambda, 1)) = q - \tfrac{1}{2}\#E_\lambda(\mathbb{F}_q),$$

y el teorema queda así demostrado. □

Para determinar la distribución de pesos del código $\mathcal{C}_2(m)$, tenemos que contar entonces el número de clases de isomorfismo de curvas elípticas sobre $\mathbb{F}_q$.

Denotamos $M_q(t)$ al número de clases de isomorfismo de curvas elípticas sobre $\mathbb{F}_q$ que cumplen

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

Proposición 5.3. *Sea $\mathbb{F}_q$ una extensión de $\mathbb{F}_2$ y sea t un entero impar. Entonces,*

$$M_q(t) = \begin{cases} H(t^2 - 4q), & \text{si } |t| < 2\sqrt{q}, \\ 0, & \text{caso contrario.} \end{cases}$$

Aquí, $H(\Delta)$ es el número de clase de Kronecker de Δ definido en la Sección 1.4.

Demostración. Es un resultado clásico. Una demostración se puede ver en [47]. □

Ahora sí calculamos el espectro del código $\mathcal{C}_2(m)$.

Teorema 5.4. *Los pesos no nulos de las palabras-código en $\mathcal{C}_2(m)$ son*

$$w_t = \tfrac{1}{2}(q - 1 + t),$$

donde $t \in \mathbb{Z}$, $t^2 < 4q$ y $t \equiv 1 \pmod 4$. Además, el número de palabras en $\mathcal{C}_2(m)$ de peso w_t está dado por

$$A_{w(t)} = \begin{cases} H(t^2 - 4q), & \text{si } t \neq 1, \\ H(1 - 4q) + q, & \text{si } t = 1. \end{cases}$$

Demostración. Consideremos la familia de curvas elípticas

$$E_a : \qquad y^2 + xy = x^3 + ax \qquad (a \in \mathbb{F}_q^*).$$

Para esta demostración seguiremos varios pasos.

(1) En primer lugar, veamos que el j-invariante de E_a es

$$j(E_a) = a^{-2}$$

para cada $a \in \mathbb{F}_q^*$.

Usando el cambio de variables visto en (1.9) dado por

$$(x, y) \mapsto (x, y + a),$$

la curva E_a se tranforma en

$$\overline{E}_a : \qquad (y + a)^2 + x(y + a) = x^3 + ax,$$

es decir,

$$\overline{E}_a : \qquad y^2 + xy = x^3 + a^2.$$

Entonces, el j-invariante de E_a está dado por

$$j(E_a) = \frac{1}{a^2} = a^{-2}.$$

Luego, cualquier curva elíptica E_q es no-supersingular, pues $j(E_a) \neq 0$. Además, todo elemento en $\mathbb{F}_q^*$ ocurre exactamente una vez como j-invariante en esta familia, pues en característica 2 todo elemento del cuerpo es un cuadrado.

(2) Se sabe que hay, para cada j-invariante distinto de cero exactamente dos curvas elípticas con este j-invariante, y si una de ellas tiene $q+1-t$ puntos sobre $\mathbb{F}_q$, entonces la otra tiene $q+1+t$ puntos (ver [38]).

(3) Veamos ahora que para cada curva de la familia, el punto

$$P = (a^{\frac{q}{2}}, 0)$$

es un punto $\mathbb{F}_q$-racional de orden 4. Tenemos que

$$(a^{\frac{q}{2}})^3 + a \cdot a^{\frac{q}{2}} = 2a^{\frac{3}{2}q} = 0,$$

entonces P es un punto $\mathbb{F}_q$-racional.

Notemos en primer lugar que $P = (a^{\frac{q}{2}}, 0) \neq -P = (a^{\frac{q}{2}}, a^{\frac{q}{2}})$. Entonces, para ver que es de orden 4 vamos a ver que $2P = -2P$. Con el cambio de variables que usamos en (1), tenemos que

$$P = (a^{\frac{q}{2}}, 0) \quad \mapsto \quad P = (a^{\frac{q}{2}}, a).$$

Luego, usando las fórmulas de adición dadas en el Capítulo 1, teniendo en cuenta que $\mathrm{char}(\mathbb{F}_q) = 2$, y $j(E_a) \neq 0$, tenemos que

$$\begin{aligned} 2P &= \Big((a^{\frac{q}{2}})^2 + \frac{a^2}{(a^{\frac{q}{2}})^2},\, (a^{\frac{q}{2}})^2 + \Big(a^{\frac{q}{2}} + \frac{a}{a^{\frac{q}{2}}}\Big)(a^q + a^{2-q} + a^q + a^{2-q}\Big) \\ &= \Big(a + a^{2-q},\, a^{\frac{q^2}{2}} + a^{2-\frac{q}{2}} + a^{\frac{q}{2}+1} + a^{3-\frac{q}{2}} + a\Big). \end{aligned}$$

Por otro lado, $-P = (a^{\frac{q}{2}}, a + a^{\frac{q}{2}})$, entonces se tiene

$$\begin{aligned} -2P &= \Big((a^{\frac{q}{2}})^2 + \frac{a^2}{(a^{\frac{q}{2}})^2},\, (a^{\frac{q}{2}})^2 + \Big(a^{\frac{q}{2}} + \frac{a + a^{\frac{q}{2}}}{a^{\frac{q}{2}}}\Big)(a^q + a^{2-q}) + a^q + a^{2-q}\Big) \\ &= \Big(a + a^{2-q},\, a + a^{\frac{q^2}{2}} + a^{2-\frac{q}{2}} + a^{1+\frac{q}{2}} + a^{3-\frac{q}{2}}\Big). \end{aligned}$$

Luego, $2P = -2P$ y, por lo tanto, P es de orden 4.

Concluimos que toda curva elíptica E sobre $\mathbb{F}_q$ tal que 4 divide a $|E(\mathbb{F}_q)| = q+1-t$ ocurre exactamente una vez en nuestra familia.

(4) Por la Proposición 5.3, el número de curvas elípticas sobre $\mathbb{F}_q$ con exactamente $q+1-t$ puntos sobre $\mathbb{F}_q$ es igual al número de clase de Kronecker $H(t^2-4q)$ cuando $t^2 < 4q$ y t es impar.

Entonces tenemos que los pesos no nulos de $\mathcal{C}_2(m)$ son los números

$$q - \tfrac{1}{2}(q+1-t) = \tfrac{1}{2}(q-1+t),$$

donde $t^2 < 4q$ y $t \equiv 1 \pmod 4$.

Cuando $t \neq 1$, sólo las palabras de tipo $c(a,1)$ pueden tener peso $\frac{q-1+t}{2}$, y hay exactamente $H(t^2-4q)$ de estas palabras. Cuando $t=1$, las palabras $c(0,1)$ y $c(a,0)$, con $a \in \mathbb{F}_q^*$, tienen peso $\frac{q}{2}$, por lo tanto, $H(1-4q)+q$ palabras tienen peso $\frac{q}{2}$. □

Esto nos da la distribución de pesos de nuestro código auxiliar $\mathcal{C}_2(m)$. A partir de esto, encontramos la distribución de pesos del código dual $M_2(m)^\perp$.

Teorema 5.5. *Los pesos no nulos de $M_2(m)^\perp$ son*

$$w_t = \tfrac{1}{2}(q-1+t),$$

donde $t \in \mathbb{Z}$, $t^2 < 4q$ y $t \equiv 1 \pmod 4$. Para $t \neq 1$, la frecuencia del peso w_t es $(q-1)H(t^2-4q)$ y el peso $w_1 = \frac{q}{2}$ tiene frecuencia $(q-1)(H(1-4q)+2)$.

Demostración. El grupo $\mathbb{F}_q^*$ actúa sobre el código $M_2(m)^\perp$ por:

$$c(a,b) \to c(\zeta a, \zeta^{-1} b), \quad \text{para } \zeta \in \mathbb{F}_q^*.$$

Las palabras en la misma órbita tienen el mismo peso.

Para $b=0$ tenemos la palabra cero y $q-1$ palabras de peso $\frac{q}{2}$ en $M_2(m)^\perp$. El conjunto de palabras con $b \neq 0$ es estable bajo la acción de $\mathbb{F}_q^*$, toda órbita tiene longitud $q-1$ y contiene exactamente una palabra $c(a,1)$ del código $\mathcal{C}_2(m)$. Por lo tanto, para los pesos distintos de $\frac{q}{2}$, el teorema se sigue del teorema anterior.

Las $q-1$ palabras con $b=0$ y las $q-1$ palabras en la órbita de $c(0,1)$ todas tienen peso $\frac{q}{2}$. Junto con las $H(1-4q)$ órbitas de las palabras $c(a,1)$ con $a \neq 0$ que tienen peso $\frac{q}{2}$ en $\mathcal{C}_2(q)$, tenemos $(q-1)(H(1-4q)+2)$ palabras de peso $\frac{q}{2}$. □

Para obtener la distribución de pesos del código de Melas, vamos a combinar el teorema anterior con la identidad de MacWilliams y la siguiente fórmula de trazas de Eicher-Selberg para $\Gamma_1(4)$ obtenida por Schoof y van der Vlugt. El nivel 4 está relacionado con el hecho de que las curvas en nuestra familia todas admiten un punto $\mathbb{F}_q$-racional de orden 4.

Teorema 5.6 ([39])**.** *Sea $m \geq 1$ y $q = 2^m$. La traza del operador de Hecke T_q actuando sobre el espacio cuspidal $S_k(\Gamma_1(4))$ de peso $k \geq 2$ está dada por:*

$$\mathrm{Tr}(T_q) = \begin{cases} -1+q-\sum_t H(t^2-4q) = 0, & \text{si } k=2, \\ -1-(-1)^{\frac{kq}{2}} \sum_t Q_{k-2}(t,q) H(t^2-4q), & \text{si } k \geq 3. \end{cases}$$

Aquí, t se mueve en $\{t \in \mathbb{Z} : t^2 < 4q,\ t \equiv 1 \pmod 4\}$ y los números $Q_k(t,n)$ están definidos recursivamente como sigue

$$Q_0(t,n) = 1, \quad Q_1(t,n) = t, \quad Q_{k+1}(t,n) = tQ_k(t,n) - nQ_{k-1}(t,n) \quad \text{para} \quad k \geq 1.$$

Demostración. Usaremos la descomposición del espacio $S_k(\Gamma_1(N),1)$ dada en (1.12), es decir $S_k(\Gamma_1(N)) = S_k(\Gamma_1(N),1) = \bigoplus_\chi S_k(\Gamma_0(N),\chi)$. Luego, para $N=4$ tenemos que

$$S_k(\Gamma_1(4)) = \begin{cases} S_k(\Gamma_0(4),1) & \text{si } k \text{ es par,} \\ S_k(\Gamma_0(4),\xi) & \text{si } k \text{ es impar,} \end{cases}$$

donde ξ denota un carácter no trivial de $(\mathbb{Z}/4\mathbb{Z})^*$.

Teniendo en cuenta el Teorema 1.12, uno puede chequear que $A_3 = -1$ y para t fijo, todos los $\mu(t,f,q)$ que ocurren en la fórmula de la traza son iguales. En efecto, uno encuentra que

$$\mu(t,f,q) = (-1)^{\frac{q}{2}}\chi(t),$$

donde χ denota 1 ó ξ dependiendo si k es par o impar.

Por lo tanto, por (1.14), la suma de los números de clase h_w puede ser reemplazada por el número de clase de Kronecker. El resultado sigue ahora directamente del Teorema 1.12. Para $k=2$ la traza es cero pues es bien conocido que $\dim(S_2(\Gamma_1(4))) = 0$. □

Finalmente damos la distribución de pesos de los códigos binarios de Melas obtenida por Schoof ([38]).

Teorema 5.7. *El número A_i de palabras de peso i en el código de Melas $M_2(m)$ está dado por*

$$q^2 A_i = \tbinom{q-1}{i} + 2(-1)^{[\frac{i+1}{2}]}(q-1)\tbinom{q/2}{[i/2]} - (q-1)\sum_{\substack{0\le j\le i \\ j\equiv i \pmod 2}} W_{i,j}(q)\,(1+\tau_{j+2}(q)),$$

donde $\tau_2(q) = -q$ y $\tau_k(q)$ denota la traza del operador de Hecke T_q sobre el espacio $S_k(\Gamma_1(4))$ para $k \ge 3$ y los polinomios $W_{i,j}$ están definidos recursivamente por $W_{0,0}=1$, $W_{1,1}=-1$,

$$(i+1)W_{i+1,j+1} = -qW_{i,j+2} - W_{i,j} - (q-i)W_{i-1,j+1}$$

para $0 \le j \le i$ e $i \equiv j \pmod 2$ y $W_{i,j} = 0$ para los restantes i,j.

Observación 5.8. Para el polinomio $Q_k(t,n)$ definido en el Teorema 5.6, cuando le asignamos a la variable t peso igual a 1 y a n peso igual a 2, entonces $Q_k(t,n)$ es visto como un polinomio homogéneo de peso k.

Viéndolo como un polinomio en t, $Q_k(t,n)$ es mónico y entonces se puede escribir

$$t^i = \sum_{j=0}^{i} \lambda_{i,j}\, Q_{i-j}(t,n)\, n^{\frac{j}{2}},$$

donde los $\lambda_{i,j}$ satisfacen $\lambda_{i,j} = 0$ cuando $j \notin \{0,1,\dots,i\}$ o j es impar,

$$\lambda_{0,0} = \lambda_{1,0} = 1 \qquad \text{y} \qquad \lambda_{i+1,j} = \lambda_{i,j-2} + \lambda_{i,j}$$

para los demás índices.

Demostración. Para $0 \leq \ell \leq q-1$, definimos

$$f_\ell(x) = K_\ell^{q-1,2}\left(\tfrac{q-1+x}{2}\right).$$

En lo que resta de la demostración denotaremos el polinomio de Krawtchouk sólo por $K_i(x)$. Por la relación de recurrencia que cumplen estos polinomios, tenemos

$$f_0(x) = 1, \qquad f_1(x) = -x, \qquad (\ell+1)f_{\ell+1}(x) = -xf_\ell(x) - (q-1)f_{\ell-1}(x).$$

Se sigue que $f_\ell(x)$ tiene grado ℓ y la paridad de $f_\ell(x)$ es igual a la paridad de ℓ. Entonces podemos escribir

$$f_\ell(x) = \sum_{\substack{0\leq k\leq \ell \\ k\equiv \ell \pmod 2}} \pi_\ell(k)\, x^k,$$

donde

$$\pi_0(0) = 1, \quad \pi_1(1) = 1, \quad (\ell+1)\pi_{\ell+1}(k+1) = -\pi_\ell(k) - (q-1)\pi_{\ell-1}(k+1).$$

Ahora aplicamos la identidad de MacWilliams para la distribución de pesos del código de Melas $M_2(m)$. Primero tenemos que:

$$q^2 A_i = \sum_{t\in D} A_{w_t} K_i(\tfrac{q-1+t}{2}) + K_i(0), \tag{5.5}$$

donde $D = \{t \in \mathbb{Z} : t^2 < 4q,\, t \equiv 1 \pmod 4\}$.

Luego, usando (5.5), el Teorema 5.5 y la definición de f_i se tiene que

$$\tfrac{q^2}{q-1} A_i = \sum_t f_i(t) H(t^2-4q) + \tfrac{K_i(0)}{q-1} + 2f_i(1),$$

donde

$$K_i(0) = \tbinom{q-1}{i}, \qquad f_i(1) = (-1)^{[\frac{i+1}{2}]}\tbinom{\frac{q}{2}-1}{[\frac{i}{2}]}.$$

Entonces,

$$\sum_t f_i(t) H(t^2-4q) = \sum_{\substack{0\leq j\leq i \\ j\equiv i \pmod 2}} \pi_i(j) \sum_t t^j H(t^2-4q).$$

Por la observación anterior, esto es

$$\sum_{\substack{0\leq j\leq i \\ j\equiv i \pmod 2}} \pi_i(j) \sum_{\substack{0\leq k\leq j \\ k \text{ par}}} \lambda_{j,k}\, q^{\frac{k}{2}} \sum_t Q_{j-k}(t,q) H(t^2-4q).$$

Usando ahora el Teorema 5.6 que da la traza del operador de Hecke T_q, esto se convierte, ya que 4 divide a q, en

$$\sum_{\substack{0\leq j\leq i \\ j\equiv i \pmod 2}} \pi_i(j) \sum_{\substack{0\leq k\leq j \\ k \text{ par}}} \lambda_{j,k} q^{\frac{k}{2}} (-1 - \tau_{j-k+2}(q)).$$

Haciendo un cambio de variables nos queda

$$\sum_t f_i(t)H(t^2-4q) = \sum_{\substack{0\le j\le i \\ j\equiv i(mod\,2)}} W_{i,j}(q)(-1-\tau_{j+2}(q)),$$

donde

$$W_{i,j}(q) = \sum_{\substack{0\le k\le i-j \\ k \text{ par}}} \pi_i(k+j)\,\lambda_{k+j,k}\,q^{\frac{k}{2}},$$

y $W_{i,j}(q)$ satisface la relación de recurrencia requerida. □

5.2 Caso ternario

Consideremos el caso $p=3$. Sean $m\ge 2$ y $q=3^m$. Sea V el espacio vectorial sobre $\mathbb{F}_3$ dado por

$$V = \{f : \mathbb{F}_q^* \to \mathbb{F}_3 \mid f \text{ es } \mathbb{F}_3\text{-lineal}\}.$$

Este espacio tiene una base que consiste de las funciones características de los elementos de $\mathbb{F}_q^*$, entonces V puede ser identificado con $(\mathbb{F}_3)^{q-1}$. Tenemos entonces que

$$M_3(m)^\perp = \{\phi(a,b) = \left(\mathrm{Tr}(ax+bx^{-1})\right)_{x\in\mathbb{F}_q^*} \,:\, a,b\in\mathbb{F}_q\}$$

y el subcódigo auxiliar

$$\mathcal{C}_3(m) = \{c(a,b)\in M_3(m)^\perp \,:\, b\in\mathbb{F}_3\}.$$

Ahora damos su distribución de pesos de $\mathcal{C}_3(m)$.

Lema 5.9. *El peso $w(a,b)$ de la palabra $c(a,b)$ en el código $M_3(m)^\perp$ satisface lo siguiente.*

(a) $w(0,0)=0$,

(b) $w(0,1)=w(0,2)=\frac{2q}{3}$,

(c) $w(a,0)=\frac{2q}{3}$ *para* $a\neq 0$,

(d) $w(a,b)=w(ab,1)$ *para* $b\neq 0$,

(e) $w(a,1)=q-\frac{1}{3}(\#X_a(\mathbb{F}_q)+1)$, *donde*

$$X_a: \qquad Y^p-Y = aX+\frac{1}{X}, \qquad a\in\mathbb{F}_q^*.$$

Demostración. Si $a=b=0$, entonces $c(a,b)$ es la palabra cero y, por lo tanto, tiene peso cero. Cuando $a=0$ y $b\neq 0$, se tiene que

$$c(0,b) = (\mathrm{Tr}(bx^{-1})),$$

entonces $w(0,b) = \frac{2q}{3}$. Similarmente, cuando $b = 0$ y $a \neq 0$ tenemos que $w(a,0) = \frac{2q}{3}$.

El grupo $\mathbb{F}_q^*$ actúa sobre $M_3(m)^\perp$ por

$$c(a,b) \mapsto c(za, z^{-1}b),$$

y esta acción preserva los pesos de las palabras código. Luego,

$$w(a,b) = w(c(a,b)) = w(c(ba, b^{-1}b)) = w(c(ab,1)) = w(ab,1),$$

entonces se cumple (d).

Tenemos que

$$w(a,1) = q - 1 - \tfrac{1}{3}\#\{x \in \mathbb{F}_q^* \,:\, \mathrm{Tr}(ax + \tfrac{1}{x} = 0)\} = q - 1 - \tfrac{1}{3}\#X_a^0(\mathbb{F}_q),$$

donde X_a^0 es la curva Artin-Schreier afín dada por

$$Y^3 - Y = aX + \frac{1}{X} \qquad \text{para } X \neq 0.$$

Además,

$$\#X_a(\mathbb{F}_q) = \#X_a^0(\mathbb{F}_q) + 2,$$

entonces se tiene que

$$w(a,1) = q - 1 - \tfrac{1}{3}(\#X_a(\mathbb{F}_q) - 2) = q - \tfrac{1}{3}(\#X_a(\mathbb{F}_q) + 1),$$

que es lo queríamos ver. □

Esto nos permite obtener la distribución de pesos del dual del código de Melas ternario.

Teorema 5.10. *Los pesos distintos de cero del código dual $M_3(m)^\perp$ son*

$$w_t = \tfrac{2}{3}(q - 1 + t),$$

con $t \in \mathbb{Z}$, $t^2 < 4q$ y $t \equiv 1 \pmod 3$. El peso $w_1 = \frac{2q}{3}$ tiene frecuencia $(q-1)(H(1-4q)+2)$ mientras que para $t \neq 1$ el peso w_t tiene frecuencia $(q-1)H(t^2-4q)$.

Demostración. La demostración de este teorema sigue del Lema 5.9 y es similar a la demostración del Teorema 5.6, teniendo en cuenta que el j-invariante de la curva es ahora a^{-3} y que, en lugar de tener un punto de orden 4, tiene un punto de orden 3. □

Estrechamente conectadas a X_a están las curvas $X_{a,\gamma}$ (resp. $X_{a,\delta}$) definidas por

$$Y^3 - Y = aX + X^{-1} + \gamma \quad (\text{respect.} \quad Y^3 - Y = aX + X^{-1} + \delta),$$

donde γ (resp. δ) es un elemento de $\mathbb{F}_q$ con $\mathrm{Tr}(\gamma) = 1$ (resp. $\mathrm{Tr}(\delta) = 2$). Tenemos que

$$\#X_{a,\gamma}(\mathbb{F}_q) + \#X_{a,\delta}(\mathbb{F}_q) + \#X_a(\mathbb{F}_q) = 6 + 3(q-1),$$

pues para $x \in \mathbb{F}_q^*$ exactamente una de las expresiones

$$ax + x^{-1}, \qquad ax + x^{-1} + \gamma, \qquad ax + x^{-1} + \delta$$

tiene traza cero, así que para cada x hay tres puntos en la unión de estas tres curvas. Más aún, tenemos

$$\#X_{a,\gamma}(\mathbb{F}_q) = \#X_{a,\delta}(\mathbb{F}_q),$$

es decir, si

$$\#X_a(\mathbb{F}_q) = q + 1 - 2t$$

entonces

$$\#X_{a\gamma}(\mathbb{F}_q) = \#X_{a,\delta}(\mathbb{F}_q) = q + 1 + t.$$

Luego, podemos determinar completamente la distribución de pesos de $M_3(m)^\perp$. Si una palabra $c(a, b)$ tiene peso $\frac{2(q-1+t)}{3}$, contiene $\frac{q-1+t}{3}$ unos y $\frac{q-1+t}{3}$ dos.

Para obtener la distribución de pesos del código Melas $M_3(m)$ vamos a combinar lo anterior con la identidad de MacWilliams y la siguiente proposición, que nos da una fórmula para las trazas del operador de Hecke T_q sobre $S_k(\Gamma_1(3))$. El nivel 3 está relacionado con el hecho de que las curvas de esta familia todas admiten un punto $\mathbb{F}_q$-racional de orden 3.

Proposición 5.11. *Sea $q = 3^m$ con $m \geq 1$, y denotaremos por $\mathrm{Tr}(T_q)$ a la traza del operador de Hecke T_q actuando en el espacio de formas cuspidales $S_k(\Gamma_1(3))$. Entonces*

$$\mathrm{Tr}(T_q) = \begin{cases} -\sum_t Q_{k-2}(t,q)H(t^2-4q) - 1, & \text{si } k \geq 3, \\ -\sum_t H(t^2-4q) - 1 + q, & \text{si } k = 2, \end{cases}$$

donde $Q_k(t, q)$ se define recursivamente por $Q_0(t, q) = 1$, $Q_1(t, q) = t$ y

$$Q_k(t,q) = tQ_{k-1}(t,q) - qQ_{k-2}(t,q) \qquad \text{para } k \geq 2.$$

Demostración. Sale a partir del Teorema 5.6 y se puede ver en [43]. □

Ahora sí estamos en condiciones de dar la distribución de pesos del código de Melas ternario $M_3(m)$.

Teorema 5.12. *El número A_i de palabras código de peso i en el código de Melas $M_3(m)$ está dado por*

$$q^2 A_i = \binom{q-1}{i}2^i + 2(q-1)\sum_{s=0}^{i}(-1)^s\binom{\frac{2q}{3}}{s}\binom{\frac{q}{3}-1}{i-s}2^{i-s} - (q-1)\sum_{j=0}^{i} W_{i,j}(q)\left(1 + T_{j+2}(q)\right),$$

donde los polinomios $W_{i,j}(q)$ con $0 \leq j \leq i$ están definidos por

$$W_{0,0} = 1, \quad W_{1,0} = 0, \quad W_{1,1} = -2,$$
$$(i+1)W_{i+1,j} = -iW_{i,j} - 2qW_{i,j+1} - 2W_{i,j-1} - 2(q-i)W_{i-1,j},$$

y cero los demás, y donde $T_2(q) = -q$ y $T_k(q)$ denota la traza del operador de Hecke T_q en el espacio $S_k(\Gamma_1(3))$ para $k \geq 3$.

Demostración. Para $0 \leq i \leq q-1$ sean $K_i^{q-1,3}(x)$ los polinomios de Krawtchouk ternarios (los denotamos en el resto de la demostración por $K_i(x)$). Definimos

$$f_i(x) = K_i^{q-1}\big(\tfrac{2(q-1+x)}{3}\big),$$

entonces se tiene que

$$f_0(x) = K_0\big(\tfrac{2(q-1+x)}{3}\big) = 1, \qquad f_1(x) = K_1\big(\tfrac{2(q-1+x)}{3}\big) = -2x,$$

y se cumple la recurrencia

$$(i+1)f_{i+1}(x) = (-i-2x)f_i(x) - 2(q-i)f_{i-1}(x).$$

Se sigue que $f_i(x)$ tiene grado i y podemos escribir

$$f_i(x) = \sum_{k=0}^{i} \pi_i(k)x^k, \tag{5.6}$$

donde

$$\pi_0(0) = 1, \qquad \pi_1(0) = 0, \qquad \pi_1(1) = -2,$$
$$(i+1)\pi_{i+1}(k) = -i\pi_i(k) - 2\pi_i(k-1) - 2(q-1)\pi_{i-1}(k).$$

Aplicamos la identidad de MacWilliams a $M_3(m)$ y $M_3(m)^\perp$ y obtenemos

$$q^2 A_i = \sum_{t\in D} A_{w_t} K_i\big(\tfrac{2(q-1+)t}{3}\big) + K_i(0),$$

donde

$$D = \{t \in \mathbb{Z} \ : \ t^2 - 4q \ \text{ y } \ t \equiv 1 \pmod 3\}.$$

Usando la distribución de pesos de $M_3(m)^\perp$, que ya conocemos, y los polinomios f_i que definimos antes, llegamos a que

$$\tfrac{q^2}{q-1} A_i = \sum_t H(t^2-4q)f_i(t) + 2f_i(1) + \tfrac{1}{q-1}K_i(0).$$

Se tiene que $K_i(0) = \binom{q-1}{i}2^i$, y además

$$f_i(1) = K_i(\tfrac{2q}{3}) = \sum_{s=0}^{i}(-1)^s \binom{\frac{2q}{3}}{s}\binom{\frac{q}{3}-1}{i-s}2^{i-s}.$$

De (5.6) obtenemos

$$\sum_t H(t^2-4q)f_i(t) = \sum_{j=0}^{i}\pi_i(j)\sum_t t^j H(t^2-4q).$$

Por lo visto en la Observación 5.8, esta expresión se convierte en

$$\sum_{j=0}^{i} \pi_i(j) \sum_{\substack{0\leq k\leq j \\ k \text{ par}}} \lambda_{j,k}\, q^{\frac{k}{2}} \sum_{t} Q_{j-k}(t,q)\, H(t^2-4q).$$

Por lo visto en el Teorema 5.5, sumado al hecho de que $\mathrm{Tr}(T_q) = 0$ en $S_2(\Gamma_1(3))$ (pues $\dim S_2(\Gamma_1(3)) = 0$), y de acuerdo a la convención de que $T_2(q) = -q$, obtenemos la expresión

$$\sum_{j=0}^{i} \pi_i(j) \sum_{\substack{k=0 \\ k \text{ par}}}^{j} \lambda_{j,k}\, q^{\frac{k}{2}}\, (-1 - T_{j-k+2}(q)). \tag{5.7}$$

Definimos

$$W_{i,j}(q) = \sum_{\substack{k=0 \\ k \text{ par}}}^{i-j} \pi_i(k+j)\lambda_{k+j,k} q^{\frac{k}{2}}.$$

Entonces, (5.7) se transforma en la expresión

$$\sum_{j=0}^{i} W_{i,j}(q)(-1 - T_{j+2}(q)).$$

Todo esto nos da la fórmula que enunciamos para $q^2 A_i$. □

Capítulo 6

Distribución de pesos de códigos de Zetterberg

Mostraremos ahora como, a partir del espectro conocido del código de Melas, se puede obtener la distribución de pesos del código de Zetterberg. Como los espectros de los códigos de Melas binarios y ternarios se conocen, podremos obtener los espectros de los códigos de Zetterberg binarios y ternarios. Para este capítulo hemos consultado los trabajos [39] y [44].

Sean p un número primo, m un entero positivo y $q = p^m$. Sea β un generador del grupo $\mu_{q+1} \subset \mathbb{F}_{q^2}^*$ de las $q+1$ raíces de la unidad. Consideramos el código $\mathcal{Z}_p(m)$ de longitud $q+1$ sobre $\mathbb{F}_{q^2}^*$ con polinomio generador $x-\beta$. El *código de Zetterberg* $Z_p(m)$ de longitud $q+1$ está definido como la restricción de $\mathcal{Z}_p(m)$ a $\mathbb{F}_p$.

Luego, por el teorema de Delsarte tenemos que

$$\begin{array}{ccc} \mathcal{Z}_p(m) & \overset{\text{dual}}{\longleftrightarrow} & \mathcal{Z}_p(m)^\perp \\ \text{Res}\downarrow & & \downarrow \text{Tr} \\ Z_p(m) & \overset{\text{dual}}{\longleftrightarrow} & Z_p(m)^\perp \end{array}$$

Entonces, se tiene

$$Z_p(m)^\perp = \{\text{Tr}(ax)_{x\in\mu_{q+1}} \,:\, a \in \mathbb{F}_{q^2}\}.$$

6.1 Caso binario

Consideremos ahora $p = 2$. Sean $m \geq 3$ y $q = 2^m$. Tenemos que

$$Z_2(m)^\perp = \{\text{Tr}(ax)_{x\in\mu_{q+1}} \,:\, a \in \mathbb{F}_{q^2}\}.$$

Entonces, la distribución de pesos de $Z_2(m)^\perp$ es inmediata del siguiente teorema.

Teorema 6.1. *Los pesos no-nulos del código dual $Z_2(m)^\perp$ y sus respectivas frecuencias están dadas por*

$$w_t = \tfrac{1}{2}(q+1-t) \qquad y \qquad A_{w_t} = (q+1)H(t^2-4q)$$

donde $t \in \mathbb{Z}$, $t^2 < 4q$ y $t \equiv 1 \pmod 4$.

Demostración. Como $\mathbb{F}_{q^2}^*$ es producto directo de μ_{q+1} y $\mathbb{F}_q^*$, podemos escribir cualquier $a \in \mathbb{F}_{q^2}^*$ como

$$a = A \cdot \varsigma, \quad \text{donde} \quad A \in \mathbb{F}_q^*, \quad \varsigma \in \mu_{q+1}.$$

Luego, el peso de la palabra $(\mathrm{Tr}(ax))_{x\in\mu_{q+1}}$ es igual a el peso de la palabra $(\mathrm{Tr}(Ax))_{x\in\mu_{q+1}}$, y tenemos que

$$\big(\mathrm{Tr}(Ax)\big)_{x\in\mu_{q+1}} = \big(\mathrm{Tr}_{q/2}(Ax+(Ax)^q)\big)_{x\in\mu_{q+1}} = \big(\mathrm{Tr}_{q/2}(A(x+\tfrac{1}{x})\big)_{x\in\mu_{q+1}}.$$

Es claro que los conjuntos

$$\{A(x+\tfrac{1}{x}) \,:\, x \in \mu_{q+1}\} \qquad \text{y} \qquad \{A(x+\tfrac{1}{x}) \,:\, x \in \mathbb{F}_q^*\}$$

tienen intersección $\{0\}$ y unión $\mathbb{F}_q$. Concluimos que

$$w((\mathrm{Tr}(ax))_{x\in\mu_{q+1}}) = q - w((A(x+\tfrac{1}{x}))_{x\in\mathbb{F}_q^*}).$$

Mientras A recorre $\mathbb{F}_q^*$, las palabras $(\mathrm{Tr}(A(x+\frac{1}{x})))_{x\in\mathbb{F}_q^*}$ recorren el conjunto de representantes de las órbitas de las palabras $c(a,b)$ del código dual del código de Melas $M_2(m)^\perp$. Como cada $A \in \mathbb{F}_q^*$ ocurre para $q+1$ valores de $a \in \mathbb{F}_{q^2}^*$ el resultado sigue del Teorema 5.4. □

A partir de esto, encontramos la distribución de pesos del código $Z_2(m)$. Conocemos los enumeradores de pesos

$$W_{M_2(m)^\perp}(x) = \sum_t (q-1)H(t^2-4q)x^{\frac{q-1+t}{2}} + 2(q-1)x^{\frac{q}{2}} + 1,$$

del dual del código de Melas $M_2(m)^\perp$ y

$$W_{Z_2(m)^\perp}(x) = \sum_t (q+1)H(t^2-4q)x^{\frac{q+1-t}{2}} + 1,$$

del dual del código de Zetterberg $Z_2(m)^\perp$.

Usando la identidad de MacWilliams se tiene que

$$\begin{aligned} q^2 W_{Z_2(m)}(x) \;&= q^2\tbinom{q+1}{q-1}(1-x^2)W_{M_2(m)}(-x) - 2(q+1)(1+x)(1-x^2)^{\frac{q}{2}} \\ &\quad -\tbinom{q+1}{q-1}(1+x)(1-x)^q + (1+x)^{q+1}. \end{aligned}$$

Esto, nos da una fórmula para los números A_i de palabras de peso i en el código de Zetterberg $Z_2(m)$.

Teorema 6.2. *El número A_i de palabras de peso i en el código de Zetterberg $Z_2(m)$ está dado por*

$$q^2 A_i = \binom{q+1}{i} - (q+1) \sum_{\substack{0 \le j \le i \\ j \equiv 1 \pmod 2}} V_{i,j}(q)(1 + \tau_{j+2}(q)).$$

Aquí, los polinomios $V_{i,j}(q)$, para $0 \le j \le i$ y $i \equiv j \pmod 2$, están definidos por:

$$V_{0,0} = 1, \quad V_{1,1} = 1, \quad (i+1)V_{i+1,j+1} = qV_{i,j+2} + V_{i,j} - (q+2-i)V_{i-1,j+1}.$$

Además, $\tau_2(q) = -q$ y $\tau_k(q)$ denota la traza del operador de Hecke T_q sobre $S_k(\Gamma_1(4))$ para $k \ge 3$.

6.2 Relación entre dos tipos de curvas Artin-Schreier

Sea p un número primo > 2. Consideramos la curva M_b sobre $\mathbb{F}_{p^m}$ definida por

$$M_b : \qquad Y^p - Y = bX - X^{-1} \qquad \text{con} \quad b \in \mathbb{F}_{p^m}^* \tag{6.1}$$

y $Z_{a,m}$ sobre $\mathbb{F}_{p^{2m}}$ definida por

$$Z_{a,m} : \qquad Y^p - Y = aX^{p^m} \qquad \text{con} \quad a \in \mathbb{F}_{p^{2m}}^*. \tag{6.2}$$

El número de puntos de la curva M_b sobre $\mathbb{F}_{p^m}$ y de la curva $Z_{a,m}$ sobre $\mathbb{F}_{p^{2m}}$ resultan estar relacionados de la siguiente manera.

Teorema 6.3. *Sean M_b y $Z_{a,m}$ las curvas definidas en (6.1) y (6.2) respectivamente. Entonces, para $b = a^{p^m+1}$ se tiene*

$$\#Z_{a,m}(\mathbb{F}_{p^{2m}}) = 2(p^{2m} - 1) + p + 1 - (p^m - 1)\#M_b(\mathbb{F}_{p^m}).$$

Demostración. Primero notemos que

$$\mathbb{F}_{p^m}^* \cdot \mu_{p^m+1} = \{\xi^2 \,:\, \xi \in \mathbb{F}_{p^{2m}}^*\},$$

ya que ambos son subgrupos del grupo cíclico $\mathbb{F}_{p^{2m}}^*$. Tenemos que

$$\#Z_a(\mathbb{F}_{p^{2m}}) = p + 1 + p(p^m - 1)t$$

con

$$\begin{aligned} t = t(a) &= \#\{u \in \mu_{p^m+1} \,:\, \mathrm{Tr}(au) = 0\} \\ &= \#\left\{u \in \mu_{p^m+1} \,:\, \mathrm{Tr}(au + \tfrac{b}{au}) = 0\right\}. \end{aligned}$$

Análogamente, se tiene que

$$\#M_b(\mathbb{F}_{p^m}) = 2 + qs$$

con

$$\begin{aligned} s = s(b) &= \#\left\{x \in \mathbb{F}_{p^m}^* \,:\, \mathrm{Tr}(bx + \tfrac{1}{x}) = 0\right\} \\ &= \#\{x \in \mathbb{F}_{p^m}^* \,:\, \mathrm{Tr}(x + \tfrac{b}{x}) = 0\}. \end{aligned}$$

Se puede comprobar que la relación que queremos es

$$s + t = 2p^{m-1}.$$

Distinguiremos dos casos, según a sea o no un cuadrado en $\mathbb{F}_{p^{2m}}^*$.

(i) a no es un cuadrado en $\mathbb{F}_{p^{2m}}^*$.

Se cumple que:

(a) El mapa $\alpha : \mathbb{F}_{p^m}^* \to \mathbb{F}_{p^m}$ dado por $x \mapsto x + \frac{b}{x}$ es inyectivo en su imagen.

(b) El mapa $\beta : \mu_{p^m+1} \to \mathbb{F}_{p^m}$ dado por $u \mapsto au + \frac{b}{au}$ es inyectivo en su imagen.

(c) $\alpha(\mathbb{F}_{p^m}^*) \cap \beta(\mu_{p^m+1}) = \varnothing$ y $\alpha(\mathbb{F}_{p^m}^*) \cup \beta(\mu_{p^m+1}) = \mathbb{F}_{p^m}$.

En efecto, si $\alpha(x) = \alpha(y)$ entonces $x = y$ o $b = xy$, es decir, $y = \frac{b}{x}$ e $y \neq x$ (pues si no $b = x^2$ y a sería un cuadrado). Análogamente, si $\beta(u) = \beta(v)$ entonces $u = v$, o $uv = \frac{b}{a^2} \in \mu_{p^m+1}$, es decir, $v = \frac{b}{a^2 u}$ y $u \neq v$ (si no, a sería un cuadrado). Para ver (3) notemos que si $\alpha(x) = \beta(u)$ entonces $a = \frac{x}{u}$ o $a = \frac{b}{ux}$, y ambas posibilidades no pueden ser pues a no pertenece a $\mathbb{F}_{p^m}^* \cdot \mu_{p^m+1}$. El resto sigue de contar elementos.

(ii) a es un cuadrado en $\mathbb{F}_{p^{2m}}^*$.

Hay sólo dos maneras de escribir a como producto de un elemento de $\mathbb{F}_{p^m}^*$ y un elemento de μ_{p^m+1}, digamos $a = c \cdot \zeta$ o bien $a = (-c)(-\zeta)$, con $c \in \mathbb{F}_{p^m}^*$ y $\zeta \in \mu_{p^m+1}$. Entonces, $b = c^2$. Tenemos que

(a) El mapa $\alpha : \mathbb{F}_{p^m}^* \to \mathbb{F}_{p^m}$ dado por $x \mapsto x + \dfrac{b}{x}$ es de grado 2 sobre $\mathbb{F}_{p^m}^* \smallsetminus \{c, -c\}$.

(b) El mapa $\beta : \mu_{p^m+1} \to \mathbb{F}_{p^m}$ dado por $u \mapsto au + \dfrac{b}{au}$ es de grado 2 sobre $\mu_{p^m+1} \smallsetminus \{\frac{c}{a}, -\frac{c}{a}\}$.

(c) $\alpha(\mathbb{F}_{p^m}^*) \cap \beta(\mu_{p^m+1}) = \{2c, -2c\}$ y $\alpha(\mathbb{F}_{p^m}^*) \cup \beta(\mu_{p^m+1}) = \mathbb{F}_{p^m}^*$.

En efecto, si $\alpha(x) = \alpha(y)$ entonces $x = y$ o $b = xy$ y esta vez podemos tener $x^2 = b$. El segundo ítem es análogo. Si $\alpha(x) = \beta(u)$ entonces $a = \frac{x}{u}$ o $a = \frac{b}{ux}$. Esto implica que $x = \pm c$ y $u = \pm\zeta$. El resto sigue contando elementos.

La ecuación

$$s + t = 2p^{m+1}$$

es consecuencia inmediata de (a), (b) y (c) (en ambos casos, respectivamente) y del hecho de que uno de cada p elementos de $\mathbb{F}_{p^m}$ tiene traza cero. $\square$

Este resultado implica una relación entre los pesos de las palabras de dos códigos diferentes. Consideramos ahora el código lineal sobre $\mathbb{F}_p$ en el $\mathbb{F}_p$-espacio vectorial

$$V = \{f : \mathbb{F}_{p^m}^* \to \mathbb{F}_p \ : \ f \text{ es } \mathbb{F}_p\text{-lineal}\}$$

dado por

$$C = \{c_b \in V \ : \ c_b(x) = \mathrm{Tr}(bx + x^{-1}), b \in \mathbb{F}_{p^m}\}$$

y definimos el código lineal sobre $\mathbb{F}_p$ en el $\mathbb{F}_p$-espacio vectorial $W = \{f : \mu_{p^m+1} \to \mathbb{F}_p\}$ por

$$D = \{d_a \in W \ : \ d_a(x) = \mathrm{Tr}(ax), a \in \mathbb{F}_{p^{2m}}\}.$$

El teorema anterior asegura que

$$w(d_a) + w(c_b) = 2p^{m-1}(p-1).$$

Esto es útil para encontrar la distribución de pesos de códigos de Zetterberg para $p \geq 3$. Lo usamos ahora en el caso ternario.

6.3 Caso ternario

Consideremos el caso $p = 3$. Sean $m \geq 1$ y $q = 3^m$. Tenemos que

$$Z_3(m)^\perp = \{\mathrm{Tr}(ax)_{x \in \mu_{q+1}} \ : \ a \in \mathbb{F}_{q^2}\}.$$

A continuación damos la distribución de pesos de $Z_3(m)^\perp$.

Teorema 6.4. *Los pesos no triviales del dual del código de Zetterberg ternario, $Z_3(m)^\perp$, y sus respectivas frecuencias están dados por*

$$w_t = \tfrac{2}{3}(q + 1 - t) \qquad y \qquad A_{w_t} = (q+1)H(t^2 - 4q),$$

donde $t \in \mathbb{Z}$, $t^2 < 4q$ y $t \equiv 1 \pmod 3$.

Demostración. Sea α un generador de $\mathbb{F}_{q^2}^*$. Es suficiente considerar los pesos $w(c(\alpha^j))$ de las palabras

$$c(\alpha^j) = \big(\mathrm{Tr}(\alpha^j x)\big)_{x \in \mu_{q+1}}, \qquad 0 \leq j \leq q-2.$$

Tenemos que contarlos con multiplicidad $q-1$ pues multiplicando α^j por un elemento de μ_{q+1} permuta las coordenadas de la palabra código. Tenemos que

$$w(c(\alpha^j)) = q + 1 - \#\{x \in \mu_{q+1} \ : \ \mathrm{Tr}(\alpha^j x) = 0\} = q + 1 - t.$$

La palabra $c(\alpha^j)$ se corresponde, según lo que vimos en la sección anterior, con la palabra

$$c(\beta^j) = \left(\mathrm{Tr}(\beta^j x + x^{-1})\right)_{x \in \mathbb{F}_q^*}$$

en $M_3(m)^\perp$, donde $\beta = \alpha^{q+1}$. Su peso es $q - 1 - s$ y se tiene que

$$s + t = \tfrac{2}{3}q.$$

Se sigue que

$$w(c(\alpha^j)) = \tfrac{4}{3}q - w(c(\beta^j)),$$

lo que prueba el teorema. □

Usando el teorema de la sección anterior podemos expresar el enumerador de pesos del código de Zetterberg ternario $Z_3(m)$ en términos del enumerador de pesos del código de Melas ternario $M_3(m)$. Resulta que

$$\begin{aligned} \tfrac{q^2}{q+1}(1+2x)^{q'-1} W_{Z_3(m)}(x) &= \tfrac{q^2}{q-1}(1-x)^{q'+1}(1+x)^{q-1} W_{M_3(m)}(x)(\tfrac{-x}{x+1}) \\ &\quad -2(1+2x)^{2q'}(1-x)^{2q'} - \tfrac{1}{q-1}(1-x)^{4q'} + \tfrac{1}{q+1}(1+2x)^{4q'}, \end{aligned}$$

donde $q' = \frac{q}{3}$.

Epílogo

En este trabajo hemos hablado de diversos temas que se relacionan entre sí y dan lugar a interesantes resultados. Éstos nos llevan a pensar en otros problemas que, si bien el trabajo ya es bastante extenso, vale la pena al menos mencionar.

A continuación, se enumeran algunas de las preguntas que nos hicimos y nos proponemos pensar más adelante.

(1) En la Sección 4.2, damos la distribución de pesos de los códigos BCH. En el caso binario, al establecer la relación con ciertas Sumas de Weil encontramos cuáles son los pesos de las palabras del código, pero no la frecuencia con la que ocurren los distintos pesos. Esto último, lo encontramos luego usando curvas elípticas. Nos interesa pensar en la forma de obtener el espectro del código utilizando solo Sumas de Weil.

(2) En el Capítulo 5, damos, en primer lugar, una relación entre los pesos de las palabras del código de Melas y ciertas sumas de Kloosterman, que no son conocidas. Luego, obtenemos el espectro de este código a partir de una curva elíptica. Nos gustaría pensar si conocer esta distribución de pesos nos da alguna informació sobre el valor de las sumas de Kloosterman con las que se relaciona el código.

(3) A partir de los resultados obtenidos por Coulter ([7],[8],[9]) sabemos que las sumas de Weil con funciones de la forma

$$F(x) = f(x) + L(x),$$

donde $f(x)$ está fijo y $L(x)$ es un polinomio linealizado, tienen el mismo resultado. Por lo tanto, si construimos códigos cíclicos a partir de estas funciones, estos codigos serán distintos (genéricamente no isomorfos) pero isospectrales. Es decir, podemos construir una familia de códigos cíclicos que tienen el mismo espectro.

Apéndice A

Ejemplos

A.1 Hamming $H_2(3)$

Notemos en primer lugar que la distribución de pesos de este código se puede conocer fácilmente. Tiene una palabra de peso cero, lo que nos dice que $A_0 = 1$, y la distancia mínima es $d = 3$, por lo que $A_1 = A_2 = 0$. Por otro lado, es conocido que la distribución de pesos de los códigos Hamming es simétrica, entonces

$$A_7 = A_0 = 1, \quad A_6 = A_1 = 0, \quad A_5 = A_2 = 0 \quad \text{y} \quad A_3 = A_4.$$

Además, el código tiene $2^4 = 16$ palabras. Entonces $A_3 = A_4 = 7$.

De igual manera, calculamos esta distribución usando los distintos caminos propuestos para analizar la dificultad de cada uno y las diferencias entre ellos.

Como código lineal.

Consideramos el código $H_2(3)$ como un código lineal con parámetros $n = 7$, $k = 4$ y $d = 3$. Como vimos, éste es un código de género a lo sumo $g = m - 2 = 1$. Tenemos la representación del polinomio enumerador de pesos de la forma

$$W_C(x) = x^n + \sum_{i=0}^{4} B_i (x-1)^i.$$

Luego, el Teorema 3.3 nos dice que

$$B_i = \tbinom{7}{i}(2^{4-i} - 1),$$

para $i \leq 3$,

$$\max\{0, \tbinom{7}{i}(2^{4-i} - 1)\} \leq B_i \leq \tbinom{7}{i}(2^{5-i} - 1),$$

para $i = 4$. Entonces, se tiene que

$$B_0 = \tbinom{7}{0}(2^4 - 1) = 15,$$

$$B_1 = \tbinom{7}{1}(2^3 - 1) = 49,$$

$$B_2 = \tbinom{7}{2}(2^2 - 1) = 63,$$

$$B_3 = \tbinom{7}{3}(2 - 1) = 35,$$

$$0 \leq \quad B_4 \leq \tbinom{7}{4}(2 - 1) = 35.$$

Ahora, sabemos que se cumple

$$A_i = \sum_{j=7-i}^{4} (-1)^{7+i+j} \tbinom{j}{7-i} B_j,$$

para $i \geq 3$. Por lo tanto, la distribución de pesos de $H_2(3)$ se calcula como sigue.

$$\begin{aligned}
A_0 &= 1, \quad \text{pues la palabra cero está en el código,} \\
A_1 &= A_2 = 0, \quad \text{pues la distancia mínima es 3,} \\
A_3 &= \tbinom{4}{4} B_4, \\
A_4 &= \tbinom{3}{3} B_3 - \tbinom{4}{3} B_4 = 35 - 4B_4, \\
A_5 &= \tbinom{2}{2} B_2 - \tbinom{3}{2} B_3 + \tbinom{4}{2} B_4 = -42 + 6B_4, \\
A_6 &= \tbinom{1}{1} B_1 - \tbinom{2}{1} B_2 + \tbinom{3}{1} B_3 - \tbinom{4}{1} B_4 = 28 - 4B_4, \\
A_7 &= \tbinom{0}{0} B_0 - \tbinom{1}{0} B_1 + \tbinom{2}{0} B_2 - \tbinom{3}{0} B_3 + \tbinom{4}{0} B_4 = -6 + B_4.
\end{aligned}$$

Es conocido que el espectro de los códigos Hamming es simétrico, es decir que

$$A_i = A_{7-1}, \quad \text{para todo} \quad i = 0, 1, \ldots 7.$$

Como $A_0 = A_7$, entonces

$$1 = -6 + B_4,$$

lo que me dice que $B_4 = 7$.

Como dual del código simplex

Consideramos ahora al código $H_2(3)$ como un código cíclico. Sabemos que

$$A_0^\perp = 1, \quad A_4^\perp = 7 \quad \text{y} \quad A_i^\perp = 0 \quad \text{si} \quad i \neq 0, 4.$$

Además $|C^\perp| = 8$, y tenemos que

$$A_k = \frac{1}{|C^\perp|} \sum_{j=0}^{n} A_j^\perp K_k(j) = \tfrac{1}{8}\big(K_k(0) + 7K_k(4)\big).$$

Podemos calcular los polinomios de Krawtchouk de dos formas distintas, por definición o a partir de la recurrencia que satisfacen. Los calcularemos en este caso usando la recurrencia.

$$\begin{aligned}
K_0(x) &= 1,\\
K_1(x) &= 7-2x,\\
K_2(x) &= (7-2x)K_1(x)-7K_0(x) = 2x^2-14x+21,\\
K_3(x) &= (7-2x)K_2(x)-6K_1(x) = \tfrac{1}{3}(-4x^3+42x^2-128x+105),\\
K_4(x) &= (7-2x)K_3(x)-5K_2(x) = \tfrac{1}{3}(2x^4-28x^3+130x^2-224x+105),\\
K_5(x) &= (7-2x)K_4(x)-4K_3(x) = \tfrac{1}{15}(-4x^5+70x^4-440x^3+1190x^2-1266x+315),\\
K_6(x) &= (7-2x)K_5(x)-3K_4(x)\\
&= \tfrac{1}{90}(8x^6-168x^5+1340x^4-5040x^3+8912x^2-6132x+630),\\
K_7(x) &= (7-2x)K_6(x)-2K_5(x)\\
&= \tfrac{1}{630}(-16x^7+392x^6-3808x^5+18620x^4-47824x^3+60368x^2-28992x+630).
\end{aligned}$$

Luego, se tiene que

$$\begin{aligned}
A_0 &= \tfrac{1}{8}\{K_0(0)+7K_0(4)\} = \tfrac{1}{8}(1+7) = 1,\\
A_1 &= \tfrac{1}{8}\{K_1(0)+7K_1(4)\} = \tfrac{1}{8}(7+7\cdot(-1)) = 0,\\
A_2 &= \tfrac{1}{8}\{K_2(0)+7K_2(4)\} = \tfrac{1}{8}(21+7\cdot(-3)) = 0,\\
A_3 &= \tfrac{1}{8}\{K_3(0)+7K_3(4)\} = \tfrac{1}{8}(35+7\cdot 3) = 7,\\
A_4 &= \tfrac{1}{8}\{K_4(0)+7K_4(4)\} = \tfrac{1}{8}(35+7\cdot 3) = 7,\\
A_5 &= \tfrac{1}{8}\{K_5(0)+7K_5(4)\} = \tfrac{1}{8}(21+7\cdot(-3)) = 0,\\
A_6 &= \tfrac{1}{8}\{K_6(0)+7K_6(4)\} = \tfrac{1}{8}(7+7\cdot(-1)) = 0,\\
A_7 &= \tfrac{1}{8}\{K_7(0)+7K_7(4)\} = \tfrac{1}{8}(1+7\cdot 1) = 1.
\end{aligned}$$

Notemos que la distribución encontrada, en ambos casos, es la que ya habíamos mencionado.

A.2 Hamming $H_2(4)$

Como dual del Simplex

Conocemos la distribución de pesos de $H_2(4)^\perp$, entonces tenemos que

$$A_i = \frac{1}{|H_2(3)^\perp|}\sum_{j=0}^{n} A_j^\perp K_i(j) = \tfrac{1}{16}\big(K_i(0)+15K_i(8)\big).$$

En este caso calculamos los $K_i(j)$ por definición. Para $j=0$ se tiene

$$K_i(0) = \tbinom{15}{i},$$

entonces

$K_0(0) = 1$, $K_4(0) = 1365$, $K_8(0) = 6435$, $K_{12}(0) = 455$,
$K_1(0) = 15$, $K_5(0) = 3003$, $K_9(0) = 5005$, $K_{13}(0) = 105$,
$K_2(0) = 105$, $K_6(0) = 5005$, $K_{10}(0) = 3003$, $K_{14}(0) = 15$,
$K_3(0) = 455$, $K_7(0) = 6435$, $K_{11}(0) = 1365$, $K_{15}(0) = 1$,

y para $j = 8$, se tiene que

$$K_i(8) = \sum_{k=1}^{i} (-1)^k \binom{8}{k} \binom{7}{i-k},$$

entonces

$$K_0(8) = \binom{8}{0}\binom{7}{0} = 1,$$
$$K_1(8) = \binom{8}{0}\binom{7}{1} - \binom{8}{1}\binom{7}{0} = -1,$$
$$K_2(8) = \binom{8}{0}\binom{7}{2} - \binom{8}{1}\binom{7}{1} + \binom{8}{2}\binom{7}{0} = -7,$$
$$K_3(8) = \binom{8}{0}\binom{7}{3} - \binom{8}{1}\binom{7}{2} + \binom{8}{2}\binom{7}{1} - \binom{8}{3}\binom{7}{0} = 7,$$
$$K_4(8) = \binom{8}{0}\binom{7}{4} - \binom{8}{1}\binom{7}{3} + \binom{8}{2}\binom{7}{2} - \binom{8}{3}\binom{7}{1} + \binom{8}{4}\binom{7}{0} = 21,$$
$$K_5(8) = \binom{8}{0}\binom{7}{5} - \binom{8}{1}\binom{7}{4} + \binom{8}{2}\binom{7}{3} - \binom{8}{3}\binom{7}{2} + \binom{8}{4}\binom{7}{1} - \binom{8}{5}\binom{7}{0} = -21,$$
$$K_6(8) = \binom{8}{0}\binom{7}{6} - \binom{8}{1}\binom{7}{5} + \binom{8}{2}\binom{7}{4} - \binom{8}{3}\binom{7}{3} + \binom{8}{4}\binom{7}{2} - \binom{8}{5}\binom{7}{1} + \binom{8}{6}\binom{7}{0} = -35,$$
$$K_7(8) = \binom{8}{0}\binom{7}{7} - \binom{8}{1}\binom{7}{6} + \binom{8}{2}\binom{7}{5} - \binom{8}{3}\binom{7}{4} + \binom{8}{4}\binom{7}{3} - \binom{8}{5}\binom{7}{2} + \binom{8}{6}\binom{7}{1} - \binom{8}{7}\binom{7}{0} = 35,$$
$$K_8(8) = -\binom{8}{1}\binom{7}{7} + \binom{8}{2}\binom{7}{6} - \binom{8}{3}\binom{7}{5} + \binom{8}{4}\binom{7}{4} - \binom{8}{5}\binom{7}{3} + \binom{8}{6}\binom{7}{2} - \binom{8}{7}\binom{7}{1} + \binom{8}{8}\binom{7}{0} = 35,$$
$$K_9(8) = \binom{8}{2}\binom{7}{7} - \binom{8}{3}\binom{7}{6} + \binom{8}{4}\binom{7}{5} - \binom{8}{5}\binom{7}{4} + \binom{8}{6}\binom{7}{3} - \binom{8}{7}\binom{7}{2} + \binom{8}{8}\binom{7}{1} = -35,$$
$$K_{10}(8) = -\binom{8}{3}\binom{7}{7} + \binom{8}{4}\binom{7}{6} - \binom{8}{5}\binom{7}{5} + \binom{8}{6}\binom{7}{4} - \binom{8}{7}\binom{7}{3} + \binom{8}{8}\binom{7}{2} = -21,$$
$$K_{11}(8) = \binom{8}{4}\binom{7}{7} - \binom{8}{5}\binom{7}{6} + \binom{8}{6}\binom{7}{5} - \binom{8}{7}\binom{7}{4} + \binom{8}{8}\binom{7}{3} = 21,$$
$$K_{12}(8) = -\binom{8}{5}\binom{7}{7} + \binom{8}{6}\binom{7}{6} - \binom{8}{7}\binom{7}{5} + \binom{8}{8}\binom{7}{4} = 7,$$
$$K_{13}(8) = \binom{8}{6}\binom{7}{7} - \binom{8}{7}\binom{7}{6} + \binom{8}{8}\binom{7}{5} = -7,$$
$$K_{14}(8) = -\binom{8}{7}\binom{7}{7} + \binom{8}{8}\binom{7}{6} = -1,$$
$$K_{15}(8) = \binom{8}{8}\binom{7}{7} = 1.$$

Ahora si, calculamos la distribución de pesos.

$A_0 = \frac{1}{16}(1 + 15) = 1$, $A_8 = \frac{1}{16}(6435 + 15 \cdot 35) = 435$,
$A_1 = \frac{1}{16}(15 + 15 \cdot (-1)) = 0$, $A_9 = \frac{1}{16}(5005 + 15 \cdot (-35)) = 280$,
$A_2 = \frac{1}{16}(105 + 15 \cdot (-7)) = 0$, $A_{10} = \frac{1}{16}(3003 + 15 \cdot (-21)) = 168$,
$A_3 = \frac{1}{16}(455 + 15 \cdot 7) = 35$, $A_{11} = \frac{1}{16}(1365 + 15 \cdot 21) = 105$,
$A_4 = \frac{1}{16}(1365 + 15 \cdot 21) = 105$, $A_{12} = \frac{1}{16}(455 + 15 \cdot 7) = 35$,
$A_5 = \frac{1}{16}(3003 + 15 \cdot (-21)) = 168$, $A_{13} = \frac{1}{16}(105 + 15 \cdot (-7)) = 0$,
$A_6 = \frac{1}{16}(5005 + 15 \cdot (-35)) = 280$, $A_{14} = \frac{1}{16}(15 + 15 \cdot (-1)) = 0$,
$A_7 = \frac{1}{16}(6435 + 15 \cdot 35) = 435$, $A_{15} = \frac{1}{16}(1 + 15) = 1$.

A.3 BCH $B_2(3)$

Cómo código lineal

Consideramos el código $B_2(3)$ como un código lineal de parámetros $n = 7$, $k = 1$, $d = 5$. Este código es de género a lo sumo $g = 2$. Su enumerador de pesos se puede escribir como

$$W_C(x) = x^n + \sum_{i=0}^{a} B_i(x-1)^i,$$

con $a = k + g - 1 = 2$.

El teorema nos dice que

$$\max\{0, \tbinom{7}{i}(2^{1-i} - 1)\} \leq B_i \leq \tbinom{7}{i}(2^3 - 1),$$

para $0 \leq i \leq 2$. Entonces se tiene

$$1 = \max\{0, \tbinom{7}{0}(2^1 - 1)\} \leq B_0 \quad \leq \tbinom{7}{0}(2^3 - 1) = 7,$$

$$0 = \max\{0, \tbinom{7}{1}(2^0 - 1)\} \leq B_1 \quad \leq \tbinom{7}{1}(2^2 - 1) = 21,$$

$$0 = \max\left\{0, \tbinom{7}{2}(2^{-1} - 1)\right\} \leq B_2 \quad \leq \tbinom{7}{2}(2^1 - 1) = 21.$$

Recordando que $d = 5$ y la relación entre los números A_i y B_i, tenemos que

$$A_0 = 1, \qquad A_1 = A_2 = A_3 = A_4 = 0$$

y las ecuaciones

$$A_5 = \sum_{j=2}^{2}(-1)^{7+5+j}\tbinom{j}{2}B_j = B_2,$$

$$A_6 = \sum_{j=1}^{2}(-1)^{7+6+j}\tbinom{j}{1}B_j = B_1 - 2B_2,$$

$$A_7 = \sum_{j=0}^{2}(-1)^{7+7+j}\tbinom{j}{0}B_j = B_0 - B_1 + B_2.$$

Es conocido que la distribución de pesos de los códigos BCH es simétrica, entonces tenemos el sistema de ecuaciones

$$\begin{cases} 0 = A_2 = A_5 = B_2, \\ 0 = A_1 = A_6 = B_1 - 2B_2, \\ 1 = A_0 = A_7 = B_0 - B_1 + B_2 \end{cases}$$

Luego,

$$B_0 = 1, \quad B_1 = 0 \quad \text{y} \quad B_2 = 0.$$

La distribución de pesos del código BCH $B_2(3)$ es entonces

$$A_1 = A_2 = A_3 = A_4 = A_5 = A_6 = 0 \qquad \text{y} \qquad A_0 = A_7 = 1.$$

Por curvas

La fórmula que obtuvimos para los números A_i es

$$64A_i = K_i(0) + 7K_i(6) + 35K_i(4) + 21K_i(2),$$

donde $K_i(x)$ son los polinomios de Krawtchouk para $n = 7$ y $p = 2$. Estos polinomios ya los dimos de manera explícita cuando calculamos la distribución de pesos del código Hamming $H_2(3)$ por curvas.

Teniendo en cuenta los polinomios ya calculados, tenemos que

$$\begin{aligned}
A_0 &= \tfrac{1}{64}(1 + 7 + 35 + 21) = 1,\\
A_1 &= \tfrac{1}{64}(7 + 7\cdot(-5) + 35\cdot(-1) + 21\cdot 3) = 0,\\
A_2 &= \tfrac{1}{64}(21 + 7\cdot 9 + 35\cdot(-3) + 21\cdot(-5)) = 0,\\
A_3 &= \tfrac{1}{64}(35 + 7\cdot(-5) + 35\cdot 3 + 21\cdot(-5)) = 0,\\
A_4 &= \tfrac{1}{64}(35 + 7\cdot(-5) + 35\cdot 3 + 21\cdot(-5)) = 0,\\
A_5 &= \tfrac{1}{64}(21 + 7\cdot 9 + 35\cdot(-3) + 21) = 0,\\
A_6 &= \tfrac{1}{64}(7 + 7\cdot(-5) + 35\cdot(-1) + 21\cdot 3) = 0,\\
A_7 &= \tfrac{1}{64}(7 + 7 + 35 + 21) = 1.
\end{aligned}$$

A.4 Melas $M_2(3)$

Veremos la distribución de pesos del código Melas $M_2(3)$. La dimensión de este código es

$$k = q - 1 - 2m = 8 - 1 - 6 = 1,$$

entonces, el código tiene dos palabras.

Esto nos dice que la distribución de pesos es

$$A_0 = 1, \qquad A_1 = A_2 = A_3 = A_4 = A_5 = A_6 = 0, \qquad A_7 = 1.$$

Calculemos ahora usando el teorema. Primero, vamos a encontrar los valores de las $\tau_k(8) = \mathrm{Tr}(T_k)$. Sabemos que si $k \neq 2$,

$$\mathrm{Tr}(T_k) = -1 - \sum_{t\in D} Q_{k-2}(t,8)\, H(t^2 - 32),$$

donde

$$D = \{t \in \mathbb{Z} : t^2 < 32,\, t \equiv 1 \pmod 4\} = \{-3, 1, 5\},$$

y $Q_{k-2}(t,8)$ está definido por:

$$Q_0(t,8) = 1, \qquad Q_1(t,8) = t, \qquad Q_{k+1}(t,8) = tQ_k(t,8) - 8Q_{k-1}(t,8).$$

Calculemos los polinomios $Q_{k-2}(t,8)$.

$$
\begin{aligned}
Q_2(t,8) &= tQ_1(t,8) - 8Q_0(t,8) = t^2 - 8.\\
Q_3(t,8) &= tQ_2(t,8) - 8Q_1(t,8) = t^3 - 16t.\\
Q_4(t,8) &= tQ_3(t,8) - 8Q_2(t,8) = t^4 - 24t^2 + 64.\\
Q_5(t,8) &= tQ_4(t,8) - 8Q_3(t,8) = t^5 - 32t^3 + 192t.\\
Q_6(t,8) &= tQ_5(t,8) - 8Q_4(t,8) = t^6 - 40t^4 + 384t^2 - 512.\\
Q_7(t,8) &= tQ_6(t,8) - 8Q_5(t,8) = t^7 - 48t^5 + 640t^3 - 2048t.
\end{aligned}
$$

Además, por lo visto en la Sección 1.4, tenemos que

$$H(-23) = 3, \qquad H(-31) = 3 \qquad \text{y} \qquad H(-7) = 1.$$

Entonces se tiene que

$$
\begin{aligned}
\tau_3(8) &= -1 - \{Q_1(-3,8)H(-23) + Q_1(1,8)H(-31) + Q_1(5,8)H(-7)\}\\
&= -1 - (-3\cdot 3 + 1\cdot 3 + 5\cdot 1) = 0,\\
\tau_4(8) &= -1 - \{Q_2(-3,8)H(-23) + Q_2(1,8)H(-31) + Q_2(5,8)H(-7)\}\\
&= -1 - (1\cdot 3 - 7\cdot 3 + 17\cdot 1) = 0,\\
\tau_5(8) &= -1 - \{Q_3(-3,8)H(-23) + Q_3(1,8)H(-31) + Q_3(5,8)H(-7)\}\\
&= -1 - (21\cdot 3 - 15\cdot 3 + 45\cdot 1) = -64,\\
\tau_6(8) &= -1 - [Q_4(-3,8)H(-23) + Q_4(1,8)H(-31) + Q_4(5,8)H(-7)]\\
&= -1 - [-71\cdot 3 + 41\cdot 3 + 89\cdot 1] = 0,\\
\tau_7(8) &= -1 - [Q_5(-3,8)H(-23) + Q_5(1,8)H(-31) + Q_5(5,8)H(-7)]\\
&= -1 - [45\cdot 3 + 161\cdot 3 + 85\cdot 1] = -704,\\
\tau_8(8) &= -1 - [Q_6(-3,8)H(-23) + Q_6(1,8)H(-31) + Q_6(5,8)H(-7)]\\
&= -1 - [433\cdot 3 - 157\cdot 3 - 287\cdot 1] = -512,\\
\tau_9(8) &= -1 - [Q_7(-3,8)H(-23) + Q_7(1,8)H(-31) + Q_7(5,8)H(-7)]\\
&= -1 - [-1659\cdot 3 - 1455\cdot 3 - 2115\cdot 1] = 11456.
\end{aligned}
$$

Ahora, calculamos los valores $W_{i,j}(8)$

$W_{0,0}(8) = 1,$
$W_{1,1}(8) = -1,$
$W_{2,0}(8) = \frac{1}{2}(-8W_{1,1}(8) - W_{1,-1}(8) - 7W_{0,0}(8)) = \frac{1}{2}(-8(-1) - 7) = \frac{1}{2},$
$W_{2,2}(8) = \frac{1}{2}(-8W_{1,3}(8) - W_{1,1}(8) - 7W_{0,2}(8)) = \frac{1}{2}(-(-1)) = \frac{1}{2},$
$W_{3,1}(8) = \frac{1}{3}(-8W_{2,2}(8) - W_{2,0}(8) - 6W_{1,1}(8)) = \frac{1}{3}(-8\frac{1}{2} - \frac{1}{2} - 6(-1)) = \frac{1}{2},$
$W_{3,3}(8) = \frac{1}{3}(-8W_{2,4}(8) - W_{2,2}(8) - 6W_{1,3}(8)) = \frac{1}{3}(-\frac{1}{2}) = -\frac{1}{6},$
$W_{4,0}(8) = \frac{1}{4}(-8W_{3,1}(8) - W_{3,-1}(8) - 5W_{2,0}(8)) = \frac{1}{4}(-8\frac{1}{2} - 5\frac{1}{2}) = -\frac{13}{8},$
$W_{4,2}(8) = \frac{1}{4}(-8W_{3,3}(8) - W_{3,1}(8) - 5W_{2,2}(8)) = \frac{1}{4}(-8\frac{1}{6} - \frac{1}{2} - 5\frac{1}{2}) = -\frac{5}{12},$
$W_{4,4}(8) = \frac{1}{4}(-8W_{3,5}(8) - W_{3,3}(8) - 5W_{2,4}(8)) = \frac{1}{4}(-\frac{1}{6}) = \frac{1}{24},$
$W_{5,1}(8) = \frac{1}{5}(-8W_{4,2}(8) - W_{4,0}(8) - 4W_{3,1}(8)) = \frac{1}{5}(-8(-\frac{5}{12} - (-\frac{13}{8}) - 5\frac{1}{2})) = \frac{71}{120},$
$W_{5,3}(8) = \frac{1}{5}(-8W_{4,4}(8) - W_{4,2}(8) - 4W_{3,3}(8)) = \frac{1}{5}(-8\frac{1}{24} - (-\frac{5}{12}) - 4(-\frac{1}{6})) = \frac{3}{20},$
$W_{5,5}(8) = \frac{1}{5}(-8W_{4,6}(8) - W_{4,4}(8) - 4W_{3,5}(8)) = \frac{1}{5}(-\frac{1}{24}) = -\frac{1}{120},$
$W_{6,0}(8) = \frac{1}{6}(-8W_{5,1}(8) - W_{5,-1}(8) - 3W_{4,0}(8)) = \frac{1}{6}(-8\frac{71}{120} - 3(-\frac{13}{8})) = \frac{17}{720},$
$W_{6,2}(8) = \frac{1}{6}(-8W_{5,3}(8) - W_{5,1}(8) - 3W_{4,2}(8)) = \frac{1}{6}(-8\frac{3}{20} - \frac{71}{120} - 3(-\frac{5}{12})) = -\frac{65}{720},$
$W_{6,4}(8) = \frac{1}{6}(-8W_{5,5}(8) - W_{5,3}(8) - 3W_{4,4}(8)) = \frac{1}{6}(-8(-\frac{1}{120}) - \frac{3}{20} - 3\frac{1}{24}) = -\frac{25}{720},$
$W_{6,6}(8) = \frac{1}{6}(-8W_{5,7}(8) - W_{5,5}(8) - 3W_{4,6}(8)) = \frac{1}{6}(-(-\frac{1}{120})) = \frac{1}{720},$
$W_{7,1}(8) = \frac{1}{7}(-8W_{6,2}(8) - W_{6,0}(8) - 2W_{5,1}(8)) = \frac{1}{7}(-8(-\frac{65}{720}) - \frac{17}{120} - 2\frac{71}{120}) = -\frac{349}{5040},$
$W_{7,3}(8) = \frac{1}{7}(-8W_{6,4}(8) - W_{6,2}(8) - 2W_{5,3}(8)) = \frac{1}{7}(-8(-\frac{25}{720}) - (-\frac{65}{720}) - 2\frac{3}{20}) = \frac{49}{5040},$
$W_{7,5}(8) = \frac{1}{7}(-8W_{6,6}(8) - W_{6,4}(8) - 2W_{5,5}(8)) = \frac{1}{7}(-8\frac{1}{720} - (-\frac{25}{720}) - 2(-\frac{1}{120})) = \frac{29}{5040},$
$W_{7,7}(8) = \frac{1}{7}(-8W_{6,8}(8) - W_{6,6}(8) - 2W_{5,7}(8)) = \frac{1}{7}(-\frac{1}{720}) = -\frac{1}{5040}.$

Ahora si calculamos la distribución de pesos

$$64A_0 = \binom{7}{0} + 2\cdot 1\cdot 7\binom{3}{0} - 7(W_{0,0}(8)(1+\tau_2(8)) = 1 + 14 - 7(1(1-8)) = 64,$$

$$64A_1 = \binom{7}{1} + 2(-1)7\binom{3}{0} - 7(W_{1,1}(8)(1+\tau_3(8))) = 7 - 14 - 7(-1(1+0)) = 7 - 14 + 7 = 0,$$

$$\begin{aligned}64A_2 &= \binom{7}{2} + 2(-1)7\binom{3}{1} - 7(W_{2,0}(8)(1+\tau_2(8)) + W_{2,2}(8)(1+\tau_4(8)))\\ &= 21 - 42 - 7(\tfrac{1}{2}(1-8) + \tfrac{1}{2}(1+0)) = 21 - 42 - 7\cdot(-3) = 0,\end{aligned}$$

$$\begin{aligned}64A_3 &= \binom{7}{3} + 2.1.7\binom{3}{1} - 7(W_{3,1}(8)(1+\tau_3(8)) + W_{3,3}(8)(1+\tau_5(8)))\\ &= 35 + 42 - 7(\tfrac{1}{2}(1+0) - \tfrac{1}{6}(1-64)) = 35 + 42 - 7\cdot 11 = 0,\end{aligned}$$

$$\begin{aligned}64A_4 &= \binom{7}{4} + 2\cdot 1\cdot 7\binom{3}{2} - 7(W_{4,0}(8)(1+\tau_2(8)) + W_{4,2}(8)(1+\tau_4(8)) + W_{4,4}(8)(1+\tau_6(8)))\\ &= 35 + 42 - 7(-\tfrac{13}{8}(1-8) - \tfrac{15}{2}(1+0) + \tfrac{1}{24}(1+0)) = 35 + 42 - 7\cdot 11 = 0,\end{aligned}$$

$$\begin{aligned}64A_5 &= \binom{7}{5} + 2(-1)7\binom{3}{2} - 7(W_{5,1}(8)(1+\tau_3(8)) + W_{5,3}(8)(1+\tau_5(8)) + W_{5,5}(8)(1+\tau_7(8)))\\ &= 21 - 42 - 7(\tfrac{71}{120}(1+0) + \tfrac{3}{20}(1-64) - \tfrac{1}{120}(1-704)) = 21 - 42 - 7\cdot(-3) = 0,\end{aligned}$$

$$\begin{aligned}64A_6 &= \binom{7}{6} - 2(-1)7\binom{3}{3} - 7(W_{6,0}(8)(1+\tau_2(8)) + W_{6,2}(8)(1+\tau_4(8)) + W_{6,4}(8)(1+\tau_6(8))\\ &\quad + W_{6,6}(8)(1+\tau_8(8)))\\ &= 7 - 14 - 7(\tfrac{17}{720}(1-8) - \tfrac{65}{720}(1+0) - \tfrac{25}{720}(1+0) + \tfrac{1}{720}(1-512))\\ &= 7 - 14 - 7\cdot(-1) = 0,\end{aligned}$$

$$\begin{aligned}64A_7 &= \binom{7}{7} + 2\cdot 1\cdot 7\binom{3}{3} - 7(W_{7,1}(8)(1+\tau_3(8)) + W_{7,3}(8)(1+\tau_5(8)) + W_{7,5}(8)(1+\tau_7(8))\\ &\quad + W_{7,7}(8)(1+\tau_9(8)))\\ &= 7 + 14 - 7(-\tfrac{349}{5040}(1+0) + \tfrac{49}{5040}(1-64) + \tfrac{29}{5040}(1-704) - \tfrac{1}{5040}(1+11456))\\ &= 1 + 14 - 7\cdot(-7) = 64.\end{aligned}$$

Luego, la distribución de pesos del código $M_2(3)$ es efectivamente la que mencionamos antes.

A.5 Melas $M_2(4)$

Encontraremos la distribución de pesos del código de Melas $M_2(4)$. La dimensión de este código es

$$k = q - 1 - 2m = 16 - 1 - 8 = 7.$$

Esto nos dice que el código tiene 2^7 palabras. A diferencia del ejemplo anterior, ahora no es claro, solo con esta información, cuál es la distribución de pesos del código.

Calculemos. Primero vamos a encontrar los valores de las $\tau_k(16)$. Sabemos que

$$\mathrm{Tr}(T_k) = -1 - \sum_{t\in D} Q_{k-2}(t,16)H(t^2-64), \quad \text{si} \quad k \neq 2,$$

donde

$$D = \{t \in \mathbb{Z} \,:\, t^2 < 64,\, t \equiv 1 \pmod 4\} = \{< 7, -3, 1, 5\}$$

y $Q_{k-2}(t,16)$ está definido por

$$Q_0(t,16)=1,\quad Q_1(t,16)=t,\quad Q_{k+1}(t,16)=-tQ_k(t,16)-16Q_{k-1}(t,16).$$

Calculamos los polinomios $Q_{k-2}(t,16)$ evaluados en cada t.

$$\begin{aligned}
&Q_0(-7,16)=1,\\
&Q_0(-3,16)=1,\\
&Q_0(1,16)=1,\\
&Q_0(5,16)=1,\\
&Q_1(-7,16)=-7,\\
&Q_1(-3,16)=-3,\\
&Q_1(1,16)=1,\\
&Q_1(5,16)=5,\\
&Q_2(-7,16)=-7(-7)-16=33,\\
&Q_2(-3,16)=-3(-3)-16=-7,\\
&Q_2(1,16)=1-16=-15,\\
&Q_2(5,16)=5\cdot 5-16=9,\\
&Q_3(-7,16)=-7\cdot 33-16(-7)=-119,\\
&Q_3(-3,16)=-3(-7)-16(-3)=69,\\
&Q_3(1,16)=-15-16=-31,\\
&Q_3(5,16)=5\cdot 9-16\cdot 5=-35,\\
&Q_4(-7,16)=-7(-119)-16\cdot 33=305,\\
&Q_4(-3,16)=-3\cdot 69-16(-7)=-95,\\
&Q_4(1,16)=-31-16(-15)=209,\\
&Q_4(5,16)=5(-35)-16\cdot 9=-319,\\
&Q_5(-7,16)=-7\cdot 305-16(-119)=-231,\\
&Q_5(-3,16)=-3(-95)-16\cdot 69=-819,\\
&Q_5(1,16)=209-16(-31)=705,\\
&Q_5(5,16)=5(-319)-16(-35)=-1035,\\
&Q_6(-7,16)=-7(-231)-16\cdot 305=-3263,\\
&Q_6(-3,16)=-3(-819)-16(-95)=3977,\\
&Q_6(1,16)=705-16\cdot 209=-2639,\\
&Q_6(5,16)=5(-1035)-16(-319)=-71,\\
&Q_7(-7,16)=-7(-3263)-16(-231)=26537,\\
&Q_7(-3,16)=-3\cdot 3977-16(-819)=1173,\\
&Q_7(1,16)=-2639-16\cdot 705=-13919,\\
&Q_7(5,16)=5(-71)-16(-1035)=16205,
\end{aligned}$$

$$
\begin{aligned}
&Q_8(-7,16) = -7\cdot 26537 - 16(-3263) = -133551,\\
&Q_8(-3,16) = -3\cdot 1173 - 16\cdot 3977 = -67151,\\
&Q_8(1,16) = -13919 - 16(-2639) = 28305,\\
&Q_8(5,16) = 5\cdot 16205 - 16(-71) = 82161,\\
&Q_9(-7,16) = -7(-133551) - 16\cdot 26537 = 510265,\\
&Q_9(-3,16) = -3(-67151) - 16\cdot 1173 = 182685,\\
&Q_9(1,16) = 28305 - 16(-13919) = 251009,\\
&Q_9(5,16) = 5\cdot 82161 - 16\cdot 16205 = 151525,\\
&Q_{10}(-7,16) = -7\cdot 510265 - 16(-133551) = -1435039,\\
&Q_{10}(-3,16) = -3\cdot 182685 - 16(-67151) = 526361,\\
&Q_{10}(1,16) = 251009 - 16\cdot 28305 = -201871,\\
&Q_{10}(5,16) = 5\cdot 151625 - 16\cdot 82161 = -556951,\\
&Q_{11}(-7,16) = -7(-1435039) - 16\cdot 510265 = 1881033,\\
&Q_{11}(-3,16) = -3\cdot 526361 - 16\cdot 182685 = -4502043,\\
&Q_{11}(1,16) = -201871 - 16\cdot 251009 = -4218015,\\
&Q_{11}(5,16) = 5(-556951) - 16\cdot 151525 = -5209155,\\
&Q_{12}(-7,16) = -7\cdot 1881033 - 16(-1435039) = 9793393,\\
&Q_{12}(-3,16) = -3(-4502043) - 16\cdot 526361 = 5084353,\\
&Q_{12}(1,16) = -4218015 - 16(-201871) = -988079,\\
&Q_{12}(5,16) = 5(-5209155) - 16(-556951) = -17134559,\\
&Q_{13}(-7,16) = -7\cdot 9793393 - 16\cdot 1881033 = -98650279,\\
&Q_{13}(-3,16) = -3\cdot 5084353 - 16(-4502043) = 56779629,\\
&Q_{13}(1,16) = -988079 - 16(-4218015) = 66500161,\\
&Q_{13}(5,16) = 5(-17134559) - 16(-5209155) = -2326315,\\
&Q_{14}(-7,16) = -7(-98650279) - 16\cdot 9793393 = 533857065,\\
&Q_{14}(-3,16) = -3\cdot 56779629 - 16\cdot 5084353 = -251688535,\\
&Q_{14}(1,16) = 66500161 - 15(-988079) = 82309425,\\
&Q_{14}(5,16) = 5(-2326315) - 16(-17134559) = 262521369,\\
&Q_{15}(-7,16) = -7\cdot 533857665 - 16(-98650279) = -2158599191,\\
&Q_{15}(-3,16) = -3(-251688535) - 16\cdot 56779629 = -153408459,\\
&Q_{15}(1,16) = 82309425 - 16\cdot 66500161 = -981693151,\\
&Q_{15}(5,16) = 5\cdot 262521369 - 16(-2326315) = 1349827885.
\end{aligned}
$$

Notemos que, por la tabla de valores para d pequeño de los números de clase de Kronecker que tenemos en la Sección 1.5, sabemos que

$$H(-15) = 2, \qquad H(-39) = 4, \qquad H(-55) = 4, \qquad H(-63) = 5.$$

Entonces, tenemos que

$$\tau_2(16) = -16,$$

$$\begin{aligned}\tau_3(16) = &-1-\{Q_1(-7,16)H(-15)+Q_1(-3,16)H(-55)+Q_1(1,16)H(-63)\\ &+Q_1(5,16)H(-39)\}=-1-(-7\cdot 2-3\cdot 4+1\cdot 5+5\cdot 4)=0,\end{aligned}$$

$$\begin{aligned}\tau_4(16) = &-1-\{Q_2(-7,16)H(-15)+Q_2(-3,16)H(-55)+Q_2(1,16)H(-63)\\ &+Q_2(5,16)H(-39)\}=-1-(33\cdot 2-7\cdot 4-15\cdot 5+9\cdot 4)=0,\end{aligned}$$

$$\begin{aligned}\tau_5(16) = &-1-\{Q_3(-7,16)H(-15)+Q_3(-3,16)H(-55)+Q_3(1,16)H(-63)\\ &+Q_3(5,16)H(-39)\}=-1-(-119\cdot 2+69\cdot 4-31\cdot 5-35\cdot 4)=256,\end{aligned}$$

$$\begin{aligned}\tau_6(16) = &-1-\{Q_4(-7,16)H(-15)+Q_4(-3,16)H(-55)+Q_4(1,16)H(-63)\\ &+Q_4(5,16)H(-39)\}=-1-(305\cdot 2-95\cdot 4+209\cdot 5-319\cdot 4)=0,\end{aligned}$$

$$\begin{aligned}\tau_7(16) = &-1-\{Q_5(-7,16)H(-15)+Q_5(-3,16)H(-55)+Q_5(1,16)H(-63)\\ &+Q_5(5,16)H(-39)\}=-1-(-231\cdot 2-819\cdot 4+705\cdot 5-1035\cdot 4)=4352,\end{aligned}$$

$$\begin{aligned}\tau_8(16) = &-1-\{Q_6(-7,16)H(-15)+Q_6(-3,16)H(-55)+Q_6(1,16)H(-63)\\ &+Q_6(5,16)H(-39)\}=-1-(-3263\cdot 2+3977\cdot 4-2639\cdot 5-71\cdot 4)=4096,\end{aligned}$$

$$\begin{aligned}\tau_9(16) = &-1-\{Q_7(-7,16)H(-15)+Q_7(-3,16)H(-55)+Q_7(1,16)H(-63)\\ &+Q_7(5,16)H(-39)\}=-1-(26537\cdot 2+1173\cdot 4-13919\cdot 5+16205\cdot 4)=-52992,\end{aligned}$$

$$\begin{aligned}\tau_{10}(16) = &-1-\{Q_8(-7,16)H(-15)+Q_8(-3,16)H(-55)+Q_8(1,16)H(-63)\\ &+Q_8(5,16)H(-39)\}=-1-(-133551\cdot 2-67151\cdot 4+28305\cdot 5+82161\cdot 4)=65536,\end{aligned}$$

$$\begin{aligned}\tau_{11}(16) = &-1-\{Q_9(-7,16)H(-15)+Q_9(-3,16)H(-55)+Q_9(1,16)H(-63)\\ &+Q_9(5,16)H(-39)\}=-1-(510265\cdot 2+182685\cdot 4+251009\cdot 5+151525\cdot 4)=-3612416,\end{aligned}$$

$$\begin{aligned}\tau_{12}(16) = &-1-\{Q_{10}(-7,16)H(-15)+Q_{10}(-3,16)H(-55)+Q_{10}(1,16)H(-63)\\ &+Q_{10}(5,16)H(-39)\}=-1-(1435039\cdot 2+526361\cdot 4-201871\cdot 5-556951\cdot 4)=4001792,\end{aligned}$$

$$\begin{aligned}\tau_{13}(16) = &-1-\{Q_{11}(-7,16)H(-15)+Q_{11}(-3,16)H(-55)+Q_{11}(1,16)H(-63)\\ &+Q_{11}(5,16)H(-39)\}=-1-(1881033\cdot 2-4502043\cdot 4-4218015\cdot 5-5209155\cdot 4)\\ &=56172800,\end{aligned}$$

$$\begin{aligned}\tau_{14}(16) = &-1-\{Q_{12}(-7,16)H(-15)+Q_{12}(-3,16)H(-55)+Q_{12}(1,16)H(-63)\\ &+Q_{12}(5,16)H(-39)\}=-1-(9793393\cdot 2+5084353\cdot 4-988079\cdot 5-17134559\cdot 4)\\ &=33554432,\end{aligned}$$

$$\begin{aligned}\tau_{15}(16) = &-1-\{Q_{13}(-7,16)H(-15)+Q_{13}(-3,16)H(-55)+Q_{13}(1,16)H(-63)\\ &+Q_{13}(5,16)H(-39)\}=-1-(-98650279\cdot 2+56779629\cdot 4+66500161\cdot 5-2326315\cdot 4)\\ &=-353013504,\end{aligned}$$

$$\begin{aligned}\tau_{16}(16) = &-1-\{Q_{14}(-7,16)H(-15)+Q_{14}(-3,16)H(-55)+Q_{14}(1,16)H(-63)\\ &+Q_{14}(5,16)H(-39)\}=-1-(533857665\cdot 2-251688535\cdot 4+82309425\cdot 5+262521369\cdot 4)\\ &=-1522593792,\end{aligned}$$

$$\begin{aligned}\tau_{17}(16) = &-1-\{Q_{15}(-7,16)H(-15)+Q_{15}(-3,16)H(-55)+Q_{15}(1,16)H(-63)\\ &+Q_{15}(5,16)H(-39)\}=-1-(-2158599191\cdot 2-153408459\cdot 4-981693151\cdot 5\\ &+1349827885\cdot 4)=4439986432.\end{aligned}$$

Calculemos ahora los valores $W_{i,j}(16)$.

$$
\begin{aligned}
W_{0,0}(16) &= 1,\\
W_{1,1}(16) &= -1,\\
W_{2,0}(16) &= \tfrac{1}{2}(-16W_{1,1}(16) - W_{1,-1}(16) - 15W_{0,0}(16))\\
&= \tfrac{1}{2}(-16\cdot(-1) - 15\cdot 1) = \tfrac{1}{2},\\
W_{2,2}(16) &= \tfrac{1}{2}(-16W_{1,3}(16) - W_{1,1}(16) - 15W_{0,2}(16))\\
&= \tfrac{1}{2}(-(-1)) = \tfrac{1}{2},\\
W_{3,1}(16) &= \tfrac{1}{3}(-16W_{2,2}(16) - W_{2,0}(16) - 14W_{1,1}(16))\\
&= \tfrac{1}{3}(-16\cdot\tfrac{1}{2} - \tfrac{1}{2} - 14\cdot(-1)) = \tfrac{11}{6},\\
W_{3,3}(16) &= \tfrac{1}{3}(-16W_{2,4}(16) - W_{2,2}(16) - 14W_{1,3}(16))\\
&= \tfrac{1}{3}(-\tfrac{1}{2}) = -\tfrac{1}{6},\\
W_{4,0}(16) &= \tfrac{1}{4}(-16W_{3,1}(16) - W_{3,-1}(16) - 13W_{2,0}(16))\\
&= \tfrac{1}{4}(-16\cdot\tfrac{11}{6} - 13\cdot\tfrac{1}{2}) = -\tfrac{215}{24},\\
W_{4,2}(16) &= \tfrac{1}{4}(-16W_{3,3}(16) - W_{3,1}(16) - 13W_{2,2}(16))\\
&= \tfrac{1}{4}(-16\cdot(-\tfrac{1}{6}) - \tfrac{11}{6} - 13\cdot\tfrac{1}{2}) = -\tfrac{34}{24},\\
W_{4,4}(16) &= \tfrac{1}{4}(-16W_{3,5}(16) - W_{3,3}(16) - 13W_{2,4}(16))\\
&= \tfrac{1}{4}(-(-\tfrac{1}{6})) = \tfrac{1}{24},\\
W_{5,1}(16) &= \tfrac{1}{5}(-16W_{4,2}(16) - W_{4,0}(16) - 12W_{3,1}(16))\\
&= \tfrac{1}{5}(-16\cdot(-\tfrac{34}{24}) - (-\tfrac{215}{24}) - 12\cdot\tfrac{11}{6}) = \tfrac{231}{120},\\
W_{5,3}(16) &= \tfrac{1}{5}(-16W_{4,4}(16) - W_{4,2}(16) - 12W_{3,3}(16))\\
&= \tfrac{1}{5}(-16\cdot\tfrac{1}{24} - (-\tfrac{34}{24}) - 12\cdot(-\tfrac{1}{6})) = \tfrac{66}{120},\\
W_{5,5}(16) &= \tfrac{1}{5}(-16W_{4,6}(16) - W_{4,4}(16) - 12W_{3,5}(16))\\
&= \tfrac{1}{5}(-\tfrac{1}{24}) = -\tfrac{1}{120},\\
W_{6,0}(16) &= \tfrac{1}{6}(-16W_{5,1}(16) - W_{5,-1}(16) - 11W_{4,0}(16))\\
&= \tfrac{1}{6}(-16\cdot\tfrac{231}{120} - 11\cdot(-\tfrac{215}{24})) = \tfrac{8129}{720},\\
W_{6,2}(16) &= \tfrac{1}{6}(-16W_{5,3}(16) - W_{5,1}(16) - 11W_{4,2}(16))\\
&= \tfrac{1}{6}(-16\cdot\tfrac{66}{120} - \tfrac{231}{120} - 11\cdot(-\tfrac{34}{24})) = \tfrac{583}{720},\\
W_{6,4}(16) &= \tfrac{1}{6}(-16W_{5,5}(16) - W_{5,3}(16) - 11W_{4,4}(16))\\
&= \tfrac{1}{6}(-16\cdot(-\tfrac{1}{120} - \tfrac{66}{120} - 11\cdot\tfrac{1}{24})) = -\tfrac{105}{720},\\
W_{6,6}(16) &= \tfrac{1}{6}(-16W_{5,7}(16) - W_{5,5}(16) - 11W_{4,6}(16))\\
&= \tfrac{1}{6}(-(-\tfrac{1}{120})) = \tfrac{1}{720},\\
W_{7,1}(16) &= \tfrac{1}{7}(-16W_{6,2} - W_{6,0}(16) - 10W_{5,1}(16))\\
&= \tfrac{1}{7}(-16\cdot\tfrac{583}{720} - \tfrac{8129}{720} - 16\cdot\tfrac{231}{120}) = -\tfrac{31317}{5040},\\
W_{7,3}(16) &= \tfrac{1}{7}(-16W_{6,4}(16) - W_{6,2}(16) - 10W_{5,3}(16))\\
&= \tfrac{1}{7}(-16\cdot(-\tfrac{105}{720}) - \tfrac{583}{720} - 10\cdot\tfrac{66}{120}) = -\tfrac{2863}{5040},
\end{aligned}
$$

$$
\begin{aligned}
W_{7,5}(16) &= \tfrac{1}{7}(-16W_{6,6}(16) - W_{6,4}(16) - 10W_{5,5}(16)) \\
&= \tfrac{1}{7}(-16 \cdot \tfrac{1}{120} - (-\tfrac{105}{720}) - 10 \cdot (-\tfrac{1}{120})) = \tfrac{149}{5040}, \\
W_{7,7}(16) &= \tfrac{1}{7}(-16W_{6,8}(16) - W_{6,6}(16) - 10W_{5,7}(16)) \\
&= \tfrac{1}{7}(-\tfrac{1}{720}) = -\tfrac{1}{5040}, \\
W_{8,0}(16) &= \tfrac{1}{8}(-16W_{7,1}(16) - W_{7,-1}(16) - 9W_{6,0}(16)) \\
&= \tfrac{1}{8}(-16 \cdot (-\tfrac{31317}{5040}) - 9 \cdot \tfrac{8129}{720}) = -\tfrac{11055}{40320}, \\
W_{8,2}(16) &= \tfrac{1}{8}(-16W_{7,3} - W_{7,1} - 9W_{6,2}) \\
&= \tfrac{1}{8}(-16 \cdot (-\tfrac{2863}{5040}) - (-\tfrac{31317}{5040}) - 9 \cdot \tfrac{583}{720}) = \tfrac{40396}{40320}, \\
W_{8,4}(16) &= \tfrac{1}{8}(-16W_{7,5}(16) - W_{7,3}(16) - 9W_{6,4}(16)) \\
&= \tfrac{1}{8}(-16\tfrac{149}{5040} - (-\tfrac{2863}{5040}) - 9 \cdot (-\tfrac{105}{720})) = \tfrac{7094}{40320}, \\
W_{8,6}(16) &= \tfrac{1}{8}(-16W_{7,7}(16) - W_{7,5} - 9W_{6,6}) \\
&= \tfrac{1}{8}(-16 \cdot (-\tfrac{1}{5040}) - \tfrac{149}{5040} - 9 \cdot \tfrac{1}{720}) = -\tfrac{196}{40320}, \\
W_{8,8}(16) &= \tfrac{1}{8}(-16W_{7,9}(16) - W_{7,7}(16) - 9W_{6,8}(16)) \\
&= \tfrac{1}{8}(-(-\tfrac{1}{5040})) = \tfrac{1}{40320}, \\
W_{9,1}(16) &= \tfrac{1}{9}(-16W_{8,2}(16) - W_{8,0}(16) - 8W_{7,1}(16)) \\
&= \tfrac{1}{9}(-16 \cdot \tfrac{40396}{40320} + \tfrac{11055}{40320} - 8 \cdot (-\tfrac{31317}{5040})) = \tfrac{1369007}{362880}, \\
W_{9,3}(16) &= \tfrac{1}{9}(-16W_{8,4}(16) - W_{8,2}(16) - 8W_{7,3}(16)) \\
&= \tfrac{1}{9}(-16 \cdot \tfrac{7094}{40320} - \tfrac{40396}{40320} - 8 \cdot (-\tfrac{2863}{5040})) = \tfrac{29332}{362880}, \\
W_{9,5}(16) &= \tfrac{1}{9}(-16W_{8,6}(16) \_ W_{8,4}(16) - 8W_{7,5}(16)) \\
&= \tfrac{1}{9}(-16 \cdot (-\tfrac{196}{40320}) - \tfrac{7094}{40320} - 8 \cdot \tfrac{149}{5040}) = -\tfrac{13494}{362880}, \\
W_{9,7}(16) &= \tfrac{1}{9}(-16W_{8,8}(16) - W_{8,5}(16) - 8W_{7,7}(16)) \\
&= \tfrac{1}{9}(-16 \cdot \tfrac{1}{40320} - (-\tfrac{196}{40320}) - 8(-\tfrac{1}{5040})) = \tfrac{244}{362880}, \\
W_{9,9}(16) &= \tfrac{1}{9}(-16W_{8,10}(16) - W_{8,8}(16) - 8W_{7,9}(16)) \\
&= \tfrac{1}{9}(-\tfrac{1}{40320}) = -\tfrac{1}{362880}, \\
W_{10,0}(16) &= \tfrac{1}{10}(-16W_{9,1}(16) - W_{9,-1}(16) - 7W_{8,0}(16)) \\
&= \tfrac{1}{10}(-16 \cdot \tfrac{1369007}{362880} - 7 \cdot (-\tfrac{11055}{40320})) = -\tfrac{21207647}{3628800}, \\
W_{10,2}(16) &= \tfrac{1}{10}(-16W_{9,3}(16) - W_{9,1}(16) - 7W_{8,2}(16)) \\
&= \tfrac{1}{10}(-16\tfrac{29332}{362880} - \tfrac{1369007}{362880} - 7 \cdot \tfrac{40396}{40320}) = -\tfrac{4383267}{3628800}, \\
W_{10,4}(16) &= \tfrac{1}{10}(-16W_{9,5}(16) - W_{9,3}(16) - 7W_{8,4}(16)) \\
&= \tfrac{1}{10}(-16(-\tfrac{13494}{362880} - \tfrac{29332}{362880} - 7\tfrac{7094}{40320}) = -\tfrac{260350}{3628800}, \\
W_{10,6}(16) &= \tfrac{1}{10}(-16W_{9,7}(16) - W_{9,5}(16) - 7W_{8,6}(16)) \\
&= \tfrac{1}{10}(-16\tfrac{244}{362880} - (-\tfrac{13494}{362880}) - 7(-\tfrac{196}{40320})) = \tfrac{21938}{3628800}, \\
W_{10,8}(16) &= \tfrac{1}{10}(-16W_{9,9}(16) - W_{9,7}(16) - 7W_{8,8}(16)) \\
&= \tfrac{1}{10}(-16(-\tfrac{1}{362880}) - \tfrac{244}{362880} - 7\tfrac{1}{40320}) = -\tfrac{291}{3628800}, \\
W_{10,10}(16) &= \tfrac{1}{10}(-16W_{9,11}(16) - W_{9,9}(16) - 7W_{8,10}(16)) \\
&= \tfrac{1}{10}(-(-\tfrac{1}{3628800})) = \tfrac{1}{3628800}, \\
W_{11,1}(16) &= \tfrac{1}{11}(-16W_{10,2}(16) - W_{10,0}(16) - 6W_{9,2}(16)) \\
&= \tfrac{1}{11}(-16(-\tfrac{4383267}{3628800}) + \tfrac{21207647}{3628800} - 6\tfrac{1369007}{362880}) = \tfrac{9199499}{39916800}, \\
W_{11,3}(16) &= \tfrac{1}{11}(-16W_{10,4}(16) - W_{10,2}(16) - 6W_{9,3}(16)) \\
&= \tfrac{1}{11}(-16(-\tfrac{260350}{3628800}) + \tfrac{4383267}{3628800} - 6\tfrac{29332}{362880}) = \tfrac{6788947}{39916800},
\end{aligned}
$$

$$
\begin{aligned}
W_{11,5}(16) &= \tfrac{1}{11}(-16W_{10,6}(16) - W_{10,4}(16) - 6W_{9,5}(16)) \\
&= \tfrac{1}{11}(-16\tfrac{21938}{3628800} + \tfrac{260350}{3628800} - 6(-\tfrac{13494}{362880})) = \tfrac{718982}{39916800}, \\
W_{11,7}(16) &= \tfrac{1}{11}(-16W_{10,8}(16) - W_{10,6}(16) - 6W_{9,7}(16)) \\
&= \tfrac{1}{11}(-16(-\tfrac{291}{3628800}) - \tfrac{21398}{3628800} - 6\tfrac{244}{362880}) = -\tfrac{31922}{39916800}, \\
W_{11,9}(16) &= \tfrac{1}{11}(-16W_{10,10}(16) - W_{10,8}(16) - 6W_{9,9}(16)) \\
&= \tfrac{1}{11}(-16\tfrac{1}{3628800} + \tfrac{291}{3628800} - 6(-\tfrac{1}{362880})) = \tfrac{335}{39916800}, \\
W_{11,11}(16) &= \tfrac{1}{11}(-16W_{10,12}(16) - W_{10,10}(16) - 6W_{9,11}(16)) \\
&= \tfrac{1}{11}(-\tfrac{1}{3628800}) = -\tfrac{1}{3916800}, \\
W_{12,0}(16) &= \tfrac{1}{12}(-16W_{11,1}(16) - W_{11,-1}(16) - 5W_{10,0}(16)) \\
&= \tfrac{1}{12}(-16\tfrac{9199499}{39916800} - 5(-\tfrac{21207647}{3628800})) = \tfrac{1019228601}{479001600}, \\
W_{12,2}(16) &= \tfrac{1}{12}(-16W_{11,3}(16) - W_{11,1}(16) - 5W_{10,2}(16)) \\
&= \tfrac{1}{12}(-16\tfrac{6788947}{39916800} - \tfrac{9199499}{39916800} - 5(-\tfrac{4383267}{3628800})) = \tfrac{123257134}{479001600}, \\
W_{12,4}(16) &= \tfrac{1}{12}(-16W_{11,5}(16) - W_{11,3}(16) - 5W_{10,4}(16)) \\
&= \tfrac{1}{12}(-16\tfrac{718982}{39916800} - \tfrac{6788947}{39916800} - 5(-\tfrac{260350}{3628800})) = -\tfrac{3973409}{479001600}, \\
W_{12,6}(16) &= \tfrac{1}{12}(-16W_{11,7}(16 - W_{11,5}(16) - 5W_{10,6}(16)) \\
&= \tfrac{1}{12}(-16(-\tfrac{31922}{39916800}) - \tfrac{718982}{39916800} - 5\tfrac{21938}{3628800}) = -\tfrac{1414820}{479001600}, \\
W_{12,8}(16) &= \tfrac{1}{12}(-16W_{11,9}(16) - W_{11,7}(16) - 5W_{10,8}(16)) \\
&= \tfrac{1}{12}(-16\tfrac{335}{39916800} + \tfrac{31922}{39916800} - 5(-\tfrac{291}{3628800})) = \tfrac{42567}{479001600}, \\
W_{12,10}(16) &= \tfrac{1}{12}(-16W_{11,11}(16) - W_{11,9}(16) - 5W_{10,10}(16)) \\
&= \tfrac{1}{12}(-16(-\tfrac{1}{39916800}) - \tfrac{335}{39916800} - 5\tfrac{1}{3628800}) = -\tfrac{374}{479001600}, \\
W_{12,12}(16) &= \tfrac{1}{12}(-16W_{11,13}(16) - W_{11,11}(16) - 5W_{10,12}(16)) \\
&= \tfrac{1}{12}(-(-\tfrac{1}{39916800})) = \tfrac{1}{479001600}, \\
W_{13,1}(16) &= \tfrac{1}{13}(-16W_{12,2}(16) - W_{12,0}16 - 4W_{11,1}(16)) \\
&= \tfrac{1}{13}(-16\tfrac{123257034}{479001600} - \tfrac{1019228601}{479001600} - 4\tfrac{9199499}{39916800}) = -\tfrac{3432917097}{6227020800}, \\
W_{13,3}(16) &= \tfrac{1}{13}(-16W_{12,4}(16) - W_{12,2}(16) - 4W_{11,3}(16)) \\
&= \tfrac{1}{13}(-16(-\tfrac{3973409}{479001600}) - \tfrac{123257034}{479001600} - 4\tfrac{6788947}{39916800}) = -\tfrac{385551946}{6227020800}, \\
W_{13,5}(16) &= \tfrac{1}{13}(-16W_{12,6}(16) - W_{12,4}(16) - 4W_{11,5}(16)) \\
&= \tfrac{1}{13}(-16(-\tfrac{1414820}{479001600}) - (-\tfrac{3973409}{479001600}) - 4\tfrac{718982}{39916800}) = -\tfrac{7900607}{6227020800}, \\
W_{13,7}(16) &= \tfrac{1}{13}(-16W_{12,8}(16) - W_{12,6}(16) - 4W_{11,7}(16)) \\
&= \tfrac{1}{13}(-16\tfrac{42567}{479001600} - (-\tfrac{1414820}{479001600}) - 4(-\tfrac{31922}{39916800})) = \tfrac{2266004}{6227020800}, \\
W_{13,9}(16) &= \tfrac{1}{13}(-16W_{12,10}(16) - W_{12,8}(16) - 4W_{11,9}(16)) \\
&= \tfrac{1}{13}(-16(-\tfrac{374}{479001600}) - \tfrac{42567}{479001600} - 4\tfrac{335}{39916800}) = -\tfrac{52663}{6227020800}, \\
W_{13,11}(16) &= \tfrac{1}{13}(-16W_{12,12}(16) - W_{12,10}(16) - 4W_{11,11}(16)) \\
&= \tfrac{1}{13}(-16\tfrac{1}{479001600} - (-\tfrac{374}{479001600} - 4(-\tfrac{1}{39916800})) = \tfrac{406}{6227020800}, \\
W_{13,13}(16) &= \tfrac{1}{13}(-16W_{12,14}(16) - W_{12,12}(16) - 4W_{11,13}(16)) \\
&= \tfrac{1}{13}(-\tfrac{1}{479001600}) = -\tfrac{1}{6227020800}, \\
W_{14,0}(16) &= \tfrac{1}{14}(-16W_{13,1}(16) - W_{13,-1}(16) - 3W_{12,0}(16)) \\
&= \tfrac{1}{14}(-16(-\tfrac{3432917097}{6227020800}) - 3\tfrac{1019228601}{6227020800}) = \tfrac{15176758113}{87178291200}, \\
W_{14,2}(16) &= \tfrac{1}{14}(-16W_{13,3}(16) - W_{13,1}(16) - 3W_{12,2}(16)) \\
&= \tfrac{1}{14}(-16(-\tfrac{385551946}{6227020800}) - (-\tfrac{3432917097}{6227020800}) - 3\tfrac{123257034}{479001600}) = \tfrac{4794723907}{87178291200},
\end{aligned}
$$

$$
\begin{aligned}
W_{14,4}(16) &= \tfrac{1}{14}(-16W_{13,5}(16) - W_{13,3}(16) - 3W_{12,4}(16)) \\
&= \tfrac{1}{14}(-16(-\tfrac{7900607}{6227020800}) - (-\tfrac{385551946}{6227020800}) - 3(-\tfrac{3973409}{479001600})) = \tfrac{666924609}{87178291200}, \\
W_{14,6}(16) &= \tfrac{1}{14}(-16W_{13,7}(16) - W_{13,5}(16) - 3W_{12,6}(16)) \\
&= \tfrac{1}{14}(-16\tfrac{2266004}{6227020800} - (-\tfrac{7900607}{6227020800}) - 3(-\tfrac{1414820}{479001600})) = \tfrac{26822523}{87178291200}, \\
W_{14,8}(16) &= \tfrac{1}{14}(-16W_{13,9}(16) - W_{13,7}(16) - 3W_{12,8}(16)) \\
&= \tfrac{1}{14}(-16(-\tfrac{52663}{6227020800}) - \tfrac{2266004}{6227020800} - 3\tfrac{42567}{479001600}) = -\tfrac{3083509}{87178291200}, \\
W_{14,10}(16) &= \tfrac{1}{14}(-16W_{13,11}(16) - W_{13,9}(16) - 3W_{12,10}(16)) \\
&= \tfrac{1}{14}(-16\tfrac{406}{6227020800} - (-\tfrac{52663}{6227020800}) - 3(-\tfrac{374}{479001600})) = \tfrac{60753}{87178291200}, \\
W_{14,12}(16) &= \tfrac{1}{14}(-16W_{13,13}(16) - W_{13,11}(16) - 3W_{12,12}(16)) \\
&= \tfrac{1}{14}(-16(-\tfrac{1}{6227020800}) - \tfrac{406}{6227020800} - 3\tfrac{1}{479001600}) = -\tfrac{429}{87178291200}, \\
W_{14,14}(16) &= \tfrac{1}{14}(-16W_{13,15}(16) - W_{13,13}(16) - 3W_{12,14}(16)) \\
&= \tfrac{1}{14}(-\tfrac{1}{6227020800}) = \tfrac{1}{87178291200}, \\
W_{15,1}(16) &= \tfrac{1}{15}(-16W_{14,2}(16) - W_{14,0}(16) - 2W_{13,1}(16)) \\
&= \tfrac{1}{15}(-16\tfrac{4794723907}{87178291200} - \tfrac{15176758113}{87178291200} - 2(-\tfrac{3432917097}{6227020800})) = \tfrac{4229338091}{87178291200\cdot 15}, \\
W_{15,3}(16) &= \tfrac{1}{15}(-16W_{14,4}(16) - W_{14,2}(16) - 2W_{13,3}(16)) \\
&= \tfrac{1}{15}(-16\tfrac{666924609}{87178291200} - \tfrac{4794723907}{87178291200} - 2(-\tfrac{385551946}{6227020800})) = -\tfrac{4670063163}{87178291200\cdot 15}, \\
W_{15,5}(16) &= \tfrac{1}{15}(-16W_{14,6}(16) - W_{14,4}(16) - 2W_{13,5}(16)) \\
&= \tfrac{1}{15}(-16\tfrac{26822523}{87178291200} - \tfrac{666924609}{87178291200} - 2(-\tfrac{7900607}{6227020800})) = -\tfrac{874867981}{87178291200\cdot 15}, \\
W_{15,7}(16) &= \tfrac{1}{15}(-16W_{14,8}(16) - W_{14,4}(16) - 2W_{13,7}(16)) \\
&= \tfrac{1}{15}(-16(-\tfrac{3083509}{87178291200}) - \tfrac{26822523}{87178291200} - 2\tfrac{2266004}{6227020800}) = \tfrac{40934491}{87178291200\cdot 15}, \\
W_{15,9}(16) &= \tfrac{1}{15}(-16W_{14,10}(16) - W_{14,8}(16) - 2W_{13,9}(16)) \\
&= \tfrac{1}{15}(-16\tfrac{60753}{87178291200} + \tfrac{3083509}{87178291200} - 2(-\tfrac{52663}{6227020800})) = \tfrac{3586025}{87178291200\cdot 15}, \\
W_{15,11}(16) &= \tfrac{1}{15}(-16W_{14,12}(16) - W_{14,10}(16) - 2W_{13,11}(16)) \\
&= \tfrac{1}{15}(-16(-\tfrac{429}{87178291200}) - \tfrac{60753}{87178291200} - 2\tfrac{406}{6227020800}) = -\tfrac{65257}{87178291200\cdot 15}, \\
W_{15,13}(16) &= \tfrac{1}{15}(-16W_{14,14}(16) - W_{14,12}(16) - 2W - 13,13(16)) \\
&= \tfrac{1}{15}(-16\tfrac{1}{87178291200} + \tfrac{429}{87178291200} - 2(-\tfrac{1}{6227020800})) = \tfrac{441}{87178291200\cdot 15}, \\
W_{15,15}(16) &= \tfrac{1}{15}(-16W_{14,16}(16) - W_{14,14}(16) - 2W_{13,15}(16)) \\
&= \tfrac{1}{15}(-\tfrac{1}{87178291200}) = -\tfrac{1}{87178291200\cdot 15}.
\end{aligned}
$$

Calculemos, ahora sí, la distribución de pesos del código $M_2(4)$.

$$
\begin{aligned}
256A_0 &= \tbinom{15}{0} + 30(-1)^0\tbinom{7}{0} - 15W_{0,0}(16)(1+\tau_2(16)) \\
&= 1 + 30 - 15(1-16) \\
&= 256, \\
256A_1 &= \tbinom{15}{1} + 30(-1)^1\tbinom{7}{0} - 15W_{1,1}(16)(1+\tau_3(16) \\
&= 15 - 30 - 15(-1)(1+0) \\
&= 0,
\end{aligned}
$$

$$
\begin{aligned}
256A_2 &= \tbinom{15}{2} + 30(-1)^1\tbinom{7}{1} - 15[W_{2,0}(16)(1+\tau_2(16)) + W_{2,2}(16)(1+\tau_4(16))] \\
&= 105 - 210 - 15[\tfrac{1}{2}(1-16) + \tfrac{1}{2}(1+0)] \\
&= 0, \\
256A_3 &= \tbinom{15}{3} + 30(-1)^2\tbinom{7}{1} - 15[W_{3,1}(16)(1+\tau_3(16)) + W_{3,3}(16)(1+\tau_5(16))] \\
&= 455 + 210 - 15[\tfrac{11}{6}(1+0) - \tfrac{1}{6}(1+256)] \\
&= 1280, \\
256A_4 &= \tbinom{15}{4} + 30(-1)^2\tbinom{7}{2} - 15[W_{4,0}(16)(1+\tau_2(16)) + W_{4,2}(16)(1+\tau_4(16)) \\
&\quad + W_{4,4}(16)(1+\tau_6(16))] \\
&= 1365 + 630 - 15[-\tfrac{215}{24}(1-16) - \tfrac{34}{24}(1+0) + \tfrac{1}{24}(1+0)] \\
&= 0, \\
256A_5 &= \tbinom{15}{5} + 30(-1)^3\tbinom{7}{2} - 15[W_{5,1}(16)(1+\tau_3(16)) + W_{5,3}(16)(1+\tau_5(16)) \\
&\quad + W_{5,5}(16)(1+\tau_7(16))] \\
&= 3003 - 630 - 15[\tfrac{231}{120}(1+0) + \tfrac{66}{120}(1+256) - \tfrac{1}{120}(1+4352)] \\
&= 768, \\
256A_6 &= \tbinom{15}{6} + 30(-1)^3\tbinom{7}{3} - 15[W_{6,0}(16)(1+\tau_2(16)) + W_{6,2}(16)(1+\tau_4(16)) \\
&\quad + W_{6,4}(16)(1+\tau_6(16)) + W_{6,6}(16)(1+\tau_8(16))] \\
&= 5005 - 1050 - 15[\tfrac{8129}{720}(1-16) + \tfrac{583}{720}(1+0) - \tfrac{105}{720}(1+0) + \tfrac{1}{720}(1+4096)] \\
&= 6400, \\
256A_7 &= \tbinom{15}{7} + 30(-1)^4\tbinom{7}{3} - 15[W_{7,1}(16)(1+\tau_3(16)) + W_{7,3}(16)(1+\tau_5(16)) \\
&\quad + W_{7,5}(16)(1+\tau_7(16)) + W_{7,7}(16)(1+\tau_9(16))] \\
&= 6435 + 1650 - 15[-\tfrac{31317}{5040} - \tfrac{2863}{5040}(1+256) + \tfrac{149}{5040}(1+4352) - \tfrac{1}{5040}(1-52992)] \\
&= 7680, \\
256A_8 &= \tbinom{15}{8} + 30(-1)^4\tbinom{7}{4} - 15[W_{8,0}(16)(1+\tau_2(16)) + W_{8,2}(16)(1+\tau_4(16)) \\
&\quad + W_{8,4}(16)(1+\tau_6(16)) + W_{8,6}(16)(1+\tau_8(16)) + W_{8,8}(16)(1+\tau_{10}(16))] \\
&= 6435 + 1050 - 15[-\tfrac{11055}{40320}(1-16) + \tfrac{40396}{40320}(1+0) + \tfrac{7094}{40320}(1+0) \\
&\quad - \tfrac{196}{40320}(1+4096) \\
&\quad + \tfrac{1}{40320}(1+65536)] \\
&= 7680, \\
256A_9 &= \tbinom{15}{9} + 30(-1)^5\tbinom{7}{4} - 15[W_{9,1}(16)(+\tau_3(16)) + W_{9,3}(16)(1+\tau_5(16)) \\
&\quad + W_{9,5}(16)(1+\tau_7(16)) + W_{9,7}(16)(1+\tau_9(16)) + W_{9,9}(16)(1+\tau_{11}(16))] \\
&= 5005 - 1650 - 15[\tfrac{1369007}{362880}(1+0) + \tfrac{29332}{362880}(1+256) - \tfrac{13494}{362880}(1+4352) \\
&\quad + \tfrac{244}{362880}(1-52992) - \tfrac{1}{362880}(1-3612416)] \\
&= 6400, \\
256A_{10} &= \tbinom{15}{10} + 30(-1)^5\tbinom{7}{5} - 15[W_{10,0}(16)(1+\tau_2(16)) + W_{10,2}(16)(1+\tau_4(16)) \\
&\quad + W_{10,4}(16)(1+\tau_6(16)) + W_{10,6}(16)(1+\tau_8(16)) + W10,8(16)(1+\tau_{10}(16)) \\
&\quad + W_{10,10}(16)(1+\tau_{12}(16))] \\
&= 3003 - 630 - 15[-\tfrac{21207647}{3628800}(1-16) - \tfrac{4383267}{3628800}(1+0) - \tfrac{260350}{3628800}(1+0) \\
&\quad + \tfrac{21938}{3628800}(1+4096) - \tfrac{291}{3628800}(1+65536) + \tfrac{1}{3628800}(1+4001792)] \\
&= 768,
\end{aligned}
$$

$$
\begin{aligned}
256A_{11} &= \tbinom{15}{11} + 30(-1)^6\tbinom{7}{5} - 15[W_{11,1}(16)(1+\tau_3(16)) + W_{11,3}(16)(1+\tau_5(16)) \\
&+ W_{11,5}(16)(1+\tau_7(16)) + W_{11,7}(16)(1+\tau_9(16)) + W_{11,9}(16)(1+\tau_{11}(16)) \\
&+ W_{11,11}(16)(1+\tau_{13}(16))] \\
&= 1365 + 630 - 15[\tfrac{9199499}{39916800}(1+0) + \tfrac{6788947}{39916800}(1+256) + \tfrac{718982}{39916800}(1+4352) \\
&- \tfrac{31922}{39916800}(1-52992) + \tfrac{335}{39916800}(1-3612416) - \tfrac{1}{39916800}(1+56172800)] \\
&= 0, \\
256A_{12} &= \tbinom{15}{12} + 30(-1)^6\tbinom{7}{6} - 15[W_{12,0}(16)(1+\tau_2(16)) + W_{12,2}(16)(1+\tau_4(16)) \\
&+ W_{12,4}(16)(1+\tau_6(16)) + W_{12,6}(16)(1+\tau_8(16)) + W_{12,8}(1+\tau_{10}(16)) \\
&+ W_{12,10}(16)(1+\tau_{12}(16)) + W_{12,12}(16)(1+\tau_{14}(16))] \\
&= 455 + 210 - 15[\tfrac{1019228601}{479001600}(1-16) + \tfrac{123257034}{479001600}(1+0) - \tfrac{3973409}{479001600}(1+0) \\
&- \tfrac{1414820}{479001600}(1+4096) + \tfrac{42567}{479001600}(1+65536) - \tfrac{374}{479001600}(1+4001792) \\
&+ \tfrac{1}{479001600}(1+33554432)] \\
&= 1200, \\
256A_{13} &= \tbinom{15}{13} + 30(-1) * 7\tbinom{7}{6} - 15[W_{13,1}(16)(1+\tau_3(16)) + W_{13,3}(16)(1+\tau_5(16)) \\
&+ W_{13,5}(16)(1+\tau_7(16)) + W_{13,7}(16)(1+\tau_9(16)) + W_{13,9}(16)(1+\tau_{11}(16)) \\
&+ W_{13,11}(16)(1+\tau_{13}(16)) + W_{13,13}(16)(1+\tau_{15}(16))] \\
&= 105 - 210 - 15[-\tfrac{3432917097}{6227020800}(1+0) - \tfrac{385551946}{622702800}(1+256) - \tfrac{7900607}{6227020800}(1+4352) \\
&+ \tfrac{2266004}{6227020800}(1-52992) - \tfrac{52663}{6227020800}(1-3612416) + \tfrac{406}{6227020800}(1+56172800) \\
&- \tfrac{1}{6227020800}(1-353013504)] \\
&= 0, \\
256A_{14} &= \tbinom{15}{14} + 30(-1)^7\tbinom{7}{7} - 15[W_{14,0}(16)(1+\tau_2(16)) + W_{14,2}(16)(1+\tau_4(16)) \\
&+ W_{14,4}(16)(1+\tau_6(16)) + W_{14,6}(16)(1+\tau_8(16)) + W_{14,8}(16)(1+\tau_{10}(16)) \\
&+ W_{14,10}(16)(1+\tau_{12}(16)) + W_{14,12}(16)(1+\tau_1 4(16)) + W_{14,14}(16)(1+\tau_1 6(16))] \\
&= 15 - 30 - 15[\tfrac{15176758113}{87178291200}(1-16) + \tfrac{4794723907}{87178291200}(1+0) + \tfrac{666924609}{87178291200}(1+0) \\
&+ \tfrac{26822523}{87178291200}(1+4096) - \tfrac{3083509}{87178291600}(1+65536) + \tfrac{60753}{87178291200}(1+4001792) \\
&- \tfrac{429}{87178291200}(1+33554432) + \tfrac{1}{87178291200}(1-1522593792)] \\
&= 0, \\
256A_{15} &= \tbinom{15}{15} + 30(-1)^8\tbinom{7}{7} - 15[W_{15,1}(16)(1+\tau_3(16)) + W_{15,3}(16)(1+\tau_5(16)) \\
&+ W_{15,5}(16)(1+\tau_7(16)) + W_{15,7}(16)(1+\tau_9(16)) + W_{15,9}(16)(1+\tau_{11}(16)) \\
&+ W_{15,11}(16)(1+\tau_{13}(16)) + W_{15,13}(16)(1+\tau_{15}(16)) + W_{15,15}(16)(1+\tau_1 7(16))] \\
&= 1 + 30 - 15[\tfrac{4229338091}{87178291200\cdot 15}(1+0) - \tfrac{4670063163}{87178291200\cdot 15}(1+256) \\
&- \tfrac{874867981}{87178291200\cdot 15}(1+4352) - \tfrac{40934491}{87178291200\cdot 15}(1-52992) + \tfrac{3586025}{87178291200\cdot 15}(1-3612416) \\
&- \tfrac{65257}{87178291200\cdot 15}(1+56172800) + \tfrac{441}{87178291200\cdot 15}(1-353013504) \\
&- \tfrac{1}{87178291200\cdot 15}(1+4439986432)] \\
&= 256.
\end{aligned}
$$

Luego, la distribución de pesos de este código está dada por

$$\begin{aligned} A_0 &= A_{15} = 1, \\ A_3 &= A_{12} = 5, \\ A_5 &= A_{10} = 3, \\ A_6 &= A_9 = 25, \\ A_7 &= A_8 = 30, \end{aligned}$$

y

$$A_1 = A_2 = A_4 = A_{11} = A_{13} = A_{14} = 0.$$

A.6 Zetterberg $Z_2(4)$

Encontremos la distribución de pesos del código Zetterberg $Z_2(4)$. Los valores $\tau_k(16)$ de la traza del operador de Hecke ya los calculamos para $M_2(4)$, para $k \leq 17$, calculemos ahora para $k = 18$ y $k = 19$.

Primero encontremos $Q_{16}(t, 16)$ y $Q_{17}(t, 16)$ para cada t.

$$\begin{aligned} Q_{16}(-7,16) &= -7(-2158599191) - 16 \cdot 6568471697 = 6568471697, \\ Q_{16}(-3,16) &= -3(-153408459) - 168 - (-251688535) = 4487241937, \\ Q_{16}(1,16) &= -981693151 - 16 \cdot 82309425 = -2298643951, \\ Q_{16}(5,16) &= 5 \cdot 1349827885 - 16 \cdot 262521369 = 2548797521, \\ Q_{17}(-7,16) &= -7 \cdot 6568471697 - 16(2158599191) = 11441714823, \\ Q_{17}(-3,16) &= -3 \cdot 4487241937 - 16(-153408459) = -11007190467, \\ Q_{17}(1,16) &= -2298643951 - 16(-981693151) = 13408446465, \\ Q_{17}(5,16) &= 5 \cdot 2548797521 - 16 \cdot 1349827885. \end{aligned}$$

Ahora, calculamos las trazas que nos faltaban.

$$\begin{aligned} \tau_{18}(16) &= -1 - [Q_{16}(-7,16)H(-15) + Q_{16}(-3,16)H(-55) + Q_{16}(1,16)H(-63) \\ &\quad + Q_{16}(5,15)H(-39)] \\ &= -1 - [6568471697 \cdot 2 - 4487241937 \cdot 4 + 2298643951 \cdot 5 + 2548797521 \cdot 4] \\ &= -29787881472, \\ \tau_{19}(16) &= -1 - [Q_{17}(-7,16)H(-15) + Q_{17}(-3,16)H(-55) + Q_{17}(1,16)H(-63) \\ &\quad + Q_{17}(5,16)H(-39)] \\ &= -1 - [-11441714823 \cdot 2 - 11007150467 \cdot 4 + 13408446465 \cdot 5 - 8853258555 \cdot 4] \\ &= 35282993498. \end{aligned}$$

Veamos entonces cuál es el valor de los $V_{i,j}(16)$ para $0 \leq i, j \leq 17$.

$$
\begin{aligned}
V_{0,0}(16) &= 1, \\
V_{1,1}(16) &= 1, \\
V_{2,0}(16) &= \tfrac{1}{2}(16V_{1,1}(16) + V_{1,-1}(16) - 17V_{0,0}(16)) \\
&= \tfrac{1}{2}(16 - 17) \\
&= -\tfrac{1}{2}, \\
V_{2,2}(16) &= \tfrac{1}{2}(16V_{1,3}(16) + V_{1,1}(16) - 17V_{0,2}(16)) \\
&= \tfrac{1}{2}, \\
V_{3,1}(16) &= \tfrac{1}{3}(16V_{2,2}(16) + V_{2,0}(16) - 16V_{1,1}(16)) \\
&= \tfrac{1}{3}(16\tfrac{1}{2} + (-\tfrac{1}{2}) - 16) \\
&= -\tfrac{17}{6}, \\
V_{3,3}(16) &= \tfrac{1}{3}(16V_{2,4}(16) + V_{2,2}(16) - 16V_{1,3}(16)) \\
&= \tfrac{1}{3}(\tfrac{1}{2}) \\
&= \tfrac{1}{6}, \\
V_{4,0}(16) &= \tfrac{1}{4}(16V_{3,1}(16) + V_{3,-1}(16) - 15V_{2,0}(16)) \\
&= \tfrac{1}{4}(16(-\tfrac{17}{6}) - 15(-\tfrac{1}{2})) \\
&- \tfrac{227}{24}, \\
V_{4,2}(16) &= \tfrac{1}{4}(16V_{3,3}(16) + V_{3,1}(16) - 15V_{2,2}(16)) \\
&= \tfrac{1}{4}(16\tfrac{1}{6} + (-\tfrac{17}{6}) - 15\tfrac{1}{2}) \\
&= -\tfrac{46}{24}, \\
V_{4,4}(16) &= \tfrac{1}{4}(16V_{3,5}(16) + V_{3,3}(16) - 15V_{2,4}(16)) \\
&= \tfrac{1}{4}(\tfrac{1}{6}) \\
&= \tfrac{1}{24}, \\
V_{5,1}(16) &= \tfrac{1}{5}(16V_{4,2}(16) + V_{4,0}(16) - 14V_{3,1}(16)) \\
&= \tfrac{1}{5}(16(-\tfrac{46}{24}) + (-\tfrac{227}{24}) - 14(-\tfrac{17}{6})) \\
&= -\tfrac{11}{120}, \\
V_{5,3}(16) &= \tfrac{1}{5}(16V_{4,4}(16) + V_{4,2}(16) - 14V_{3,3}(16)) \\
&= \tfrac{1}{5}(16\tfrac{1}{24} + (-\tfrac{46}{24}) - 14\tfrac{1}{6}) \\
&= -\tfrac{86}{120}, \\
V_{5,5}(16) &= \tfrac{1}{5}(16V_{4,6}(16) + V_{4,4}(16) - 14V_{3,5}(16)) \\
&= \tfrac{1}{5}(\tfrac{1}{24}) \\
&= \tfrac{1}{120}, \\
V_{6,0}(16) &= \tfrac{1}{6}(16V_{5,1}(16) + V_{5,-1}(16) - 13V_{4,0}(16)) \\
&= \tfrac{1}{6}(16(-\tfrac{11}{120}) - 13(-\tfrac{227}{24})) \\
&= \tfrac{14579}{720}, \\
V_{6,2}(16) &= \tfrac{1}{6}(16V_{5,3}(16) + V_{5,1}(16) - 13V_{4,2}(16)) \\
&= \tfrac{1}{6}(16(-\tfrac{86}{120}) + (-\tfrac{11}{120}) - 13(-\tfrac{46}{24})) \\
&= \tfrac{1603}{720},
\end{aligned}
$$

$$
\begin{aligned}
V_{6,4}(16) &= \tfrac{1}{6}(16V_{5,5}(16) + V_{5,3}(16) - 13V_{4,4}(16)) \\
&= \tfrac{1}{6}(16\tfrac{1}{120} + (-\tfrac{86}{120}) - 13\tfrac{1}{24}) \\
&= -\tfrac{135}{720}, \\
V_{6,6}(16) &= \tfrac{1}{6}(16V_{5,7}(16) + V_{5,5}(16) - 13V_{4,6}(16)) \\
&= \tfrac{1}{6}(\tfrac{1}{120}) \\
&= \tfrac{1}{720}, \\
V_{7,1}(16) &= \tfrac{1}{7}(16V_{6,2}(16) + V_{6,0}(16) - 12V_{5,1}(16)) \\
&= \tfrac{1}{7}(16\tfrac{1603}{720} + \tfrac{14579}{720} - 12(-\tfrac{11}{120})) \\
&= \tfrac{41019}{5040}, \\
V_{7,3}(16) &= \tfrac{1}{7}(16V_{6,4}(16) + V_{6,2}(16) - 12V_{5,3}(16)) \\
&= \tfrac{1}{7}(16(-\tfrac{135}{720}) + \tfrac{1603}{720} - 12(-\tfrac{86}{120})) \\
&= \tfrac{5635}{5040}, \\
V_{7,5}(16) &= \tfrac{1}{7}(16V_{6,6}(16) + V_{6,4}(16) - 12V_{5,5}(16)) \\
&= \tfrac{1}{7}(16\tfrac{1}{720} + (-\tfrac{135}{720}) - 12\tfrac{1}{120}) \\
&= -\tfrac{191}{5040}, \\
V_{7,7}(16) &= \tfrac{1}{7}(16V_{6,8}(16) + V_{6,6}(16) - 12V_{5,7}(16)) \\
&= \tfrac{1}{7}(\tfrac{1}{720}) \\
&= \tfrac{1}{5040}, \\
V_{8,0}(16) &= \tfrac{1}{8}(16V_{7,1}(16) + V_{7,-1}(16) - 11V_{6,0}(16)) \\
&= \tfrac{1}{8}(16\tfrac{41019}{5040} - 11\tfrac{14579}{720}) \\
&= -\tfrac{466279}{40320}, \\
V_{8,2}(16) &= \tfrac{1}{8}(16V_{7,3}(16) + V_{7,1}(16) - 11V_{6,2}(16)) \\
&= \tfrac{1}{8}(16\tfrac{5635}{5040} + \tfrac{41019}{5040} - 11\tfrac{1603}{720}) \\
&= \tfrac{7748}{4032}, \\
V_{8,4}(16) &= \tfrac{1}{8}(16V_{7,5}(16) + V_{7,3}(16) - 11V_{6,4}(16)) \\
&= \tfrac{1}{8}(16(-\tfrac{191}{5040}) + \tfrac{5635}{5040} - 11(-\tfrac{135}{720})) \\
&= \tfrac{12974}{40320}, \\
V_{8,6}(16) &= \tfrac{1}{8}(16V_{7,7}(16) + V_{7,5}(16) - 11V_{6,6}(16)) \\
&= \tfrac{1}{8}(16\frac{1}{5040} + (-\tfrac{191}{5040}) - 11\tfrac{1}{720}) \\
&= -\tfrac{252}{40320}, \\
V_{8,8}(16) &= \tfrac{1}{8}(16V_{7,9}(16) + V_{7,7}(16) - 11V_{6,8}(16)) \\
&= \tfrac{1}{8}(\tfrac{1}{5040}) \\
&= \tfrac{1}{40320}, \\
V_{9,1}(16) &= \tfrac{1}{9}(16V_{8,2}(16) + V_{8,0}(16) - 10V_{7,1}(16)) \\
&= \tfrac{1}{9}(16\tfrac{7748}{40320} + (-\tfrac{466279}{40320}) - 10\tfrac{41019}{5040}) \\
&= -\tfrac{3623831}{362880}, \\
V_{9,3}(16) &= \tfrac{1}{9}(16V_{8,4}(16) + V_{8,2}(16) - 10V_{7,3}(16)) \\
&= \tfrac{1}{9}(16\tfrac{12974}{40320} + \tfrac{7748}{40320} - 10\tfrac{5635}{5040}) \\
&= -\tfrac{235468}{362880},
\end{aligned}
$$

$$
\begin{aligned}
V_{9,5}(16) &= \tfrac{1}{9}(16V_{8,6}(16) + V_{8,4}(16) - 10V_{7,5}(16)) \\
&= \tfrac{1}{9}(16(-\tfrac{252}{40320}) + \tfrac{12974}{40320} - 10(-\tfrac{191}{5040})) \\
&= \tfrac{24222}{362880}, \\
V_{9,7}(16) &= \tfrac{1}{9}(16V_{8,8}(16) + V_{8,6}(16) - 10V_{7,7}(16)) \\
&= \tfrac{1}{9}(16\tfrac{40320}{+}(-\tfrac{252}{40320}) - 10\tfrac{1}{5040}) \\
&= -\tfrac{316}{362880}, \\
V_{9,9}(16) &= \tfrac{1}{9}(16V_{8,10}(16) + V_{8,8}(16) - 10V_{7,9}(16)) \\
&= \tfrac{1}{9}(\tfrac{1}{40320}) \\
&= \tfrac{1}{362880}, \\
V_{10,0}(16) &= \tfrac{1}{10}(16V_{9,1}(16) + V_{9,-1}(16) - 9V_{8,0}(16)) \\
&= \tfrac{1}{10}(16(-\tfrac{3623831}{362880}) - 9(-\tfrac{466279}{40320})) \\
&= -\tfrac{20212697}{3628800}, \\
V_{10,2}(16) &= \tfrac{1}{10}(16V_{9,3}(16) + V_{9,1}(16) - 9V_{8,2}(16)) \\
&= \tfrac{1}{10}(16(-\tfrac{235468}{362880}) + (-\tfrac{3623831}{362880}) - 9\tfrac{7748}{40320}) \\
&= -\tfrac{8018907}{3628800}, \\
V_{10,4}(16) &= \tfrac{1}{10}(16V_{9,5}(16) + V_{9,3}(16) - 9V_{8,4}(16)) \\
&= \tfrac{1}{10}(16\tfrac{24222}{362880} + (-\tfrac{235468}{362880}) - 9\tfrac{12974}{40320}) \\
&= -\tfrac{898810}{3628800}, \\
V_{10,6}(16) &= \tfrac{1}{10}(16V_{9,7}(16) + V_{9,5}(16) - 9V_{8,6}(16)) \\
&= \tfrac{1}{10}(16(-\tfrac{316}{362880}) + \tfrac{24222}{362880} - 9(-\tfrac{252}{40320})) \\
&= \tfrac{39578}{3628800}, \\
V_{10,8}(16) &= \tfrac{1}{10}(16V_{9,9}(16) + V_{9,7}(16) - V_{8,8}(16) \\
&= \tfrac{1}{10}(16\tfrac{1}{362880} + (-\tfrac{316}{362880}) - 9\tfrac{1}{40320}) \\
&= -\tfrac{381}{3628800}, \\
V_{10,10}(16) &= \tfrac{1}{10}(16V_{9,11}(16) + V_{9,9}(16) - 9V_{8,10}(16)) \\
&= \tfrac{1}{10}(\tfrac{1}{362880}) \\
&= \tfrac{1}{3628800}, \\
V_{11,1}(16) &= \tfrac{1}{11}(16V_{10,2}(16) + V_{10,0}(16) - 8V_{9,1}(16)) \\
&= \tfrac{1}{11}(16(-\tfrac{8018907}{3628800}) + (-\tfrac{20212697}{3628800}) - 8(-\tfrac{3623831}{362880})) \\
&= \tfrac{141391271}{39916800}, \\
V_{11,3}(16) &= \tfrac{1}{11}(16V_{10,4}(16) + V_{10,2}(16) - 8V_{9,3}(16)) \\
&= \tfrac{1}{11}(16(-\tfrac{898810}{3628800}) + (-\tfrac{8018907}{3628800}) - 8(-\tfrac{235468}{362880})) \\
&= -\tfrac{3562427}{39916800}, \\
V_{11,5}(16) &= \tfrac{1}{11}(16V_{10,6}(16) + V_{10,4}(16) - 8V_{9,5}(16)) \\
&= \tfrac{1}{11}(16\tfrac{39578}{3628800} + (-\tfrac{898810}{3628800} - 8\tfrac{24222}{362880})) \\
&= -\tfrac{2203322}{39916800}, \\
V_{11,7}(16) &= \tfrac{1}{11}(16V_{10,8}(16) + V_{10,6}(16) - 8V_{9,7}(16)) \\
&= \tfrac{1}{11}(16(-\tfrac{381}{3628800}) + \tfrac{39578}{3628800} - 8(-\tfrac{316}{362880})) \\
&= \tfrac{58762}{39916800},
\end{aligned}
$$

$$
\begin{aligned}
V_{11,9}(16) &= \tfrac{1}{11}(16V_{10,10}(16) + V_{10,8}(16) - 8V_{9,9}(16)) \\
&= \tfrac{1}{11}(16\tfrac{1}{3628800} + (-\tfrac{381}{3628800}) - 8\tfrac{1}{362880}) \\
&= -\tfrac{445}{39916800}, \\
V_{11,11}(16) &= \tfrac{1}{11}(16V_{10,12}(16) + V_{10,10}(16) - 8V_{9,11}(16)) \\
&= \tfrac{1}{11}(\tfrac{1}{3628800}) \\
&= \tfrac{1}{39916800}, \\
V_{12,0}(16) &= \tfrac{1}{12}(16V_{11,1}(16) + V_{11,-1}(16) - 7V_{10,0}(16)) \\
&= \tfrac{1}{12}(16\tfrac{141391271}{39916800} - 7(-\tfrac{20212697}{3628800})) \\
&= \tfrac{3818638005}{479001600}, \\
V_{12,2}(16) &= \tfrac{1}{12}(16V_{11,3}(16) + V_{11,1}(16) - 7V_{10,2}(16)) \\
&= \tfrac{1}{12}(16(-\tfrac{3562427}{39916800}) + \tfrac{141391271}{39916800} - 7(-\tfrac{8018907}{3628800})) \\
V_{12,4}(16) &= \tfrac{1}{12}(16V_{11,5}(16) + V_{11,3}(16) - 7V_{10,4}(16)) \\
&= \tfrac{1}{12}(16(-\tfrac{2203322}{39916800}) + (-\tfrac{3562427}{39916800}) - 7(-\tfrac{898810}{3628800})) \\
&= \tfrac{30392791}{479001600}, \\
V_{12,6}(16) &= \tfrac{1}{12}(16V_{11,7}(16) + V_{11,5}(16) - 7V_{10,6}(16)) \\
&= \tfrac{1}{12}(16\tfrac{58762}{39916800} + (-\tfrac{2203322}{39916800}) - 7\tfrac{39578}{3628800}) \\
&= -\tfrac{4310636}{479001600}, \\
V_{12,8}(16) &= \tfrac{1}{12}(16V_{11,9}(16) + V_{11,7}(16) - 7V_{10,8}(16)) \\
&= \tfrac{1}{12}(16(-\tfrac{445}{39916800}) + \tfrac{58762}{39916800} - 7(-\tfrac{381}{3628800})) \\
&= \tfrac{80979}{479001600}, \\
V_{12,10}(16) &= \tfrac{1}{12}(16V_{11,11}(16) + V_{11,9}(16) - 7V_{10,10}(16)) \\
&= \tfrac{1}{12}(16\tfrac{1}{39916800} + (-\tfrac{445}{39916800}) - 7\tfrac{1}{3628800}) \\
&= -\tfrac{506}{479001600}, \\
V_{12,12}(16) &= \tfrac{1}{12}(16V_{11,13}(16) + V_{11,11}(16) - 7V_{10,12}(16)) \\
&= \tfrac{1}{12}(\tfrac{1}{39916800}) \\
&= \tfrac{1}{479001600}, \\
V_{13,1}(16) &= \tfrac{1}{13}(16V_{12,2}(16) + V_{12,0}(16) - 6V_{11,1}(16)) \\
&= \tfrac{1}{13}(16\tfrac{701848278}{479001600} + \tfrac{3818638005}{479001600} - 6\tfrac{141391271}{39916800}) \\
&= \tfrac{4868038941}{6227020800}, \\
V_{13,3}(16) &= \tfrac{1}{13}(16V_{12,4}(16) + V_{12,2}(16) - 6V_{11,3}(16)) \\
&= \tfrac{1}{13}(16\tfrac{30392791}{479001600} + \tfrac{701848278}{479001600} - 6(-\tfrac{3562427}{39916800})) \\
&= \tfrac{1444627678}{6227020800}, \\
V_{13,5}(16) &= \tfrac{1}{13}(16V_{12,6}(16) + V_{12,4}(16) - 6V_{11,5}(16)) \\
&= \tfrac{1}{13}(16(-\tfrac{4310636}{479001600}) + \tfrac{30392791}{479001600} - 6(-\tfrac{2203322}{39916800})) \\
&= \tfrac{120061799}{6227020800}, \\
V_{13,7}(16) &= \tfrac{1}{13}(16V_{12,8}(16) + V_{12,6}(16) - 6V_{11,7}(16)) \\
&= \tfrac{1}{13}(16\tfrac{80979}{479001600} + (-\tfrac{4310636}{479001600}) - 6\tfrac{58762}{39916800}) \\
&= -\tfrac{7245836}{6227020800},
\end{aligned}
$$

$$
\begin{aligned}
V_{13,9}(16) &= \tfrac{1}{13}(16V_{12,10}(16) + V_{12,8}(16) - 6V_{11,9}(16)) \\
&= \tfrac{1}{13}(16(-\tfrac{506}{479001600}) + \tfrac{80979}{479001600} - 6(-\tfrac{445}{39916800})) \\
&= \tfrac{104923}{6227020800}, \\
V_{13,11}(16) &= \tfrac{1}{13}(16V_{12,12}(16) + V_{12,10}(16) - 6V_{11,11}(16)) \\
&= \tfrac{1}{13}(16\tfrac{1}{479001600} + (-\tfrac{506}{479001600}) - 6\tfrac{1}{39916800}) \\
&= -\tfrac{562}{6227020800}, \\
V_{13,13}(16) &= \tfrac{1}{13}(16V_{12,14}(16) + V_{12,12}(16) - 6V_{11,13}(16)) \\
&= \tfrac{1}{13}(\tfrac{1}{479001600}) \\
&= \tfrac{1}{6227020800}, \\
V_{14,0}(16) &= \tfrac{1}{14}(16V_{13,1}(16) + V_{13,-1}(16) - 5V_{12,0}(16)) \\
&= \tfrac{1}{14}(16\tfrac{4868038941}{6227020800} - 5\tfrac{3818638005}{479001600}) \\
&= -\tfrac{170322847269}{87178291200}, \\
V_{14,2}(16) &= \tfrac{1}{14}(16V_{13,3}(16) + V_{13,1}(16) - 5V_{12,2}(16)) \\
&= \tfrac{1}{14}(16\tfrac{1444627678}{6227020800} + \tfrac{4868038941}{6227020800} - 5\tfrac{701848278}{479001600}) \\
&= -\tfrac{17638056281}{87178291200}, \\
V_{14,4}(16) &= \tfrac{1}{14}(16V_{13,5}(16) + V_{13,3}(16) - 5V_{12,4}(16)) \\
&= \tfrac{1}{14}(16\tfrac{120061799}{6227020800} + \tfrac{1444627678}{6227020800} - 5\tfrac{30392791}{479001600}) \\
&= \tfrac{1390085047}{87178291200}, \\
V_{14,6}(16) &= \tfrac{1}{14}(16V_{13,7}(16) + V_{13,5}(16) - 5V_{12,6}(16)) \\
&= \tfrac{1}{14}(16(-\tfrac{7245836}{6227020800}) + \tfrac{120061799}{6227020800} - 5(-\tfrac{4310636}{479001600})) \\
&= \tfrac{284319763}{87178291200}, \\
V_{14,8}(16) &= \tfrac{1}{14}(16V_{13,9}(16) + V_{13,7}(16) - 5V_{12,8}(16)) \\
&= \tfrac{1}{14}(16\tfrac{104923}{6227020800} + (-\tfrac{7245836}{6227020800}) - 5\tfrac{80979}{479001600}) \\
&= -\tfrac{10830703}{87178291200}, \\
V_{14,10}(16) &= \tfrac{1}{14}(16V_{13,11}(16) + V_{13,9}(16) - 5V_{12,10}(16)) \\
&= \tfrac{1}{14}(16(-\tfrac{562}{6227020800}) + \tfrac{104923}{6227020800} - 5(-\tfrac{506}{479001600})) \\
&= \tfrac{128821}{87178291200}, \\
V_{14,12}(16) &= \tfrac{1}{14}(16V_{13,13}(16) + V_{13,11}(16) - 5V_{12,12}(16)) \\
&= \tfrac{1}{14}(16\tfrac{1}{6227020800} + (-\tfrac{562}{6227020800}) - 5\tfrac{1}{479001600}) \\
&= -\tfrac{611}{87178291200}, \\
V_{14,14}(16) &= \tfrac{1}{14}(16V_{13,15}(16) + V_{13,13}(16) - 5V_{12,14}(16)) \\
&= \tfrac{1}{14}(\tfrac{1}{6227020800}) \\
&= \tfrac{1}{87178291200}, \\
V_{15,1}(16) &= \tfrac{1}{15}(16V_{14,2}(16) + V_{14,0}(16) - 4V_{13,1}(16)) \\
&= \tfrac{1}{15}(16(-\tfrac{17638056281}{87178291200}) + (-\tfrac{170322847269}{87178291200}) - 4\tfrac{4868038941}{6227020800}) \\
&= -\tfrac{725141928461}{87178291200\cdot 15}, \\
V_{15,3}(16) &= \tfrac{1}{15}(16V_{14,4}(16) + V_{14,2}(16) - 4V_{13,3}(16)) \\
&= \tfrac{1}{15}(16\tfrac{1390085047}{87178291200} + (-\tfrac{17638056281}{87178291200}) - 4\tfrac{1444627678}{6227020800}) \\
&= -\tfrac{76295845497}{87178291200\cdot 15},
\end{aligned}
$$

$$
\begin{aligned}
V_{15,5}(16) &= \tfrac{1}{15}(16V_{14,6}(16) + V_{14,4}(16) - 4V_{13,5}(16)) \\
&= \tfrac{1}{15}(16\tfrac{284319763}{87178291200} + \tfrac{1390085047}{87178291200} - 4\tfrac{120061799}{6227020800}) \\
&= -\tfrac{784259489}{87178291200\cdot 15}, \\
V_{15,7}(16) &= \tfrac{1}{15}(16V_{14,8}(16) + V_{14,6}(16) - 4V_{13,7}(16)) \\
&= \tfrac{1}{15}(16(-\tfrac{10830703}{87178291200}) + \tfrac{284319763}{87178291200} - 4(-\tfrac{7245836}{6227020800})) \\
&= \tfrac{516795331}{87178291200\cdot 15}, \\
V_{15,9}(16) &= \tfrac{1}{15}(16V_{14,10}(16) + V_{14,8}(16) - 4V_{13,9}(16)) \\
&= \tfrac{1}{15}(16\tfrac{128821}{87178291200} + (-\tfrac{10830703}{87178291200}) - 4\tfrac{104923}{6227020800}) \\
&= -\tfrac{14645255}{87178291200\cdot 15}, \\
V_{15,11}(16) &= \tfrac{1}{15}(16V_{14,12}(16) + V_{14,10}(16) - 4V_{13,11}(16)) \\
&= \tfrac{1}{15}(16(-\tfrac{611}{87178291200}) + \tfrac{128821}{87178291200} - 4(-\tfrac{562}{6227020800})) \\
&= \tfrac{150517}{87178291200\cdot 15}, \\
V_{15,13}(16) &= \tfrac{1}{15}(16V_{14,14}(16) + V_{14,2}(16) - 4V_{13,13}(16)) \\
&= \tfrac{1}{15}(16\tfrac{1}{87178291200} + (-\tfrac{611}{87178291200}) - 4\tfrac{1}{6227020800}) \\
&= -\tfrac{651}{87178291200\cdot 15}, \\
V_{15,15}(16) &= \tfrac{1}{15}(16V_{14,16}(16) + V_{14,14}(16) - 4V_{13,15}(16)) \\
&= \tfrac{1}{15}(\tfrac{1}{87178291200}) \\
&= \tfrac{1}{87178291200\cdot 15}, \\
V_{16,0}(16) &= \tfrac{1}{16}(16V_{15,1}(16) + V_{15,-1}(16) - 3V_{14,0}(16)) \\
&= \tfrac{1}{16}(16(-\tfrac{725141928461}{87178291200\cdot 15}) - 3(-\tfrac{170322847269}{87178291200})) \\
&= \tfrac{-16\cdot 725141928461 + 15\cdot 510968541807}{87178291200\cdot 240}, \\
V_{16,2}(16) &= \tfrac{1}{16}(16V_{15,3}(16) + V_{15,1}(16) - 3V_{14,2}(16)) \\
&= \tfrac{1}{16}(16(-\tfrac{76295845497}{87178291200\cdot 15}) - \tfrac{725141928461}{87178291200\cdot 15} - 3(-\tfrac{17638056281}{87178291200})) \\
&= \tfrac{-16\cdot 76295845497 - 725141928461 + 15\cdot 52914168843}{87178291200\cdot 240}, \\
V_{16,4}(16) &= \tfrac{1}{16}(16V_{15,5}(16) + V_{15,3}(16) - 3V_{14,4}(16)) \\
&= \tfrac{1}{16}(16(-\tfrac{784259489}{87178291200\cdot 15}) - \tfrac{76295845497}{87178291200\cdot 15} - 3\tfrac{1390085047}{87178291200}) \\
&= -\tfrac{151397824436}{}, \\
V_{16,6}(16) &= \tfrac{1}{16}(16V_{15,7}(16) + V_{15,5}(16) - 3V_{14,6}(16)) \\
&= \tfrac{1}{16}(16\tfrac{516795331}{87178291200\cdot 15} - \tfrac{784259489}{87178291200\cdot 15} - 3\tfrac{284319763}{87178291200}) \\
&= -\tfrac{5309923528}{87178291200\cdot 240}, \\
V_{16,8}(16) &= \tfrac{1}{16}(16V_{15,9}(16) + V_{15,7}(16) - 3V_{14,8}(16)) \\
&= \tfrac{1}{16}(16(-\tfrac{14645255}{87178291200\cdot 15}) + \tfrac{516795331}{87178291200\cdot 15} - 3(-\tfrac{10830703}{87178291200})) \\
&= \tfrac{769852886}{87178291200\cdot 240}, \\
V_{16,10}(16) &= \tfrac{1}{16}(16V_{15,11}(16) + V_{15,9}(16) - 3V_{14,10}(16)) \\
&= \tfrac{1}{16}(16\tfrac{150517}{87178291200\cdot 15} - \tfrac{14645255}{87178291200\cdot 15} - 3\tfrac{128821}{87178291200}) \\
&= -\tfrac{18033928}{87178291200\cdot 240}, \\
V_{16,12}(16) &= \tfrac{1}{16}(16V_{15,13}(16) + V_{15,11}(16) - 3V_{14,12}(16)) \\
&= \tfrac{1}{16}(16(-\tfrac{651}{87178291200\cdot 15}) + \tfrac{150517}{87178291200\cdot 15} - 3(-\tfrac{611}{87178291200})) \\
&= \tfrac{167596}{87178291200\cdot 240},
\end{aligned}
$$

$$
\begin{aligned}
V_{16,14}(16) &= \tfrac{1}{16}(16V_{15,15}(16) + V_{15,13}(16) - 3V_{14,14}(16)) \\
&= \tfrac{1}{16}(16\frac{1}{87178291200 \cdot 15} - \tfrac{651}{87178291200\cdot 15} - 3\tfrac{1}{87178291200}) \\
&= -\tfrac{680}{87178291200\cdot 240}, \\
V_{16,16}(16) &= \tfrac{1}{16}(16V_{15,17}(16) + V_{15,15}(16) - 3V_{14,16}(16)) \\
&= \tfrac{1}{16}(\tfrac{1}{87178291200\cdot 15}) \\
&= \tfrac{1}{87178291200\cdot 240}, \\
V_{17,1}(16) &= \tfrac{1}{17}(16V_{16,2}(16) + V_{16,0}(16) - 2V_{15,1}(16)) \\
&= \tfrac{1}{17}(16\tfrac{-16\cdot 76295845497-725141928461+15\cdot 52914168843}{87178291200\cdot 240} + \tfrac{-16\cdot 725141928461+15\cdot 510968541807}{87178291200\cdot 240} \\
&- 2(-\tfrac{725141928461}{87178291200\cdot 15})) \\
&= \tfrac{16(-16\cdot 76295845497-725141928461+15\cdot 52914168843)-16\cdot 725141928461+15\cdot 510968541807+32\cdot 725141928461}{87178291200\cdot 4080}, \\
V_{17,3}(16) &= \tfrac{1}{17}(16V_{16,4}(16) + V_{16,2}(16) - 2V_{15,3}(16)) \\
&= \tfrac{1}{17}(16(-\tfrac{151397824436}{87178291200\cdot 240} + \tfrac{-16\cdot 76295845497-725141928461+15\cdot 52914168843}{87178291200\cdot 240} \\
&- 2(-\tfrac{76295845497}{87178291200\cdot 15})) \\
&= \tfrac{-16\cdot 151397824416\cdot 76295845497-725141928461+15\cdot 52914168843+32\cdot 76295845497}{87178291200\cdot 4080}, \\
V_{17,5}(16) &= \tfrac{1}{17}(16V_{16,6}(16) + V_{16,4}(16) - 2V_{15,5}(16)) \\
&= \tfrac{1}{17}(16(-\tfrac{5309923528}{87178291200\cdot 240}) - \tfrac{151397824436}{87178291200\cdot 240} - 2(-\tfrac{784259489}{87178291200\cdot 15})) \\
&= -\tfrac{211260297236}{87178291200\cdot 4080}, \\
V_{17,7}(16) &= \tfrac{1}{17}(16V_{16,8}(16) + V_{16,6}(16) - 2V_{15,7}(16)) \\
&= \tfrac{1}{17}(16\tfrac{769852886}{87178291200\cdot 240} - \tfrac{5309923528}{87178291200\cdot 240} - 2\tfrac{516795331}{87178291200\cdot 15}) \\
&= -\tfrac{9529727944}{87178291200\cdot 4080}, \\
V_{17,9}(16) &= \tfrac{1}{17}(16V_{16,10}(16) + V_{16,8}(16) - 2V_{15,9}(16)) \\
&= \tfrac{1}{17}(16(-\tfrac{18033928}{87178291200\cdot 240}) + \tfrac{769852886}{87178291200\cdot 240} - 2(-\tfrac{14645255}{87178291200\cdot 15})) \\
&= \tfrac{949958198}{87178291200\cdot 4080}, \\
V_{17,11}(16) &= \tfrac{1}{17}(16V_{16,12}(16) + V_{16,10}(16) - 2V_{15,11}(16)) \\
&= \tfrac{1}{17}(16\tfrac{167596}{87178291200\cdot 240} - \tfrac{18033928}{87178291200\cdot 240} - 2\tfrac{150517}{87178291200\cdot 15}) \\
&= -\tfrac{20168936}{87178291200\cdot 4080}, \\
V_{17,13}(16) &= \tfrac{1}{17}(16V_{16,14}(16) + V_{16,12}(16) - 2V_{15,13}(16)) \\
&= \tfrac{1}{17}(16(\tfrac{680}{87178291200\cdot 240}) + \tfrac{167596}{87178291200\cdot 240} - 2(-\tfrac{651}{87178291200})) \\
&= \tfrac{177548}{87178291200\cdot 4080}, \\
V_{17,15}(16) &= \tfrac{1}{17}(16V_{16,16}(16) + V_{16,14}(16) - 2V_{15,15}(16)) \\
&= \tfrac{1}{17}(16\tfrac{1}{87178291200\cdot 240} - \tfrac{680}{87178291200\cdot 240} - 2\tfrac{1}{87178291200\cdot 15}) \\
&= -\tfrac{696}{87178291200\cdot 4080}, \\
V_{17,17}(16) &= \tfrac{1}{17}(16V_{16,18}(16) + V_{16,16}(16) - 2V_{15,17}(16)) \\
&= \tfrac{1}{17}(\tfrac{1}{87178291200\cdot 240}) \\
&= \tfrac{1}{87178291200\cdot 4080}.
\end{aligned}
$$

Luego, la distribución de pesos del código Zetterberg $Z_2(4)$ está dada por

$$\begin{aligned}
256A_0 &= \tbinom{17}{0} - 17\,[V_{0,0}(16)(1+\tau_2(16))] \\
&= 1 - 17\,[1-16] \\
&= 256, \\
256A_1 &= \tbinom{17}{1} - 17\,[V_{1,1}(16)(1+\tau_3(16))] \\
&= 17 - 17\,[1+0] \\
&= 0, \\
256A_2 &= \tbinom{17}{2} - 17\,[V_{2,0}(16)(1+\tau_2(16)) + V_{2,2}(16)(1+\tau_4(16))] \\
&= 136 - 17\left[-\tfrac{1}{2}(1-16+\tfrac{1}{2}(1+0)\right] \\
&= 0, \\
256A_3 &= \tbinom{17}{3} - 17\,[V_{3,1}(16)(1+\tau_3(16)) + V_{3,3}(16)(1+\tau_5(16))] \\
&= 680 - 17\left[-\tfrac{17}{6}(1+0) + \tfrac{1}{6}(1+256)\right] \\
&= 0, \\
256A_4 &= \tbinom{17}{4} - 17\,[V_{4,0}(16)(1+\tau_2(16)) + V_{4,2}(16)(1+\tau_4(16)) + V_{4,4}(16)(1+\tau_6(16))] \\
&= 2380 - 17\left[-\tfrac{227}{24}(1-16) - \tfrac{46}{24}(1+0) + \tfrac{1}{24}(1+0)\right] \\
&= 0, \\
256A_5 &= \tbinom{17}{5} - 17\,[V_{5,1}(16)(1+\tau_3(16)) + V_{5,3}(16)(1+\tau_5(16)) + V_{5,5}(16)(1+\tau_7(16))] \\
&= 6188 - 17\left[-\tfrac{11}{120}(1+0) - \tfrac{86}{120}(1+256) + \tfrac{1}{120}(1+4352)\right] \\
&= 8704, \\
256A_6 &= \tbinom{17}{6} - 17[V_{6,0}(16)(1+\tau_2(16)) + V_{6,2}(16)(1+\tau_4(16)) + V_{6,4}(16)(1+\tau_6(16)) \\
&\quad + V_{6,6}(16)(1+\tau_8(16))] \\
&= 12376 - 17\left[\tfrac{14579}{720}(1-16) + \tfrac{1603}{720}(1+0) - \tfrac{135}{720}(1+0) + \tfrac{1}{720}(1+4096)\right] \\
&= 17408, \\
256A_7 &= \tbinom{17}{7} - 17[V_{7,1}(16)(1+\tau_3(16)) + V_{7,3}(16)(1+\tau_5(16)) + V_{7,5}(16)(1+\tau_7(16)) \\
&\quad + V_{7,7}(16)(1+\tau_9(16))] \\
&= 19448 - 17[\tfrac{41019}{5040}(1+0) + \tfrac{5635}{5040}(1+256) - \tfrac{191}{5040}(1+4352) + \tfrac{1}{5040}(1-52992)] \\
&= 17408, \\
256A_8 &= \tbinom{17}{8} - 17[V_{8,0}(16)(1+\tau_2(16)) + V_{8,2}(16)(1+\tau_4(16)) + V_{8,4}(16)(1+\tau_6(16)) \\
&\quad + V_{8,6}(16)(1+\tau_8(16)) + V_{8,8}(16)(1+\tau_{10}(16))] \\
&= 24310 - 17[-\tfrac{466279}{40320}(1-16) + \tfrac{7748}{40320}(1+0) + \tfrac{12974}{40320}(1+0) - \tfrac{252}{40320}(1+4096) \\
&\quad + \tfrac{1}{40320}(1+65536)] \\
&= 21760, \\
256A_9 &= \tbinom{17}{9} - 17[V_{9,1}(16)(1+\tau_3(16)) + V_{9,3}(16)(1+\tau_5(16)) + V_{9,5}(16)(1+\tau_7(16)) \\
&\quad + V_{9,7}(16)(1+\tau_9(16)) + V_{9,9}(16)(1+\tau_{11}(16))] \\
&= 24310 - 17[-\tfrac{3623831}{362880}(1+0) - \tfrac{235468}{362880}(1+256) + \tfrac{24222}{362880}(1+4352) \\
&\quad - \tfrac{316}{362880}(1-52992) + \tfrac{1}{362880}(1-3612416)] \\
&= 21760,
\end{aligned}$$

$$
\begin{aligned}
256A_{10} &= \tbinom{17}{10} - 17[V_{10,0}(16)(1+\tau_2(16)) + V_{10,2}(16)(1+\tau_4(16)) + V_{10,4}(16)(1+\tau_6(16)) \\
&\quad + V_{10,6}(16)(1+\tau_8(16)) + V_{10,8}(16)(1+\tau_{10}(16)) + V_{10,10}(16)(1+\tau_{12}(16))] \\
&= 19448 - 17[-\tfrac{20212697}{3628800}(1-16) - \tfrac{8018907}{3628800}(1+0) - \tfrac{898810}{3628800}(1+0) + \tfrac{39578}{3628800}(1+4096) \\
&\quad - \tfrac{381}{3628800}(1+65536) + \tfrac{1}{3628800}(1+4001792)] \\
&= 17408, \\
256A_{11} &= \tbinom{17}{11} - 17[V_{11,1}(16)(1+\tau_3(16)) + V_{11,3}(16)(1+\tau_5(16)) + V_{11,5}(16)(1+\tau_7(16)) \\
&\quad + V_{11,7}(16)(1+\tau_9(16)) + V_{11,9}(16)(1+\tau_{11}(16)) + V_{11,11}(16)(1+\tau_{13}(16))] \\
&= 12376 - 17[\tfrac{141391271}{39916800}(1+0) - \tfrac{3562427}{39916800}(1+256) - \tfrac{2203322}{39916800}(1+4352) \\
&\quad + \tfrac{58762}{39916800}(1-52992) - \tfrac{445}{39916800}(1-3612416) + \tfrac{1}{39916800}(1+56172800)] \\
&= 17408, \\
256A_{12} &= \tbinom{17}{12} - 17[V_{12,0}(16)(1+\tau_2(16)) + V_{12,2}(16)(1+\tau_4(16)) + V_{12,4}(16)(1+\tau_6(16)) \\
&\quad + V_{12,6}(16)(1+\tau_8(16)) + V_{12,8}(16)(1+\tau_{10}(16)) + V_{12,10}(16)(1+\tau_{12}(16)) \\
&\quad + V_{12,12}(16)(1+\tau_{14}(16))] \\
&= 6188 - 17[\tfrac{3818638005}{479001600}(1-16) + \tfrac{701848278}{479001600}(1+0) + \tfrac{30392791}{479001600}(1+0) \\
&\quad - \tfrac{4310636}{479001600}(1+4096) + \tfrac{80979}{479001600}(1+65536) - \tfrac{506}{479001600}(1+4001792) \\
&\quad + \tfrac{1}{479001600}(1+33554432)] \\
&= 8704, \\
256A_{13} &= \tbinom{17}{13} - 17[V_{13,1}(16)(1+\tau_3(16)) + V_{13,3}(16)(1+\tau_5(16)) + V_{13,5}(16)(1+\tau_7(16)) \\
&\quad + V_{13,7}(16)(1+\tau_9(16)) + V_{13,9}(16)(1+\tau_{11}(16)) + V_{13,11}(16)(1+\tau_{13}(16)) \\
&\quad + V_{13,13}(16)(1+\tau_{15}(16))] \\
&= 2380 - 17[\tfrac{4868038941}{6227020800}(1+0) + \tfrac{1444627678}{6227020800}(1+256) + \tfrac{120061799}{6227020800}(1+4352) \\
&\quad - \tfrac{7245836}{6227020800}(1-52992) + \tfrac{104923}{6227020800}(1-3612416) - \tfrac{562}{6227020800}(1+56172800) \\
&\quad + \tfrac{1}{6227020800}(1-353013504)] \\
&= 0, \\
256A_{14} &= \tbinom{17}{14} - 17[V_{14,0}(16)(1+\tau_2(16)) + V_{14,2}(16)(1+\tau_4(16)) + V_{14,4}(16)(1+\tau_6(16)) \\
&\quad + V_{14,6}(16)(1+\tau_8(16)) * V_{14,8}(16)(1+\tau_{10}(16)) + V_{14,10}(16)(1+\tau_{12}(16)) \\
&\quad + V_{14,12}(16)(1+\tau_{14}(16)) + V_{14,14}(16)(1+\tau_{16}(16))] \\
&= 680 - 17[-\tfrac{170322847269}{87178291200}(1-16) - \tfrac{17638056281}{87178291200}(1+0) + \tfrac{1390085047}{87178291200}(1+0) \\
&\quad + \tfrac{284319763}{87178291200}(1+4096) - \tfrac{10830703}{87178291200}(1+65536) + \tfrac{128821}{87178291200}(1+4001792) \\
&\quad - \tfrac{611}{87178291200}(1+33554432) + \tfrac{1}{87178291200}(1-1522593792)] \\
&= 0, \\
256A_{15} &= \tbinom{17}{15} - 17[V_{15,1}(16)(1+\tau_3(16)) + V_{15,3}(16)(1+\tau_5(16)) + V_{15,5}(16)(1+\tau_7(16)) \\
&\quad + V_{15,7}(16)(1+\tau_9(16)) + V_{15,9}(16)(1+\tau_{11}(16)) + V_{15,11}(16)(1+\tau_{13}(16)) \\
&\quad + V_{15,13}(16)(1+\tau_{15}(16)) + V_{15,15}(16)(1+\tau_{17}(16))] \\
&= 136 - 17[-\tfrac{725141928461}{87178291200\cdot 15}(1+0) - \tfrac{76295845497}{87178291200\cdot 15}(1+256) - \tfrac{784259489}{87178291200\cdot 15}(1+4352) \\
&\quad + \tfrac{516795331}{87178291200\cdot 15}(1-52992) - \tfrac{14645255}{87178291200\cdot 15}(1-3612416) + \tfrac{150517}{87178291200\cdot 15}(1+56172800) \\
&\quad - \tfrac{651}{87178291200\cdot 15}(1-353013504) + \tfrac{1}{87178291200\cdot 15}(1+4439986432)] \\
&= 0,
\end{aligned}
$$

$$
\begin{aligned}
256A_{16} &= \tbinom{17}{16} - 17[V_{16,0}(16)(1+\tau_2(16)) + V_{16,2}(16)(1+\tau_4(16)) + V_{16,4}(16)(1+\tau_6(16)) \\
&\quad + V_{16,6}(16)(1+\tau_8(16)) + V_{16,8}(16)(1+\tau_{10}(16)) + V_{16,10}(16)(1+\tau_{12}(16)) \\
&\quad + V_{16,12}(16)(1+\tau_{14}(16)) + V_{16,14}(16)(1+\tau_{16}(16)) + V_{16,16}(16)(1+\tau_{18}(16)) \\
&= 17 - 17[\tfrac{-16\cdot 725141928461+15\cdot 510968541807}{87178291200\cdot 240}(1-16) \\
&\quad + \tfrac{-16\cdot 76295845497-725141928461+15\cdot 52914168843}{87178291200\cdot 240}(1+0) - \tfrac{151397824436}{87178291200\cdot 240}(1+0) \\
&\quad - \tfrac{5309923528}{87178291200\cdot 240}(1+4096) + \tfrac{769852886}{87178291200\cdot 240}(1+65536) - \tfrac{18033928}{87178291200\cdot 240}(1+4001792) \\
&\quad + \tfrac{167596}{87178291200\cdot 240}(1+33554432) - \tfrac{680}{87178291200\cdot 240}(1-1522593792) \\
&\quad + \tfrac{1}{87178291200\cdot 240}(1-29787881472)] \\
&= 0, \\
256A_{17} &= \tbinom{17}{17} - 17[V_{17,1}(16)(1+\tau_3(16)) + V_{17,3}(16)(1+\tau_5(16)) + V_{17,5}(16)(1+\tau_7(16)) \\
&\quad + V_{17,7}(16)(1+\tau_9(16)) + V_{17,9}(16)(1+\tau_{11}(16)) + V_{17,11}(16)(1+\tau_{13}(16)) \\
&\quad + V_{17,13}(16)(1+\tau_{15}(16)) + V_{17,15}(16)(1+\tau_{17}(16)) + V_{17,17}(16)(1+\tau_{19}(16))] \\
&= 1 - 17[(\tfrac{16(-16\cdot 76295845497-725141928461+15\cdot 52914168843)}{87178291200\cdot 4080} \\
&\quad - \tfrac{16\cdot 725141928461+15\cdot 510968541807+32\cdot 725141928461}{87178291200\cdot 4080})(1+0) \\
&\quad + \tfrac{-16\cdot 151397824416\cdot 76295845497-725141928461+15\cdot 52914168843+32\cdot 76295845497}{87178291200\cdot 4080}(1+256) \\
&\quad - \tfrac{211260297236}{87178291200\cdot 4080}(1+4352) - \tfrac{9529727944}{87178291200\cdot 4080}(1-52992) + \tfrac{949958198}{87178291200\cdot 4080}(1-3612416) \\
&\quad - \tfrac{20168936}{87178291200\cdot 4080}(1+56172800) + \tfrac{177548}{87178291200\cdot 4080}(1-353013504) \\
&\quad - \tfrac{696}{87178291200\cdot 4080}(1+4439986432) + \tfrac{1}{87178291200\cdot 4080}(1+35282993408)] \\
&= 256.
\end{aligned}
$$

Por lo tanto, el espectro de $Z_2(4)$ es

$$
\begin{aligned}
A_0 &= A_{17} = 1, \\
A_1 &= A_{16} = 0, \\
A_2 &= A_{15} = 0, \\
A_3 &= A_{14} = 0, \\
A_4 &= A_{13} = 0, \\
A_5 &= A_{12} = 34, \\
A_6 &= A_{11} = 68, \\
A_7 &= A_{10} = 68, \\
A_8 &= A_9 = 85.
\end{aligned}
$$

Bibliografía

[1] R.C. Bose, D.K. Ray-Chaudhuri. *On a class of error correcting binary group codes*. Inform. and Control 3 (68–79) 1960.

[2] R.C. Bose, D.K. Ray-Chaudhuri. *Further results on error correcting binary group codes*. Inform. and Control 3 (279–290) 1960.

[3] B.C. Berndt, R.J. Evans, K.S. Williams. *Gauss and Jacobi Sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.

[4] L. Chihara, D. Stanton. *Zeros of generalized Krawtchouk polynomials*. J. Approx. Theory **60:1** (43–57) 1990.

[5] Henri Cohen. *Trace des operateur de Hecke sur* $\Gamma_0(N)$. Seminaire de Theorie des Nombres de Bordeaux (1–9) 1976.

[6] Keith Conrad. *On Weil?s proof of the bound for Kloosterman sums*. J. Number Theory **97** (439–446) 2002.

[7] Robert S. Coulter. *Explicit evaluations of some Weil sums*. Acta Arithmetica **83** (241–251) 1998.

[8] Robert S. Coulter. *Further evaluations of Weil sums*. Acta Arithmetica **86** (217–226) 1998.

[9] Robert S. Coulter. *On the evaluation of a class of Weil sums in characteristic 2*. New Zealand J. Math. **28:2** (171–184) 1999.

[10] Philippe Delsarte. *On subfield subcodes of modified Reed-Solomon codes*. IEEE Transactions on Information Theory **21:5** (575–576) 1975.

[11] P. Diaconis, R. L. Graham. *The Radon transform on* $\mathbb{Z}_2^k$. Pacific J. Math. **118:2** (323–345) 1985.

[12] F. Diamond, J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics, Springer-Verlag, 2008.

[13] Laurent Habsieger. *Integral zeroes of Krawtchouk polynomials*. Codes and association schemes, 151–165, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **56**, Amer. Math. Soc., 2001.

[14] Laurent Habsieger. *Integer zeros of q-Krawtchouk polynomials in classical combinatorics*. Special issue in honor of Dominique Foata's 65th birthday (Philadelphia, PA, 2000). Adv. in Appl. Math. **27:2-3** (427–437) 2001.

[15] L. Habsieger, D. Stanton. *More zeros of Krawtchouk polynomials*. Graphs Combin. **9:2** (163–172) 1993.

[16] Richard W. Hamming. *Error detecting and error correcting codes*. The Bell System Technical Journal **29:2** (147–160) 1950.

[17] T. Hiramatsu, G. Köhler. *Coding theory and number theory*. Mathematics and its applications. Kluwer Academic Publishers, 2003.

[18] Alexis Hocquenghem. *Codes correcteurs d'erreurs*. Chiffres (Paris) **2** (147–156) 1959.

[19] W.C. Huffman, V. Pless. *Fundamentals of error correcting codes*. Cambridge University Press, 2003.

[20] Norman E. Hurt. *Many rational points: coding theory and algebraic geormetry*. Mathematics and its applications. Springer science & Business Media, 2003.

[21] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1988.

[22] I. Krasikov, S. Litsyn. *On integral zeros of Krawtchouk polynomials*. J. Combin. Theory Ser. A **74:1** (71–99) 1996.

[23] I. Krasikov, S. Litsyn. *Survey of binary Krawtchouk polynomials*. Codes and association schemes, 199–211, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 56, Amer. Math. Soc., 2001.

[24] Dae S. Kim. *Weight distributions of Hamming codes (I)*. arXiv preprint arXiv:0710.1467 2007.

[25] Gilles Lachaud. *Distribution of the weights of the dual of the Melas code*. Discrete Mathematics **79:1** (103–106) 1990.

[26] V. Levenshtein. *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*. IEEE Trans. Inform. Theory **41:5** (1303–1321) 1995.

[27] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, revised edition, 1994.

[28] R. Lidl, H. Niederreiter. *Finite Fields*. Volume 20 of Encyclopedia of Mathematics and its Applications, 1997.

[29] Florence J. MacWilliams. *A theorem on the distribution of weights in a systematic code*. Bell System Technycal Journal **42:1** (79–94) 1963.

[30] F.J. MacWilliams, N.A.J. Sloane. *The theory of error correcting codes*. North-Holland Publishing Company, 1977.

[31] R. J. Miatello, R. A. Podestá, J. P. Rossetti. $\mathbb{Z}_2^k$*-manifolds are isospectral on forms*. Math. Zeitschrift **258** (301–317) 2008.

[32] R. J. Miatello, R. A. Podestá. *Spectral theory of the Atiyah-Patodi-Singer operator on compact flat manifolds*. Jour. Geom. Analysis **22** (1027–1054) 2012.

[33] R.J. Miatello, J.P. Rossetti. *Flat manifolds isospectral on p-forms*. Jour. Geom. Anal. **11** (649–667) 2001.

[34] G.L. Mullen, D. Panario. *Handbook of finite fields*. CRC Press, 2013.

[35] David E. Muller. *Application of Boolean algebra to switching circuit design and to error detection*. IEEE Trans. Computers **3** (6–12) 1954.

[36] Irving S. Reed. *A class of multiple-error-correcting codes and the decoding scheme*. IRE Trans. Inform. Theory IT-4 (38–49) 1954.

[37] Steven Roman. *Coding and information theory*. Graduate texts in Mathematics. Springer Verlag, 1992.

[38] René Schoof. *Families of curves and weight distributions of codes*. Bulletin of the American Mathematical Society **32:2** (171–180) 1995.

[39] R. Schoof, M. van der Vlugt. *Hecke operators and weight distribution of certain codes*. Journal of Combinatorial Theory Serie A, **57:2** (163–183) 1991.

[40] J.H. Silverman, J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer Verlag, 1992.

[41] S.A. Stepanov. *Arithmetic of Algebraic Curves*. Monographs in Contemporary Mathematics, Consultants Bureau, New York, 1994.

[42] M. Tsfasman, S. Vladut, D. Nogin. *Algebraic geometric codes: Basic notions*. American Mathematical Society, 2007.

[43] G. van der Geer, R. Schoof, M. van der Vlugt. *Weight formulas for ternary Melas codes*. Mathematics of Computation **58:198** (781–792) 1992.

[44] G. Van der Geer, M. van der Vlugt. *Artin-Schreier curves and codes*. Journal of Algebra **139:1** (256–272) 1991.

[45] Denis E. Videla. *Espectro de códigos cíclicos y grafos asociados*. Tesis Doctoral, FaMAF (UNC), 2018.

[46] Zhe-Xian. Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co. Inc., River Edge, NJ, 2003.

[47] William C. Waterhouse. *Abelian varietes over finite fields*. Annales scientifiques de l'Ecole Normale Supérieure **2:4** (521–560) 1969.

[48] Jacques Wolfmann. *The weights of the dual code of the Melas code over $GF(3)$.* Discrete Mathematics **74:3** (327–329) 1989.