Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas

Cotas superiores para códigos extremales

Vanessa Paola Ochoa Garcés

Trabajo presentado como requisito parcial para optar al título de Magíster en Matemáticas

Director: Dr. rer. nat. Ismael Gutiérrez García

Agradecimientos

Son numerosas las personas a quienes tengo que agradecer por ayudarme a obtener un logro más en mi vida.

Primeramente, mis más sinceros agradecimientos están dirigidos al más estupendo matemático que existe, al creador de un mundo que refleja matemáticas por doquier, a quién ha estado incondicionalmente conmigo, animándome a continuar pese a muchas dificultades. Me refiero a mi gran y mejor amigo, Jehová Dios. A él, a quien todo se lo debo.

También quiero agradecer a mis padres, Carlos y Amibel, que han sido un gran apoyo a lo largo de mi carrera, a mi estimado profesor Ismael Gutiérrez, quién ha sacado tanto tiempo de su apretado horario para colaborar en la pronta entrega de este trabajo, a todo el personal docente de la universidad del norte y a mis amigas Kelly, Yaridis, Andrea y Karina. Pero, hay alguien a quién agradezco especialmente, al amor de mi vida: Eduardo Mendoza.

Todas estas personas, de una u otra manera, han aportado para la culminación de mi trabajo de grado.

A todos, muchas gracias.

Introducción

Los códigos auto-duales son de gran importancia en la teoría de códigos ya que muchos de los más reconocidos códigos se caracterizan por ser de este tipo. Además, detrás de estos existe una teoría matemática amplia.

C.L. Mallows y N.J.A. Sloane obtuvieron, utilizando la teoría de invariantes, cotas superiores para la distancia mínima d y la longitud n de códigos auto-duales. Dichas cotas son llamadas las cotas de Mallows-Sloane. Sin embargo, Iwann Duursma utilizó otro método para obtener exactamente las mismas cotas y de forma mucho más sencilla. Su trabajo lo publicó en el 2001 en un documento titulado "Polinomios enumeradores de pesos de códigos extremales y ultraesféricos". Es un interesante trabajo, pero se encuentra incompleto. El objetivo de mi tesis es, precisamente, detallar el método utilizado por Duursma y ajustar esta teoría para probar las cotas superiores de Zhang Yuan-Sheng.

En el primer capítulo se encuentran los preliminares: conceptos básicos de la teoría de los códigos.

El primer resultado importante es el teorema 2.1.15, en donde se hallaron las siguientes cotas:

$$d + cd^{\perp} \leq n + c(c+1),$$

$$2d + cd^{\perp} \leq n + c(c+2).$$

Luego, en el teorema 2.2.1 se observa que es necesaria la condición $A_{d+c}/A_d \geq 0$ para la existencia de códigos con dichos parámetros. La obtención de las cotas de Mallows-Sloane se hallan en el teorema 2.3.5 y las cotas de Zhang Yuan-sheng, en el teorema 2.3.12.

Índice general

Capítulo 1

Preliminares

1.1. Generalidades

Consideraremos un conjunto finito $\mathbb{A} = \{a_1, ..., a_q\}$. A este conjunto lo llamaremos alfabeto. A sus elementos, $a_1, ..., a_q$ les llamamos letras o símbolos. Las sucesiones finitas de elementos de $\mathbb{A}$ se denominan palabras. La palabra $a_{i1}a_{i2}...a_{in}$ se dice que tiene longitud n. Una palabra de longitud n se puede considerar como un elemento de $\mathbb{A}^n$. A continuación, definiremos la distancia entre dos palabras de este tipo.

Definición 1.1.1 *Sean $\mathbb{A}$ un alfabeto con q elementos y $n \in \mathbb{N}$. Si $u, v \in \mathbb{A}^n$ con $u = (u_1, ..., u_n)$ y $v = (v_1, ..., v_n)$, entonces la distancia de Hamming entre u y v, notada $d(u, v)$, está definida así:*

$$d(u, v) := \left|\{j \mid u_j \neq v_j, j = 1, ..., n\}\right|.$$

Es decir, d cuenta el número de posiciones en que u y v difieren.

Teorema 1.1.2 *Sean $\mathbb{A}$ un alfabeto con $|\mathbb{A}| = q$ y $n \in \mathbb{N}$. Entonces:*

1. *d es una métrica sobre $\mathbb{A}$.*
2. *Si $\mathbb{A}$ es un grupo abeliano, notado aditivamente, entonces d es invariante bajo traslaciones. Esto es,*

   $$d(u, v) = d(u + w, v + w),$$

   para todo $u, v, w \in \mathbb{A}^n$.

DEMOSTRACIÓN.

1. Basta probar que

   $$d(u, v) \leq d(u, w) + d(w, v),$$

   puesto que, de la definición 1.1.1, se tiene inmediatamente que

I) $d(u,v) \geq 0$,

II) $d(u,v) = 0 \Leftrightarrow u = v$,

III) $d(u,v) = d(v,u)$.

Sean $u = (u_1, ..., u_j, ..., u_n)$, $v = (v_1, ..., v_j, ..., v_n)$ y $w = (w_1, ..., w_j, ..., w_n)$. Comparando sólo los términos de la posición j, tenemos que si $u_j \neq v_j$, entonces $u_j \neq w_j$ o $v_j \neq w_j$ pues, de lo contrario, $u_j = v_j$. Entonces,

$$d(u_j, v_j) = 1$$

y $d(u_j, w_j) + d(w_j, v_j)$ es o uno o dos. Al sumar todas las posiciones de u, v y w, siempre se verificará que:

$$d(u,v) \leq d(u,w) + d(w,v).$$

Esto demuestra que d es una métrica.

2. Si $u_j \neq v_j$, entonces $u_j + w_j \neq v_j + w_j$. Luego, se cumple que d es invariante bajo traslaciones.

□

A continuación, definiremos el concepto de código y, además, introduciremos algunos parámetros importantes.

Definición 1.1.3 *Sean $\mathbb{A}$ un alfabeto, $n \in \mathbb{N}$ y $C \subseteq \mathbb{A}^n$.*

1. *Si $|C| > 1$, entonces la distancia mínima de C con respecto a la distancia de Hamming, notada $d(C)$, se define así:*

$$d(C) := \min \{d(c_1, c_2) \mid c_1, c_2 \in C; c_1 \neq c_2\}.$$

2. *Si $|C| = 1$, entonces $d(C) := 0$.*

3. *Si $d(C) =: d$ y $|C| = M$, entonces diremos que C es un (n, M, d)-código y los números n, M y d se llamarán los parámetros del código.*

1.2. Códigos lineales

Es común considerar a $\mathbb{A}$ como un cuerpo finito. De ahora en adelante, nuestro alfabeto será un cuerpo finito y lo notaremos $\mathbb{K}$.

Definición 1.2.1 *Si $\mathbb{K} = \{a_1, ..., a_q\}$, un código q-ario sobre $\mathbb{K}$ es un subconjunto C del conjunto de todas las palabras sobre $\mathbb{K}$. Los elementos de C se llaman codewords. Si $n \in \mathbb{N}$ y C es un subespacio de $\mathbb{K}^n$, notado $C \preceq \mathbb{K}^n$, entonces diremos que C es un código lineal sobre $\mathbb{K}$ de longitud n. Si $\dim_{\mathbb{K}} C = k$, entonces es usual hablar de un $[n,k]$-código y si, además, $d(C) = d$ y $|\mathbb{K}| = q$, entonces diremos que C es un $[n,k,d]$-código o un $[n,k,d]_q$-código sobre $\mathbb{K}$.*

Definición 1.2.2 *Sea $n \in \mathbb{N}$. Entonces:*

1. *Para $x \in \mathbb{K}^n$, definimos el peso de x, notado $wt(x)$, de la siguiente manera:*

$$wt(x) := \left|\{j \mid x_j \neq 0, j = 1, ..., n\}\right|.$$

2. *Si $\{0\} \neq C \preceq \mathbb{K}^n$, entonces se define el peso mínimo de C, notado $wt(C)$, como:*

$$wt(C) := \min\{wt(x) \mid x \in C, x \neq 0\}.$$

   Si $C = \{0\}$, entonces $wt(C) := 0$.

3. *El soporte de $x = (x_1, ..., x_n) \in \mathbb{K}^n$, notado $sop(x)$,se define así:*

$$sop(x) := \{j \mid x_j \neq 0\}.$$

   Si $U \subseteq \mathbb{K}^n$, entonces $sop(U) := \bigcup_{u \in U} sop(u)$.

El siguiente teorema nos muestra que si un código es lineal, su distancia mínima puede hallarse con sólo determinar su peso mínimo y recíprocamente.

Teorema 1.2.3 *Si $C \neq \{0\}$ es un código lineal, entonces $wt(C) = d(C)$.*

DEMOSTRACIÓN.

$$\begin{aligned} d(C) &= \min\{d(c, c') \mid c, c' \in C; c \neq c'\} \\ &= \min\{d(c - c, c' - c) \mid c, c' \in C; c \neq c'\} \\ &= \min\{d(0, c' - c) \mid c, c' \in C; c \neq c'\} \\ &= \min\{d(0, c'') \mid c'' = c - c'; c, c', c'' \in C; c \neq c'\} \\ &= \min\{wt(c'') \mid c'' \in C, c'' \neq 0\} \\ &= wt(C). \end{aligned}$$

Luego, $d(C) = wt(C)$. □

Este último resultado es de suma importancia para efectos del cálculo. Calcular la distancia mínima sugiere realizar $\binom{|C|}{2}$ cálculos mientras que el peso mínimo implica realizar $|C| - 1$ cálculos. Para $|C|$ muy grande la diferencia es sustancial.

Definición 1.2.4 *Sean $|\mathbb{K}| = q$ y $n \in \mathbb{N}$. Definamos la función*

$$(\cdot|\cdot) : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}$$

de la siguiente manera: Para $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{K}^n$,

$$(x, y) \longmapsto (x|y) := \sum_{j=1}^{n} x_j y_j.$$

A continuación se demuestran algunas propiedades de la función $(\cdot|\cdot)$.

Lema 1.2.5 *Sean $u, v, w \in \mathbb{K}^n$ y $\alpha, \beta \in \mathbb{K}$. Entonces:*

1. $(u+v|w) = (u|w) + (v|w)$.
2. $(\alpha u|v) = \alpha(u|v)$.
3. $(u|v) = (v|u)$.
4. $(\bar{0}|v) = 0$, *con* $\bar{0} = (0, ..., 0)$.
5. *Si para todo $v \in \mathbb{K}^n$ se verifica que $(u|v) = 0$, entonces $u = \bar{0}$. Cuando esto sucede se dice que $(\cdot|\cdot)$ es una forma bilineal simétrica no degenerada.*

DEMOSTRACIÓN. Sean $u = (u_1, ..., u_n)$, $v = (v_1, ..., v_n)$ y $w = (w_1, ..., w_n)$. Entonces:

1.
$$\begin{aligned}(u+v|w) &= ((u_1+v_1, ..., u_n+v_n)|(w_1, ..., w_n)) \\ &= (u_1+v_1)w_1 + ... + (u_n+v_n)w_n \\ &= u_1w_1 + v_1w_1 + ... + u_nw_n + v_nw_n \\ &= (u_1w_1 + ... + u_nw_n) + (v_1w_1 + ... + v_nw_n) \\ &= (u|w) + (v|w).\end{aligned}$$

2.
$$\begin{aligned}(\alpha u|v) &= ((\alpha u_1, ..., \alpha u_n)|(v_1, ..., v_n)) \\ &= (\alpha u_1)v_1 + ... + (\alpha u_n)v_n \\ &= \alpha(u_1v_1) + ... + \alpha(u_nv_n) \\ &= \alpha(u_1v_1 + ... + u_nv_n) \\ &= \alpha(u|v).\end{aligned}$$

3.
$$\begin{aligned}(u|v) &= u_1v_1 + ... + u_nv_n \\ &= v_1u_1 + ... + v_nu_n \\ &= (v|u).\end{aligned}$$

4.
$$\begin{aligned}(\bar{0}|v) &= 0v_1 + ... + 0v_n \\ &= 0 + ... + 0 \\ &= 0.\end{aligned}$$

5. Sea $\beta = (e_1, ..., e_n)$ la base canónica para $\mathbb{K}^n$. Por hipótesis, se verifica que $(u|\beta) = 0$. Esto es, $(u|e_j) = 0$. Pero $(u|e_j) = u_j$. Entonces, $u = \bar{0}$.

□

Definición 1.2.6 *Sean C un $[n,k]$-código sobre $\mathbb{K}$ y $|\mathbb{K}| = q$.*

1. *El código dual de C, notado $C^\perp$, se define así:*

$$C^\perp := \{v \in \mathbb{K}^n \mid (c|v) = 0, \forall c \in C\}.$$

2. *C se llama auto-ortogonal si y sólo si $C \subseteq C^\perp$.*
3. *C se llama auto-dual si y sólo si $C = C^\perp$.*

Teorema 1.2.7 *Sean C un $[n,k]$-código sobre $\mathbb{K}$, $|\mathbb{K}| = q$ y $n \in \mathbb{N}$. Entonces:*

1. $(C^\perp)^\perp = C$.
2. *Si C es auto-dual, entonces $k = \frac{n}{2}$.*

DEMOSTRACIÓN.

1. Si $x \in C$ y $v \in C^\perp$, con x, v cualesquiera, entonces $(x|v) = 0$. Por lo tanto, $x \in (C^\perp)^\perp$ y se tiene que $C \subseteq (C^\perp)^\perp$.

   Demostramos ahora que $\dim_k C = \dim_k (C^\perp)^\perp$. Recordemos que si C es un $[n,k]$-código sobre $\mathbb{K}$, entonces $C^\perp$ es un $[n, n-k]$-código sobre $\mathbb{K}$. Por consiguiente,

$$\begin{aligned} \dim_k (C^\perp)^\perp &= n - \dim_k C^\perp \\ &= n - (n-k) \\ &= k \\ &= \dim_k C. \end{aligned}$$

   Tenemos, entonces, que $C \subseteq (C^\perp)^\perp$ y $\dim_k C = \dim_k (C^\perp)^\perp$. Esto nos permite concluir que $(C^\perp)^\perp = C$.

2. Si C es auto-dual, entonces $C = C^\perp$ y como $C^\perp$ es un $[n, n-k]$-código y C un $[n,k]$-código sobre $\mathbb{K}$, se tiene que $n - k = k$. Esto es, $k = \frac{n}{2}$.

□

Definición 1.2.8 *Sean $|\mathbb{K}| = q$, $C \preceq \mathbb{K}^n$ y $r, n \in \mathbb{N}$. Diremos que C es un código r-divisible si y sólo si se verifica que $r \mid wt(c)$, para todo $c \in C$. Además,*

1. *Si C es 2-divisible, entonces C se denomina par.*

2. *Si C es 4-divisible, entonces C se denomina doblemente par.*

Teorema 1.2.9 *Todo código lineal binario doblemente par es auto-ortogonal.*

DEMOSTRACIÓN. Sea C un código lineal binario doblemente par. Entonces, por definición, $4 \mid wt(c)$, para todo $c \in C$. Tomando $c, c' \in C$, con $c = (c_1, ..., c_n)$ y $c' = (c'_1, ..., c'_n)$, tendremos que

$$(c|c') = \sum_{j=1}^{n} c_i c'_i = |sop(c) \cap sop(c')|.$$

Además, se verifica que:

$$wt(c + c') = wt(c) + wt(c') - 2|sop(c) \cap sop(c')|.$$

Como C es lineal, $c + c' \in C$ y C es doblemente par, entonces $4 \mid wt(c + c')$, $4 \mid wt(c)$ y $4 \mid wt(c')$. Luego,

$$2 \mid |sop(c) \cap sop(c')|.$$

Esto nos permite concluir que $(c|c') = 0$ y, por lo tanto, que C es auto-ortogonal. □

Lema 1.2.10 *Sea C un código binario y auto-dual de longitud n. Entonces:*

1. *C es par.*
2. *Si $4 \mid wt(c)$, para todo c en una base de C, entonces C es doblemente par.*

DEMOSTRACIÓN.

1. Por hipótesis, $C \subseteq C^{\perp}$. Esto significa que $(C|c) = 0$, para todo $c \in C$. Esto es, $\sum_{i=1}^{n} c_i^2 = 0$. Además, C es un código binario, por lo que $\sum_{i=1}^{n} c_i = 0$. Luego, $wt(C)$ es par, es decir, $2|wt(C)$ y por tanto C es par.

2. Es suficiente demostrar que si $4 \mid wt(c)$ y $4 \mid wt(c')$, entonces $4 \mid wt(c + c')$. Esto se sigue del teorema 1.2.9, pues en su demostración

   $$wt(c + c') = wt(c) + wt(c') - 2|sop(c) \cap sop(c')|$$

   y, teniendo en cuenta que C es auto-dual, tenemos que $(c, c') = 0$, para todo $c, c' \in C$. Pero

   $$(c|c') = |sop(c) \cap sop(c')| \cdot 1 = 0.$$

   Luego, $|sop(c) \cap sop(c')|$ es par. Es decir, $2 \mid |sop(c) \cap sop(c')|$. Con lo que

   $$4 \mid (2|sop(c) \cap sop(c')|)$$

   y $4 \mid wt(c + c')$.
   Ahora, sea $\beta = (v_1, ..., v_k)$ una base de C. Entonces, $4 \mid wt(v_j)$. Si $c \in C$, tendremos que

   $$c = \sum_{j=1}^{k} \alpha_i v_i$$

y

$$wt(c) = \alpha_1 v_1 + ... + \alpha_k v_k,$$

por lo que $4 \mid wt(c)$, para todo $c \in C$. Entonces, C es doblemente par.

□

Definición 1.2.11 *Sean C un $[n,k]$-código sobre $\mathbb{K}$ y $|\mathbb{K}| = q$. Denotamos con A_j el número de codewords con peso j, para $0 \leq j \leq n$. Definimos el polinomio enumerador de pesos de C, notado $A(x)$, por*

$$A(x) = \sum_{j=0}^{n} A_j x^j \in \mathbb{Z}[x]$$

y el vector $(A_0 = 1, A_1, ..., A_n)$ se denomina la distribución de pesos de C.

Observaciones 1.2.12 *El valor distinto de cero más pequeño de i tal que $A_i > 0$, es la distancia mínima del código. El enumerador de pesos de un código también puede ser representado por el polinomio homogéneo en dos indeterminadas*

$$A(x,y) = \sum_i A_i x^{n-i} y^i$$

y el resultado de una substitución lineal podrá ser escrita como $A((x,y)\sigma)$.

Definición 1.2.13 *Sea C un código de longitud n sobre $\mathbb{F}_2$. Si el codeword $(1,...,1) \in C$, diremos que C es auto-complementario.*

Lema 1.2.14 *Sea C un código binario auto-complementario con longitud n. Entonces $A_i = A_{n-i}$, para $i = 1, ..., n-1$.*

DEMOSTRACIÓN. Sea $B_i := \{x \in C \mid w(x) = i\} \subseteq C$. Entonces, por definición, $A_i = |B_i|$, con $i = 1, ..., n-1$. Probemos que $|B_i| = |B_{n-i}|$. Para esto, definamos la función

$$\varphi : B_i \to B_{n-i},$$

con $\varphi(x) = c_0 - x = c_0 + x \in C$ y $c_0 = (1, ..., 1) \in C$. Es fácil ver que φ es una biyección. Por lo tanto, $|B_i| = |B_{n-i}|$. Entonces,

$$A_i = |B_i| = |B_{n-i}| = A_{n-i}.$$

Luego, $A_i = A_{n-i}$, para $i = 1, ..., n-1$. □

Teorema 1.2.15 ***[Dualidad de Mac-Williams]**.Sean $|\mathbb{K}| = q$, C un $[n,k]$-código sobre $\mathbb{K}$ con polinomio enumerador de pesos $A(z)$. Notemos con $A^\perp(z)$ al polinomio enumerador de pesos de $C^\perp$. Entonces*

$$A^\perp(z) = q^{-k}(1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right)$$

o

$$A^\perp(x,y) = x^n A^\perp\left(\frac{y}{x}\right) = q^{-k} A(x + (q-1)y, x - y).$$

DEMOSTRACIÓN. Ver [9], pág. 90. □

Capítulo 2

Cotas superiores para códigos auto-duales

2.1. Divisibilidad de polinomios enumeradores de pesos

Definición 2.1.1 *Sea p un polinomio homogéneo en n indeterminadas sobre el cuerpo de los números complejos. Definimos el operador diferencial, notado $p(D)$, mediante la substitución de cada aparición de x_j en p por $\frac{\partial}{\partial x_j}$.*

Ejemplo 2.1.2 *1. Sea $p(x,y) = 2x^2y^4 + x - 3xy$. Entonces, el operador diferencial de p está dado por*

$$p(D) = 2\frac{\partial^6}{\partial x^2 \partial y^4} + \frac{\partial}{\partial x} - 3\frac{\partial^2}{\partial x \partial y}.$$

2. Sea $p(u,v) = (v + 3u^3v^5)u^2$. Entonces, $p(D)$ está dado por

$$p(D) = \frac{\partial^3}{\partial v \partial u^2} + 3\frac{\partial^{10}}{\partial u^5 \partial v^5}.$$

Para la obtención de cotas superiores para la longitud n y la distancia mínima d de un código C con polinomio enumerador de pesos homogéneo $A(x,y)$, resulta de especial interés encontrar parejas de polinomios $a(x,y)$ y $p(x,y)$ tales que:

$$a(x,y) \mid p(x,y)(D)A(x,y) \tag{2.1}$$

Observaciones 2.1.3 *Un código lineal con distancia mínima d tiene como polinomio enumerador de pesos al polinomio*

$$A(x,y) = x^n + A_d x^{n-d} y^d + ... + A_n y^n.$$

Entonces,

$$\begin{aligned} y(D)A(x,y) &:= \frac{\partial}{\partial y}(x^n + A_d x^{n-d}y^d + ... + A_n y^n) \\ &= dA_d x^{n-d}y^{d-1} + (d+1)A_{d+1}x^{n-(d+1)}y^d + ... + nA_n y^{n-1} \\ &= dA_d x^{n-d}y^{d-1} + (d+1)A_{d+1}x^{n-d-1}y^{d-1}y + ... + nA_n y^{d-1}y^{n-d}. \end{aligned}$$

Luego, tendríamos nuestra primera relación de la forma (2.1) pues se observa que

$$y^{d-1} \mid y(D)A(x,y) \tag{2.2}$$

Lema 2.1.4 *Si se tienen transformaciones lineales de la forma*

$$(u,v) = (x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

entonces podemos obtener sus transformaciones del operador diferencial de la forma

$$(\tfrac{\partial}{\partial x}, \tfrac{\partial}{\partial y}) = (\tfrac{\partial}{\partial u}, \tfrac{\partial}{\partial v})\begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

DEMOSTRACIÓN. Como $(u,v) = (x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces tenemos que $u = xa + yc$ y $v = xb + yd$. Por lo tanto, $\frac{\partial u}{\partial x} = a$, $\frac{\partial v}{\partial x} = b$, $\frac{\partial u}{\partial y} = c$ y $\frac{\partial v}{\partial y} = d$. Luego,

$$\tfrac{\partial}{\partial x}(u,v) = (a,b).$$

y

$$\tfrac{\partial}{\partial y}(u,v) = (c,d).$$

En consecuencia, tenemos que

$$\frac{\partial}{\partial x} = a\frac{\partial}{\partial u} + b\frac{\partial}{\partial v}$$

y

$$\frac{\partial}{\partial y} = c\frac{\partial}{\partial u} + d\frac{\partial}{\partial v},$$

y de estas dos últimas igualdades se obtiene lo deseado. Esto es,

$$(\tfrac{\partial}{\partial x}, \tfrac{\partial}{\partial y}) = (\tfrac{\partial}{\partial u}, \tfrac{\partial}{\partial v})\begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

□

Lema 2.1.5 *Sean $\mathbb{K}$ un cuerpo, $(u,v) = (x,y)\sigma$, con $\sigma \in Mat_2(\mathbb{K})$ invertible y $p(x,y)$, $A(x,y)$ polinomios homogéneos con coeficientes en $\mathbb{K}$. Entonces,*

$$p((u,v)\sigma^T)(D)A(u,v) = p(x,y)(D)A((x,y)\sigma),$$

donde σ^T es la transpuesta de σ.

DEMOSTRACIÓN. Por hipótesis $(u,v) = (x,y)\sigma$.

Entonces,

$$A((x,y)\sigma) = A(u,v). \tag{2.3}$$

Ahora, por el lema 2.1.4, tenemos que

$$(\tfrac{\partial}{\partial x}, \tfrac{\partial}{\partial y}) = (\tfrac{\partial}{\partial u}, \tfrac{\partial}{\partial v})\sigma^T.$$

Por lo tanto,

$$p(\tfrac{\partial}{\partial x}, \tfrac{\partial}{\partial y}) = p\left((\tfrac{\partial}{\partial u}, \tfrac{\partial}{\partial v})\sigma^T\right),$$

o, equivalentemente,

$$p(x,y)(D) = p((u,v)\sigma^T)(D). \tag{2.4}$$

De (2.3) y (2.4) se obtiene la igualdad deseada. □

Lema 2.1.6 *Sean C un código lineal binario auto-complementario de longitud n y distancia mínima d y $A(x,y) \in \mathbb{Z}[x,y]$ su polinomio enumerador de pesos. Entonces, $A(x,y) = A(y,x)$.*

DEMOSTRACIÓN. Del lema 1.2.14 se tiene que

$$A_i = A_{n-i}. \tag{2.5}$$

Como el polinomio enumerador de pesos de C es de la forma

$$A(x,y) = A_0x^n + A_1x^{n-1}y + A_2x^{n-2}y^2 + ... + A_{n-1}xy^{n-1} + A_ny^n,$$

entonces por (2.5) tendríamos que

$$A(x,y) = A_nx^n + A_{n-1}x^{n-1}y + A_{n-2}x^{n-2}y^2 + ... + A_1xy^{n-1} + A_0y^n.$$

Reescribiendo,

$$A(x,y) = A_0y^n + A_1y^{n-1}x + ... + A_{n-2}y^2x^{n-2} + A_{n-1}yx^{n-1} + A_nx^n = A(y,x).$$

En conclusión, $A(x,y) = A(y,x)$. □

Lema 2.1.7 *Sean C un código lineal binario auto-complementario de longitud n y distancia mínima d y $A(x,y) \in \mathbb{Z}[x,y]$ su polinomio enumerador de pesos. Entonces, $(xy)^{d-1} \mid xy(D)A(x,y)$.*

DEMOSTRACIÓN. Consideremos la transformación lineal

$$(u,v) = (x,y)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Entonces, $u = y$ y $v = x$. Por tanto, $x^{d-1} = v^{d-1}$, $v(D) = x(D)$ y $A(u,v) = A(y,x)$. Utilizando (2.2),

$$x^{d-1} = v^{d-1} \mid v(D)A(u,v) = x(D)A(y,x)$$

y por el lema 2.1.6,

$$x^{d-1} = v^{d-1} \mid v(D)A(u,v) = x(D)A(x,y).$$

Ahora tenemos que

$$x^{d-1} \mid x(D)A(x,y). \tag{2.6}$$

De (2.2) y (2.6), se tiene la afirmación. □

Lema 2.1.8 *Sea C un $[n,k]$-código sobre $\mathbb{F}_q$ con polinomio enumerador de pesos homogéneo dado por $A(x,y)$. Entonces, $A^{\perp}(x,y) = q^{-k}A(x+(q-1)y, x-y)$.*

DEMOSTRACIÓN. Del teorema de la Dualidad de Mac-Williams tenemos que

$$\begin{aligned}
A^{\perp}(x,y) &= x^n A^{\perp}\left(\frac{y}{x}\right) \\
&= x^n q^{-k}(1+(q-1)(y/x))^n A\left(\frac{1-y/x}{1+(q-1)(y/x)}\right) \\
&= x^n q^{-k}\frac{(x+(q-1)y)^n}{x^n} A\left(\frac{x-y}{x+(q-1)y}\right) \\
&= q^{-k}(x+(q-1)y)^n \sum_{i=0}^{n} A_i \frac{(x-y)^i}{(x+(q-1)y)^i} \\
&= q^{-k}\sum_{i=0}^{n} A_i (x+(q-1)y)^{n-i}(x-y)^i \\
&= q^{-k}A(x+(q-1)y, x-y).
\end{aligned}$$

□

Observaciones 2.1.9 *Sea*

$$\sigma = \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}$$

y definamos $(u,v) = (x,y)\sigma$*, usualmente denominada transformación de Mc-Williams. Entonces,* $u = x + (q-1)y$*,* $v = x - y$ *y* $u - v = qy$*. En consecuencia,*

$$\begin{aligned} A^{\perp}(u,v) &= A^{\perp}(x+(q-1)y, x-y) \\ &= q^{-k}A(x+(q-1)y+(q-1)(x-y), qy) \\ &= q^{-k}A(qx,qy) \\ &= q^{-k}\sum_{i=0}^{n} A_i (qx)^{n-i}(qy)^i \\ &= q^{-k}\sum_{i=0}^{n} A_i q^n x^{n-i} y^i \\ &= q^{n-k}A(x,y). \end{aligned}$$

En conclusión, $A^{\perp}(u,v) = q^{n-k}A(x,y)$*.*

Lema 2.1.10 *Sean* $A(x,y) \in \mathbb{Z}[x,y]$ *el polinomio enumerador de pesos homogéneo de un código* C *con longitud* n *y distancia mínima* d *y* $d^{\perp}$ *la distancia mínima de* $C^{\perp}$*. Entonces,*

1. $(x-y)^{d^{\perp}-1} \mid (x(q-1)-y)(D)A(x,y)$.
2. *Si el código* C *es, además, binario y par, entonces*

$$(x^2-y^2)^{d^{\perp}-1} \mid (x^2-y^2)(D)A(x,y).$$

DEMOSTRACIÓN.

1. Sea σ la matriz considerada en la observación anterior. Nuevamente, tenemos que $u = x + (q-1)y$, $v = x - y$ y $u - v = qy$. Luego, para $C^{\perp}$ se verifica que

$$v^{d^{\perp}-1} = (x-y)^{d^{\perp}-1}.$$

Pero por (2.2):

$$v^{d^{\perp}-1} \mid v(D)A^{\perp}(u,v).$$

Entonces,

$$q(x-y)^{d^{\perp}-1} = qv^{d^{\perp}-1} \mid qv(D)A^{\perp}(u,v)$$

y por la observación anterior, $A^{\perp}(u,v) = A(x,y)q^{n-k}$. Por tanto,

$$q(x-y)^{d^{\perp}-1} = qv^{d^{\perp}-1} \mid qv(D)A^{\perp}(u,v) = qv(D)A(x,y)q^{n-k}. \tag{2.7}$$

Ahora, probemos que

$$((q-1)x-y)(D) = qv(D).$$

En efecto, sea

$$p(x,y) = (q-1)x - y. \tag{2.8}$$

De la igualdad (2.4):

$$\begin{aligned}((q-1)x-y)(D) &= p(x,y)(D)\\ &= p((u,v)\sigma^T)(D)\\ &= p(u+v,(q-1)u-v)(D)\\ &= ((q-1)(u+v)-((q-1)u-v))(D) \qquad \text{por (2.8)}\\ &= qv(D).\end{aligned}$$

Luego,

$$((q-1)x-y)(D) = qv(D). \tag{2.9}$$

Por (2.7) y (2.9):

$$(x-y)^{d^\perp-1} \mid ((q-1)x-y)(D)A(x,y)q^{n-k-1}.$$

Esto nos permite concluir que

$$(x-y)^{d^\perp-1} \mid ((q-1)x-y)(D)A(x,y).$$

2. Nuevamente consideramos la transformación de Mac-Williams. Entonces, por el lema 2.1.4, sus transformaciones de operadores diferenciales son de la forma

$$(\tfrac{\partial}{\partial x},\tfrac{\partial}{\partial y}) = (\tfrac{\partial}{\partial u},\tfrac{\partial}{\partial v})\begin{pmatrix}1 & q-1\\ 1 & -1\end{pmatrix}.$$

Por lo tanto,

$$(\tfrac{\partial}{\partial u},\tfrac{\partial}{\partial v}) = (\tfrac{\partial}{\partial x},\tfrac{\partial}{\partial y})q^{-1}\begin{pmatrix}1 & q-1\\ 1 & -1\end{pmatrix} = \left(\tfrac{\partial}{\partial x}q^{-1}+\tfrac{\partial}{\partial y}q^{-1},\tfrac{\partial}{\partial x}q^{-1}(q-1)-\tfrac{\partial}{\partial y}q^{-1}\right).$$

Con lo cual, se tiene que

$$u(D) = q^{-1}(x+y)(D). \tag{2.10}$$

Por otra parte, dado que C es binario ($q=2$) y, además, par, entonces $u = x+y$ y $v = x-y$. Luego,

$$u^{d^\perp-1} = (x+y)^{d^\perp-1}. \tag{2.11}$$

Por el lema 2.1.8 y (2.10):

$$u(D)A^\perp(u,v) = 2^{-1}(x+y)(D)A(x,y)2^{n-k}. \tag{2.12}$$

De (2.6) sabemos que

$$u^{d^\perp-1} \mid u(D)A^\perp(u,v). \tag{2.13}$$

Usando entonces (2.11), (2.12) y (2.13), tenemos que

$$(x+y)^{d^\perp-1} = u^{d^\perp-1} \mid u(D)A^\perp(u,v) = 2^{-1}(x+y)(D)A(x,y)2^{n-k}.$$

Por lo que

$$(x+y)^{d^\perp-1} \mid (x+y)(D)A(x,y)2^{n-k-1}.$$

Además, por la parte 1 de este teorema y teniendo en cuenta que $q = 2$, se tiene que

$$(x-y)^{d^\perp-1} \mid (x-y)(D)A(x,y).$$

Por consiguiente,

$$(x+y)^{d^\perp-1}(x-y)^{d^\perp-1} \mid (x+y)(D)A(x,y)(x-y)(D)A(x,y)2^{n-k-1},$$

es decir,

$$(x^2-y^2)^{d^\perp-1} \mid (x^2-y^2)(D)A(x,y)2^{n-k-1}.$$

En conclusión,

$$(x^2-y^2)^{d^\perp-1} \mid (x^2-y^2)(D)A(x,y).$$

□

Lema 2.1.11 *Sean C un código c-divisible de longitud n y distancia mínima d, $A(x,y) \in \mathbb{Z}[x,y]$ su polinomio enumerador de pesos homogéneo de C y $d^\perp$ la distancia mínima de $C^\perp$. Entonces,*

1. $(x^c-y^c)^{d^\perp-c} \mid ((q-1)^c x^c - y^c)(D)A(x,y)$.
2. *Si el código C es, además, binario y par, entonces*

$$(x^c-y^c)^{d^\perp-c+1} \mid (x^c-y^c)(D)A(x,y).$$

DEMOSTRACIÓN.

1. Para el polinomio enumerador de pesos de un código c-divisible C, se verifica que

$$A(x,y) = A(x,\zeta y),$$

para todo $\zeta \in \mathbb{C}$, con $\zeta^c = 1$. En efecto,

$$A(x,\zeta y) = \sum_i A_i x^{n-i}\zeta^i y^i = \sum_i A_i x^{n-i} y^i = A(x,y).$$

Esto último porque, si $c \nmid i$, entonces $A_i = 0$ y si $c \mid i$, entonces $\zeta^i = 1$, pues el código es c-divisible. Como transformación lineal se tiene:

$$(u,v) = (x,y)\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix},$$

para todo $\zeta \in \mathbb{C}$, con $\zeta^c = 1$. Esto es, $u = x$ y $v = \zeta y$. De la parte 1 del lema 2.1.10, tenemos que:

$$(u-v)^{d^\perp-1} \mid ((q-1)u - v)(D)A(u,v).$$

Reemplazando $u = x$ y $v = \zeta y$, se sigue que

$$(x - \zeta y)^{d^\perp - 1} \mid ((q-1)x - \zeta y)(D)A(x, \zeta y) = ((q-1)x - \zeta y)(D)A(x, y).$$

Sean $\zeta_1, ..., \zeta_c$ las c-ésimas raíces complejas de la unidad. Se considera

$$(x - \zeta_i y)^{d^\perp - 1} \mid ((q-1)x - \zeta_i y)(D)A(x, y),$$

para $i = 1, ..., c$. En primer lugar, consideremos ζ_1. Entonces,

$$(x - \zeta_1 y)^{d^\perp - 1} \mid ((q-1)x - \zeta_1 y)(D)A(x, y).$$

Esto significa que existe un polinomio homogéneo $f(x, y)$ tal que

$$(x - \zeta_1 y)^{d^\perp - 1} f(x, y) = ((q-1)x - \zeta_1 y)(D)A(x, y).$$

Entonces,

$$((q-1)x - \zeta_2 y)(D)(x - \zeta_1 y)^{d^\perp - 1} f(x, y) = ((q-1)x - \zeta_2 y)((q-1)x - \zeta_1 y)(D)A(x, y).$$

Ahora, consideremos el lado izquierdo de esta ecuación. Sea

$$\theta(x, y) := ((q-1)x - \zeta_2 y)(D)(x - \zeta_1 y)^{d^\perp - 1} f(x, y).$$

Entonces,

$$\begin{aligned}
\theta(x,y) &= ((q-1)\tfrac{\partial}{\partial x} - \zeta_2 \tfrac{\partial}{\partial y})(x - \zeta_1 y)^{d^\perp - 1} f(x,y) \\
&= (q-1)\tfrac{\partial}{\partial x}(x - \zeta_1 y)^{d^\perp - 1} f(x,y) - \zeta_2 \tfrac{\partial}{\partial y}(x - \zeta_1 y)^{d^\perp - 1} f(x,y) \\
&= (q-1)[(d^\perp - 1)(x - \zeta_1 y)^{d^\perp - 2} f(x,y) + (x - \zeta_1 y)^{d^\perp - 1} \tfrac{\partial}{\partial x} f(x,y)] \\
&\quad -\zeta_2[(d^\perp - 1)(x - \zeta_1 y)^{d^\perp - 2}(-\zeta_1) f(x,y) + (x - \zeta_1 y)^{d^\perp - 1} \tfrac{\partial}{\partial y} f(x,y)] \\
&= (q-1)(d^\perp - 1)(x - \zeta_1 y)^{d^\perp - 2} f(x,y) + (q-1)(x - \zeta_1 y)^{d^\perp - 1} \tfrac{\partial}{\partial x} f(x,y) \\
&\quad +\zeta_1\zeta_2(d^\perp - 1)(x - \zeta_1 y)^{d^\perp - 2} f(x,y) - \zeta_2 (x - \zeta_1 y)^{d^\perp - 1} \tfrac{\partial}{\partial y} f(x,y) \\
&= (d^\perp - 1)(x - \zeta_1 y)^{d^\perp - 2} f(x,y)[(q-1) + \zeta_1\zeta_2] \\
&\quad +(x - \zeta_1 y)^{d^\perp - 1}[(q-1)\tfrac{\partial}{\partial x} - \zeta_2 \tfrac{\partial}{\partial y}] f(x,y) \\
&= (d^\perp - 1)((q-1) + \zeta_1\zeta_2)(x - \zeta_1 y)^{d^\perp - 2} f(x,y) \\
&\quad +((q-1)x - \zeta_2 y)(D)(x - \zeta_1 y)^{d^\perp - 1} f(x,y).
\end{aligned}$$

Por tanto, se observa que

$$(x - \zeta_1 y)^{d^\perp - 2} \mid ((q-1)x - \zeta_2 y)(D)(x - \zeta_1 y)^{d^\perp - 1} f(x, y)$$

o

$$(x - \zeta_1 y)^{d^\perp - 2} \mid ((q-1)x - \zeta_2 y)((q-1)x - \zeta_1 y)(D)A(x, y),$$

pues $(x - \zeta_1 y)^{d^\perp - 1} f(x, y) = ((q-1)x - \zeta_1 y)(D)A(x, y)$. Luego,

$$(x-\zeta_1 y)^{d^\perp-2} \mid (\prod_{i=1}^{2}((q-1)x-\zeta_i y))(D)A(x,y).$$

Realizando este proceso para ζ_3 hasta ζ_c, obtenemos que

$$(x-\zeta_1 y)^{d^\perp-c} \mid (\prod_{i=1}^{c}((q-1)x-\zeta_i y))(D)A(x,y).$$

Dado que esto es aplicable para todos los términos $(x-\zeta_i y)$, con $i = 1,...,c$, y los $(x-\zeta_i y)$ son distintos dos a dos, se deduce que

$$\prod_{i=1}^{c}(x-\zeta_i y)^{d^\perp-c} \mid (\prod_{i=1}^{c}((q-1)x-\zeta_i y))(D)A(x,y)$$

o

$$(\prod_{i=1}^{c}(x-\zeta_i y))^{d^\perp-c} \mid (\prod_{i=1}^{c}((q-1)x-\zeta_i y))(D)A(x,y).$$

Teniendo en cuenta que $\prod_{i=1}^{c}(x-\zeta_i y) = x^c - y^c$ y

$$\prod_{i=1}^{c}((q-1)x-\zeta_i y) = ((q-1)^c x^c - y^c),$$

se obtiene lo deseado:

$$(x^c-y^c)^{d^\perp-c} \mid ((q-1)^c x^c - y^c)(D)A(x,y).$$

2. Para un código binario y par se tiene, por la parte 2 del lema 2.1.10, que:

$$(u^2-v^2)^{d^\perp-1} \mid (u^2-v^2)(D)A(u,v).$$

Considerando la misma transformación lineal de la forma

$$(u,v) = (x,y)\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix},$$

para todo $\zeta \in \mathbb{C}$, con $\zeta^c = 1$ y reemplazando $u = x$ y $v = \zeta y$, se sigue que

$$\begin{aligned}(x^2-\zeta^2 y^2)^{d^\perp-1} &\mid (x^2-\zeta^2 y^2)(D)A(x,\zeta y) \\ &= (x^2-\zeta^2 y^2)(D)A(x,y).\end{aligned}$$

Sean $\zeta_1,...,\zeta_c$ las c-ésimas raíces de la unidad. Entonces,

$$(x^2-\zeta_i^2 y^2)^{d^\perp-1} \mid (x^2-\zeta_i^2 y^2)(D)A(x,y),$$

para $i = 1,...,c$, o

$$(x^2-\zeta_j y^2)^{d^\perp-1} \mid (x^2-\zeta_j y^2)(D)A(x,y),$$

para $j = 1,..., \frac{c}{2}$, con $\zeta_i^2 = \zeta_j$ y $(\zeta_j)^{c/2} = 1$.
Esto no dá lugar a ninguna dificultad pues el código es par, así que $2 \mid wt(c)$, para

todo $c \in C$ y, por tanto, $\frac{c}{2} \in \mathbb{Z}$. El término será examinado como antes. Centrémonos, en primer lugar, en ζ_1. Entonces,

$$(x^2 - \zeta_1 y^2)^{d^\perp - 1} \mid (x^2 - \zeta_1 y^2)(D)A(x,y).$$

Lo que equivale a

$$(x^2 - \zeta_1 y^2)^{d^\perp - 1} f(x,y) = (x^2 - \zeta_1 y^2)(D)A(x,y),$$

donde $f(x,y)$ es un polinomio homogéneo. Multiplicando a esta última igualdad por el factor $(x^2 - \zeta_2 y^2)(D)$, tenemos que

$$(x^2 - \zeta_2 y^2)(D)(x^2 - \zeta_1 y^2)^{d^\perp - 1} f(x,y) = (x^2 - \zeta_2 y^2)(x^2 - \zeta_1 y^2)(D)A(x,y).$$

De nuevo, consideramos el lado izquierdo de esta última ecuación y, razonando como lo hicimos anteriormente, obtenemos:

$$\begin{aligned} \vartheta(x,y) \;=\; & 4(d^\perp - 1)(d^\perp - 2)(x^2 - \zeta_1^2 \zeta_2 y^2) f(x,y)(x^2 - \zeta_1 y^2)^{d^\perp - 3} \\ & + 2(d^\perp - 1)[2x \tfrac{\partial}{\partial x} f(x,y) + f(x,y) + 2y\zeta_1\zeta_2 \tfrac{\partial}{\partial y} f(x,y) + \zeta_1\zeta_2 f(x,y)] \\ & (x^2 - \zeta_1 y^2)^{d^\perp - 2} + (x^2 - \zeta_2 y^2)(D) f(x,y)(x^2 - \zeta_1 y^2)^{d^\perp - 1}, \end{aligned}$$

donde $\vartheta(x,y) = (x^2 - \zeta_2 y^2)(D)(x^2 - \zeta_1 y^2)^{d^\perp - 1} f(x,y)$. Así vemos que,

$$(x^2 - \zeta_1 y^2)^{d^\perp - 3} \mid (x^2 - \zeta_2 y^2)(D)(x^2 - \zeta_1 y^2)^{d^\perp - 1} f(x,y)$$

o

$$(x^2 - \zeta_1 y^2)^{d^\perp - 3} \mid (x^2 - \zeta_2 y^2)(x^2 - \zeta_1 y^2)^{d^\perp - 1}(D)A(x,y),$$

pues $(x^2 - \zeta_2 y^2)(D)(x^2 - \zeta_1 y^2)^{d^\perp - 1} f(x,y) = (x^2 - \zeta_2 y^2)(x^2 - \zeta_1 y^2)(D)A(x,y)$.
Continuando con esto para ζ_3 hasta $\zeta_{\frac{c}{2}}$, se sigue que

$$(x^2 - \zeta_1 y^2)^{d^\perp - c + 1} \mid (\textstyle\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2))(D)A(x,y).$$

Esto se aplica a todos los términos $(x^2 - \zeta_j y^2)$, para $j = 1, ..., \frac{c}{2}$ y además, los términos $(x^2 - \zeta_j y^2)$ son distintos dos a dos. Entonces,

$$\textstyle\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2)^{d^\perp - c + 1} \mid (\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2))(D)A(x,y)$$

o

$$[\textstyle\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2)]^{d^\perp - c + 1} \mid (\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2))(D)A(x,y).$$

Teniendo en cuenta que

$$\prod_{j=1}^{c/2}(x^2 - \zeta_j y^2) = x^c - y^c$$

y

$$(\prod_{j=1}^{c/2}(x^2-\zeta_j y^2)) = (x^c - y^c),$$

se obtiene lo deseado:

$$(x^c-y^c)^{d^\perp-(c-1)} \mid (x^c-y^c)(D)A(x,y).$$

□

Definición 2.1.12 *Sea C un código sobre un cuerpo $\mathbb{K}$ y $c \in \mathbb{N}$.*

Diremos que C es de tipo 1, si C es c-divisible.

Si, además, C es binario, par y auto-complementario(con lo cual, su código dual también), entonces diremos que es de tipo 2.

Lema 2.1.13 *Para un código c-divisible C de longitud n, distancia mínima d, polinomio enumerador de pesos $A(x,y)$ y distancia mínima de $C^\perp$, dada por $d^\perp$, se tiene que*

(Tipo 1) $y^{d-c-1}(x^c-y^c)^{d^\perp-c-1} \mid y(y^c-(q-1)^c x^c)(D)A(x,y)$,

(Tipo 2) $(xy)^{d-c-1}(x^c-y^c)^{d^\perp-c-1} \mid xy(y^c-x^c)(D)A(x,y)$.

DEMOSTRACIÓN.

1. Por (2.2) se sabe que $y^{d-1} \mid y(D)A(x,y)$. Pero, por la parte 1 del lema anterior:

   $$(x^c-y^c)^{d^\perp-c} \mid ((q-1)^c x^c - y^c)(D)A(x,y).$$

   De ello se deduce que

   $$y^{d-c-1} \mid y((q-1)^c x^c - y^c)(D)A(x,y)$$

   y

   $$(x^c-y^c)^{d^\perp-c-1} \mid y((q-1)^c x^c - y^c)(D)A(x,y).$$

   De donde se obtiene que:

   $$y^{d-c-1}(x^c-y^c)^{d^\perp-c-1} \mid y(y^c-(q-1)^c x^c)(D)A(x,y).$$

2. Ahora, para un código binario par C de tipo 2 y con $(1,...,1) \in C$, se tiene que $(xy)^{d-1} \mid xy(D)A(x,y)$, teniendo en cuenta el lema 2.1.7. Pero por la parte 2 del lema anterior:

   $$(x^c-y^c)^{d^\perp-c+1} \mid (x^c-y^c)(D)A(x,y).$$

   De ello se deduce que

   $$(xy)^{d-c-1} \mid xy(x^c-y^c)(D)A(x,y)$$

   y

   $$(x^c-y^c)^{d^\perp-c+1-2} \mid xy(x^c-y^c)(D)A(x,y).$$

   De donde se obtiene que:

   $$(xy)^{d-c-1}(x^c-y^c)^{d^\perp-c-1} \mid xy(y^c-x^c)(D)A(x,y).$$

□

Notación 2.1.14 *En adelante, para $a, n \in \mathbb{Z}$, utilizaremos la notación $(a)_n$ para referirnos al producto*

$$(a)_n = a(a+1)\cdots(a+n-1).$$

Teorema 2.1.15 *Sean C un código c-divisible de longitud n con distancia mínima d, polinomio enumerador de pesos $A(x,y)$ y distancia mínima de $C^\perp$, dada por $d^\perp$. Entonces,*

(Tipo 1) $d + cd^\perp \leq n + c(c+1)$,

(Tipo 2) $2d + cd^\perp \leq n + c(c+2)$.

La igualdad se verifica si y sólo si

(Tipo 1) $y(y^c - (q-1)^c x^c)(D)A(x,y) = (d-c)_{c+1} A_d y^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}$,

(Tipo 2) $xy(y^c - x^c)(D)A(x,y) = (n-d)(d-c)_{c+1} A_d (xy)^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}$.

DEMOSTRACIÓN.

1. Sean $p(x,y) := y(y^c - (q-1)^c x^c)$ y $a(x,y) := y^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}$. Entonces, el grado del polinomio homogéneo
$$p(x,y)(D)A(x,y)$$
es $n-c-1$, ya que el grado de $A(x,y)$ es n. Además, el grado del polinomio $a(x,y)$ es
$$d - c - 1 + cd^\perp - c^2 - c.$$
Por la parte 1 del lema anterior, tenemos que
$$a(x,y) \mid p(x,y)(D)A(x,y).$$
Entonces, el grado del polinomio $a(x,y)$ es menor o igual que el grado del polinomio $p(x,y)(D)A(x,y)$. Así que
$$d - c - 1 + cd^\perp - c^2 - c \leq n - c - 1.$$
Esto es,
$$d + cd^\perp - c^2 - c \leq n$$
o
$$d + cd^\perp \leq n + c^2 + c.$$
Así obtenemos el resultado deseado:
$$d + cd^\perp \leq n + c(c+1).$$
Ahora, la igualdad se dá si y sólo si
$$p(x,y)(D)A(x,y) = Ka(x,y),$$
siendo K una constante (comparando en lo más mínimo los coeficientes de y). El grado más pequeño de y en $a(x,y)$ es $d-c-1$. En $p(x,y)(D)A(x,y)$, el coeficiente de y^{d-c-1} es $(d-c)_{c+1}A_d$. Esto demuestra la afirmación.

2. Ahora, sean $p(x,y) := xy(y^c - x^c)$ y $a(x,y) := (xy)^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}$. Para el tipo 2, el grado del polinomio $p(x,y)(D)A(x,y)$ es $n-c-2$ y como

$$\begin{aligned} a(x,y) &= (xy)^{d-c-1}(x^c - y^c)^{d^\perp - c - 1} \\ &= x^{d-c-1}y^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}, \end{aligned}$$

entonces el grado de $a(x,y)$ es $2(d-c-1) + cd^\perp - c^2 - c$. Por la parte 2 del lema anterior tenemos que

$$a(x,y) \mid p(x,y)(D)A(x,y).$$

Entonces, el grado del polinomio $a(x,y)$ es menor o igual que el grado del polinomio $p(x,y)(D)A(x,y)$. Así que

$$2(d-c-1) + cd^\perp - c^2 - c \leq n - c - 2.$$

Luego,

$$2d - 2c + cd^\perp - c^2 \leq n.$$

Esto es,

$$2d + cd^\perp \leq n + c^2 + 2c.$$

Obteniendo así lo que queremos:

$$2d + cd^\perp \leq n + c(c+2).$$

Ahora, la igualdad es verdadera si y sólo si

$$p(x,y)(D)A(x,y) = Ka(x,y),$$

siendo K una constante (comparando en lo más mínimo los coeficientes de y). El grado más pequeño de y en $a(x,y)$ es $d-c-1$. En $p(x,y)(D)A(x,y)$, el coeficiente de y^{d-c-1} es $(n-d)(d-c)_{c+1}A_d$. Esto demuestra la afirmación.

□

2.2. Polinomios enumeradores de pesos con coeficientes positivos

Para que un polinomio enumerador de pesos, como en el teorema 2.1.15, pueda ser realizable mediante un código, forzosamente los coeficientes deben ser no negativos. Sin embargo, esto no es condición suficiente para que un código con tales parámetros exista.

Teorema 2.2.1 *Sea C un código c-divisible de longitud n con distancia mínima d, distancia mínima de $C^\perp$ dada por $d^\perp$ y con las cotas obtenidas en el teorema 2.1.15. Entonces, $A_{d+c}/A_d \geq 0$, si*

(Tipo 1) $\quad (d^\perp - c - 1)(d-c)_c \leq (q-1)^c(n-d-c+1)_c$,

(Tipo 2) $(d^{\perp}-c-1)(d-c)_c \leq (n-d-c)_c$.

DEMOSTRACIÓN.

1. Consideremos, en primer lugar, los códigos del tipo 1. Por la segunda parte del teorema 2.1.15, tenemos que: $d+cd^{\perp} = n+c(c+1)$ si y sólo si

$$y(y^c-(q-1)^c x^c)(D)A(x,y) = (d-c)_{c+1}A_d y^{d-c-1}(x^c-y^c)^{d^{\perp}-c-1}. \tag{2.14}$$

Note que

$$\begin{aligned} y(y^c-(q-1)^c x^c)(D)A(x,y) &= (y^{c+1}-(q-1)^c yx^c)(D)A(x,y) \\ &= (\tfrac{\partial}{\partial y})^{c+1}A(x,y)-(q-1)^c\tfrac{\partial}{\partial y}(\tfrac{\partial}{\partial x})^c A(x,y). \end{aligned}$$

Sea ahora $k=\frac{n-d}{c}$. Entonces, el polinomio enumerador de pesos $A(x,y)\in\mathbb{Z}[x,y]$ de un código c-divisible de longitud n tiene la forma:

$$A(x,y) = x^n + \textstyle\sum_{i=0}^{k} A_{d+ic}x^{n-d-ic}y^{d+ic}.$$

Por tanto,

$$\begin{aligned} (\tfrac{\partial}{\partial y})^{c+1}A(x,y) &= (\tfrac{\partial}{\partial y})^{c+1}x^n + \sum_{i=0}^{k}(\tfrac{\partial}{\partial y})^{c+1}(A_{d+ic}x^{n-d-ic}y^{d+ic}) \\ &= \sum_{i=0}^{k} A_{d+ic}x^{n-d-ic}(d+ic-c)\cdots(d+ic-1)(d+ic)y^{d+ic-(c+1)} \\ &= \sum_{i=0}^{k} A_{d+ic}(d+ic-c)_{c+1}x^{n-d-ic}y^{d+ic-c-1} \end{aligned}$$

y

$$\begin{aligned} \tfrac{\partial}{\partial y}(\tfrac{\partial}{\partial x})^c A(x,y) &= \tfrac{\partial}{\partial y}(\tfrac{\partial}{\partial x})^c x^n + \sum_{i=0}^{k}(\tfrac{\partial}{\partial y}(\tfrac{\partial}{\partial x})^c)(A_{d+ic}x^{n-d-ic}y^{d+ic}) \\ &= \sum_{i=0}^{k} A_{d+ic}(\tfrac{\partial}{\partial x})^c(x^{n-d-ic})(\tfrac{\partial}{\partial y}(y^{d+ic})) \\ &= \sum_{i=0}^{k} A_{d+ic}(n-d-ic-c+1)\cdots(n-d-ic-1)(n-d-ic) \\ &\quad x^{n-d-ic-c}(d+ic)y^{d+ic-1} \\ &= \sum_{i=0}^{k} A_{d+ic}(n-d-ic-c+1)_c(d+ic)x^{n-d-ic-c}y^{d+ic-1}. \end{aligned}$$

Luego,

$$\begin{aligned} y(y^c-(q-1)^c x^c)(D)A(x,y) &= \sum_{i=0}^{k} A_{d+ic}(d+ic-c)_{c+1}x^{n-d-ic}y^{d+ic-c-1} \\ &\quad -(q-1)^c\sum_{i=0}^{k} A_{d+ic}(n-d-ic-c+1)_c(d+ic) \\ &\quad x^{n-d-ic-c}y^{d+ic-1} \\ &= \sum_{i=0}^{k} A_{d+ic}x^{n-d-ic-c}y^{d+ic-c-1}[(d+ic-c)_{c+1}x^c \\ &\quad -(q-1)^c(n-d-ic-c+1)_c(d+ic)y^c]. \end{aligned}$$

Estamos interesados en determinar el coeficiente del término $x^{n-d-c}y^{d-1}$ a ambos lados de la igualdad 2.14. Éste se obtiene cuando $i=0$ e $i=1$. Esto es, respectivamente:

$$[A_d(d-c)_{c+1}]x^{n-d}y^{d-c-1}-[(q-1)^c(n-d-c+1)_c dA_d]x^{n-d-c}y^{d-1}$$

y

$$[(d)_{c+1}A_{d+c}]x^{n-d-c}y^{d-1}-[(q-1)^c(n-d-2c+1)_c(d+c)A_{d+c}]x^{n-d-2c}y^{d+c-1}.$$

Entonces, el coeficiente buscado es:

$$(d)_{c+1}A_{d+c}-(q-1)^c(n-d-c+1)_c dA_d. \tag{2.15}$$

Por otra parte, para $(d-c)_{c+1}A_d y^{d-c-1}(x^c-y^c)^{d^\perp-c-1}$ el coeficiente de $x^{n-d-c}y^{d-1}$ es

$$-(d-c)_{c+1}A_d(d^\perp-c-1).$$

En efecto, por el teorema 2.1.15, se tiene que $(n-d)/c = d^\perp-c-1$. Si $k := d^\perp-c-1$, entonces

$$\begin{aligned} (d-c)_{c+1}A_d y^{d-c-1}(x^c-y^c)^{d^\perp-c-1} &= (d-c)_{c+1}A_d y^{d-c-1}(x^c-y^c)^k \\ &= (d-c)_{c+1}A_d y^{d-c-1}\sum_{i=0}^{k}\binom{k}{i}(-1)^i x^{c(k-i)}y^{ci} \\ &= \sum_{i=0}^{k}\binom{k}{i}(-1)^i(d-c)_{c+1}A_d y^{d-c-1}x^{c(k-i)}. \end{aligned}$$

Cuando $i=1$, se obtiene el coeficiente de $x^{n-d-c}y^{d-1}$.

Ahora, como

$$y(y^c-(q-1)^c x^c)(D)A(x,y) = (d-c)_{c+1}A_d y^{d-c-1}(x^c-y^c)^{d^\perp-c-1}$$

y teniendo en cuenta que los coeficientes de $x^{n-d-c}y^{d-1}$, observamos que:

$$(d)_{c+1}A_{d+c}-(q-1)^c(n-d-c+1)_c dA_d = -(d-c)_{c+1}A_d(d^\perp-c-1).$$

Entonces,

$$(d)_{c+1}A_{d+c} = [(q-1)^c(n-d-c+1)_c d - (d-c)_{c+1}(d^\perp - c - 1)]A_d.$$

O, de otra forma,

$$(d)_{c+1}\frac{A_{d+c}}{A_d} = (q-1)^c(n-d-c+1)_c d - (d-c)_{c+1}(d^\perp - c - 1).$$

Como $(d)_{c+1} > 0$, entonces $A_{d+c}/A_d \geq 0$, si

$$(q-1)^c(n-d-c+1)_c d \geq (d-c)_{c+1}(d^\perp - c - 1).$$

Pero $d > 0$. Entonces, $A_{d+c}/A_d \geq 0$, si

$$(q-1)^c(n-d-c+1)_c \geq \frac{(d-c)_{c+1}(d^\perp - c - 1)}{d}.$$

Sin embargo,

$$\begin{aligned}(d-c)_{c+1} &= (d-c)(d-c+1)\cdots(d-c+c+1-2)(d-c+c+1-1)\\ &= (d-c)(d-c+1)\cdots(d-1)(d).\end{aligned}$$

Entonces,

$$\begin{aligned}\frac{(d-c)_{c+1}}{d} &= (d-c)(d-c+1)\cdots(d-1)\\ &= (d-c)(d-c+1)\cdots(d-c+c-1)\\ &= (d-c)_c.\end{aligned}$$

Luego,

$$A_{d+c}/A_d \geq 0, \text{ si } (d-c)_c(d^\perp - c - 1) \leq (q-1)^c(n-d-c+1)_c.$$

2. Ahora, consideremos los códigos del tipo 2. Por el teorema 2.1.15 tenemos que: $2d + cd^\perp = n + c(c+2)$ si y sólo si

$$xy(y^c - x^c)(D)A(x,y) = (n-d)(d-c)_{c+1}A_d(xy)^{d-c-1}(x^c - y^c)^{d^\perp - c - 1}. \tag{2.16}$$

Por un lado,

$$\begin{aligned}xy(y^c - x^c)(D)A(x,y) &= (xy^{c+1} - x^{c+1}y)(D)A(x,y)\\ &= [\tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} - (\tfrac{\partial}{\partial x})^{c+1}\tfrac{\partial}{\partial y}]A(x,y)\\ &= \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1}A(x,y) - (\tfrac{\partial}{\partial x})^{c+1}\tfrac{\partial}{\partial y}A(x,y).\end{aligned}$$

Ahora, sea $\lambda = \frac{n-2d}{c}$. Entonces el polinomio enumerador de pesos $A(x,y) \in \mathbb{Z}[x,y]$ de un código binario auto-complementario de longitud n tiene la forma:

$$A(x,y) = x^n + \sum_{i=0}^{\lambda} A_{d+ic} x^{n-d-ic} y^{d+ic} + y^n.$$

Por tanto,

$$\begin{aligned}
\tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} A(x,y) &= \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} x^n + \sum_{i=0}^{\lambda} \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1}(A_{d+ic} x^{n-d-ic} y^{d+ic}) \\
&\quad + \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} y^n \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic) x^{n-d-ic-1}(d+ic)(d+ic-1)\cdots(d+ic-c) \\
&\quad y^{d+ic-(c+1)} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic) x^{n-d-ic-1}(d+ic-c)_{c+1} y^{d+ic-c-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(d+ic-c)_{c+1} x^{n-d-ic-1} y^{d+ic-c-1}
\end{aligned}$$

y

$$\begin{aligned}
(\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} A(x,y) &= (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} x^n + \sum_{i=0}^{\lambda} (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y}(A_{d+ic} x^{n-d-ic} y^{d+ic}) \\
&\quad + (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} y^n \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(n-d-ic-1)\cdots(n-d-ic-c) \\
&\quad x^{n-d-ic-(c+1)}(d+ic) y^{d+ic-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c)_{c+1}(d+ic) x^{n-d-ic-c-1} y^{d+ic-1}.
\end{aligned}$$

Luego,

$$\begin{aligned}
xy(y^c - x^c)(D)A(x,y) &= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(d+ic-c)_{c+1} x^{n-d-ic-1} y^{d+ic-c-1} \\
&\quad - \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c)_{c+1}(d+ic) x^{n-d-ic-c-1} y^{d+ic-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic} x^{n-d-ic-c-1} y^{d+ic-c-1} [(n-d-ic)(d+ic-c)_{c+1} x^c \\
&\quad - (n-d-ic-c)_{c+1}(d+ic) y^c].
\end{aligned}$$

Nuevamente, estamos interesados en determinar el coeficiente del término $x^{n-d-c} y^{d-1}$ a ambos lados de 2.16. Éste también se obtiene cuando $i = 0$ e $i = 1$. Esto es, respectivamente:

$$(d-c)_{c+1}(n-d) A_d x^{n-d-1} y^{d-c-1} - (n-d-c)_{c+1} d A_d x^{n-d-c-1} y^{d-1}$$

y

$$(d)_{c+1}(n-d-c)A_{d+c}x^{n-d-c-1}y^{d-1} - (n-d-2c)_{c+1}(d+c)A_{d+c}x^{n-d-2c-1}y^{d+c-1}.$$

Entonces, el coeficiente buscado es:

$$(d)_{c+1}(n-d-c)A_{d+c} - (n-d-c)_{c+1}dA_d. \tag{2.17}$$

Por otra parte, razonando como lo hicimos anteriormente, para

$$(d-c)_{c+1}(n-d)A_d(xy)^{d-c-1}(x^c-y^c)^{d^\perp-c-1},$$

el coeficiente de $x^{n-d-c-1}y^{d-1}$ es $-(d-c)_{c+1}(n-d)A_d(d^\perp-c-1)$.

Ahora, como

$$xy(y^c-x^c)(D)A(x,y) = (d-c)_{c+1}(n-d)A_d(xy)^{d-c-1}(x^c-y^c)^{d^\perp-c-1}$$

y teniendo en cuenta los coeficientes de $x^{n-d-c-1}y^{d-1}$, observamos que:

$$(d)_{c+1}(n-d-c)A_{d+c} - (n-d-c)_{c+1}dA_d = -(d-c)_{c+1}(n-d)A_d(d^\perp-c-1).$$

Entonces,

$$(d)_{c+1}(n-d-c)A_{d+c} = [(n-d-c)_{c+1}d - (d-c)_{c+1}(n-d)(d^\perp-c-1)]A_d$$

o, equivalentemente,

$$(d)_{c+1}(n-d-c)\frac{A_{d+c}}{A_d} = (n-d-c)_{c+1}d - (d-c)_{c+1}(n-d)(d^\perp-c-1).$$

Si $n-d-c<0$, entonces $\frac{A_{d+c}}{A_d}=0$. Si $n-d-c=0$, es decir, si $n=d+c$, entonces se sigue que $\frac{A_{d+c}}{A_d}=\frac{A_n}{A_d}$ y este es positivo, ya que se verifica que $A_n=A_0=1$ y $A_d>0$. Dado que siempre $(d)_{c+1}>0$, se tiene que $A_{d+c}/A_d\geq 0$ sólo si

$$(n-d-c)_{c+1}d \geq (d-c)_{c+1}(n-d)(d^\perp-c-1).$$

Como $d>0$ y $(n-d)>0$, se verifica que $A_{d+c}/A_d\geq 0$ si y sólo si

$$\frac{(n-d-c)_{c+1}}{(n-d)} \geq \frac{(d-c)_{c+1}(d^\perp-c-1)}{d}.$$

Sin embargo,

$$\begin{aligned}(n-d-c)_{c+1} &= (n-d-c)(n-d-c+1)\cdots(n-d-c+c-1)(n-d-c+c)\\ &= (n-d-c)(n-d-c+1)\cdots(n-d-1)(n-d).\end{aligned}$$

Entonces,

$$\begin{aligned}\frac{(n-d-c)_{c+1}}{(n-d)} &= (n-d-c)(n-d-c+1)\cdots(n-d-1)\\ &= (n-d-c)(n-d-c+1)\cdots(n-d-c+c-1)\\ &= (n-d-c)_c\end{aligned}$$

y ya probamos que $\frac{(d-c)_{c+1}}{d}=(d-c)_c$. Luego,

$$A_{d+c}/A_d \geq 0, \text{ si } (d-c)_c(d^\perp - c - 1) \leq (n-d-c)_c.$$

□

2.3. Polinomios enumeradores auto-duales

Sea $\sigma \in GL(2,\mathbb{Q})$. Esto es, σ pertenece al conjunto de las matrices invertibles de tamaño 2×2 con entradas racionales. Además, σ sea dada por la transformación de Mac-Williams

$$\sigma = \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}.$$

Sean $\gamma(x,y)$ y $p(x,y)$ polinomios homogéneos sobre los enteros definidos de la siguiente manera:

(Tipo 1) $\gamma(x,y) = y(y^c - x^c)$ y $p(x,y) = y(y^c - (q-1)^c x^c)$,

(Tipo 2) $\gamma(x,y) = xy(y^c - x^c)$ y $p(x,y) = xy(y^c - x^c)$.

Se verifica que $p(x,y) = \gamma((x,y)\rho)$, para

$$\rho = \begin{pmatrix} q-1 & 0 \\ 0 & 1 \end{pmatrix},$$

con $\rho \in GL(2,\mathbb{Q})$. En efecto,

$$\begin{aligned} \gamma((x,y)\rho) &= \gamma((x,y)\begin{pmatrix} q-1 & 0 \\ 0 & 1 \end{pmatrix}) \\ &= \gamma((q-1)x,y) \\ &= y(y^c - (q-1)^c x^c) \\ &= p(x,y). \end{aligned}$$

Lema 2.3.1 *Con las notaciones anteriores, se cumple que*

$$\gamma((x,y)\sigma) = \lambda\gamma(x,y) \Leftrightarrow p((x,y)\sigma^T) = \lambda p(x,y).$$

Esto significa que $\gamma(x,y)$ es invariante con respecto a σ si y sólo si $p(x,y)$ es invariante con respecto a σ^T.

DEMOSTRACIÓN. Supongamos que $\gamma((x,y)\sigma) = \lambda\gamma(x,y)$. Sabemos que $p(x,y) = \gamma((x,y)\rho)$ y, además, con un cálculo directo, se tiene que

$$\rho\sigma = \sigma^T\rho.$$

Por tanto,

$$\begin{aligned} p((x,y)\sigma^T) &= \gamma((x,y)\sigma^T\rho) \\ &= \gamma((x,y)\rho\sigma) \\ &= \lambda\gamma((x,y)\rho) \\ &= \lambda p(x,y). \end{aligned}$$

Recíprocamente, supongamos que $p((x,y)\sigma^T) = \lambda p(x,y)$. Dado que $p(x,y) = \gamma((x,y)\rho)$, se verifica que $p((x,y)\rho^{-1}) = \gamma(x,y)$. Además, $\sigma\rho^{-1} = \rho^{-1}\sigma^T$, pues ya probamos que $\rho\sigma = \sigma^T\rho$. Luego,

$$\begin{aligned} \gamma((x,y)\sigma) &= p((x,y)\sigma\rho^{-1}) \\ &= p((x,y)\rho^{-1}\sigma^T) \\ &= \lambda p((x,y)\rho^{-1}) \\ &= \lambda\gamma(x,y). \end{aligned}$$

□

Lema 2.3.2 *Con las notaciones anteriores, la igualdad*

$$\gamma((x,y)\sigma) = \lambda\gamma(x,y)$$

se cumple sólo para los siguientes parámetros:

	$(q,c) = (q,1)$	$(\lambda = q)$
Tipo 2	$(q,c) = (2,2)$	$(\lambda = 4)$
Tipo 2	$(q,c) = (2,4)$	$(\lambda = 8)$
Tipo 1	$(q,c) = (3,3)$	$(\lambda = 9)$
Tipo 1	$(q,c) = (4,2)$	$(\lambda = 8)$

DEMOSTRACIÓN.

1) En primer lugar, se acotarán las posibilidades para q. Sea $c = 1$. Entonces,

$$\begin{aligned} \gamma((x,y)\sigma) &= \gamma\left((x,y)\begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}\right) \\ &= \gamma(x+y(q-1), x-y) \\ &= (x-y)((x-y)^1 - (x+y(q-1))^1) \\ &= (x-y)(-y-y(q-1)) \\ &= -xy - xy(q-1) + y^2 + y^2(q-1) \\ &= -xyq + qy^2 \\ &= qy(y-x) \\ &= q\gamma(x,y). \end{aligned}$$

Los parámetros son, por lo tanto, $(q,c) = (q,1)$ y $\lambda = q$ y ese es el primer caso. Sean ahora $c > 1$ y y un cero de $\gamma(1,y)$, con $y \neq 0,1$. Puesto que

$$\gamma((x,y)\sigma) = \lambda\gamma(x,y),$$

se sigue que

$$\begin{aligned} 0 &= \lambda\gamma(1,y) \\ &= \gamma((1,y)\sigma) \\ &= \gamma(1+y(q-1),1-y) \\ &= (1-y)((1-y)^c - (1+y(q-1))^c). \end{aligned}$$

El caso $y = 1$ fué excluido. Entonces, $1-y \neq 0$. Por tanto, $\gamma((1,y)\sigma) = 0$ si y sólo si $(1-y)^c = (1+y(q-1))^c$. Examinemos lo que el parámetro q tiene que cumplir para que

$$|1+y(q-1)| = |1-y|.$$

Veamos:

$$\begin{aligned} |1+y(q-1)| = |1-y| &\Leftrightarrow (1+y(q-1))^2 = (1-y)^2 \\ &\Leftrightarrow 1-2y+y^2 = 1+2y(q-1)+y^2(q-1)^2 \\ &\Leftrightarrow qy(2+qy-2y) = 0 \\ &\Leftrightarrow 2+qy-2y = 0 \\ &\Leftrightarrow y(q-2)+2 = 0. \end{aligned}$$

Con lo cual, se deduce que $q \leq 4$, ya que $y \in \mathbb{Z}$. En consecuencia, q se limita a las opciones: $q \in \{2,3,4\}$.

2) Para el tipo 1, $\gamma(x,y)$ y $p(x,y)$ son polinomios homogéneos de grado $c+1$. Además, sabemos que

$$\gamma((x,y)\sigma^2) = \gamma((x,y)\sigma\sigma) = \lambda\gamma((x,y)\sigma) = \lambda^2\gamma(x,y)$$

y, por otro lado, que

$$\begin{aligned} \gamma((x,y)\sigma^2) &= \gamma\left((x,y)\begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}^2\right) \\ &= \gamma\left((x,y)\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}\right) \\ &= \gamma(qx,qy) \\ &= qy(q^cy^c - q^cx^c) \\ &= q^{c+1}y(y^c - x^c) \\ &= q^{c+1}\gamma(x,y). \end{aligned}$$

Luego, $\lambda^2\gamma(x,y) = q^{c+1}\gamma(x,y)$, obteniendo así para el tipo 1:

$$\lambda^2 = q^{c+1}$$

o, equivalentemente,

$$\lambda = \pm\sqrt{q^{c+1}},$$

y para el tipo 2:

$$\lambda^2 = 2^{c+2}$$

o, equivalentemente,

$$\lambda = \pm\sqrt{2^{c+2}},$$

teniendo en cuenta que, en este caso, $\gamma(x,y)$ y $p(x,y)$ son polinomios homogéneos de grado $c+2$ y $q=2$.

3) Examinemos, en primer lugar, los parámetros que se obtienen para el tipo 1. Con respecto al λ que se obtuvo en 2), tenemos que

$$\gamma((x,y)\sigma) = \lambda\gamma(x,y) = \lambda y(y^c - x^c) = \pm\sqrt{q^{c+1}}(y^{c+1} - yx^c).$$

Además,

$$\begin{aligned}
\gamma((x,y)\sigma) &= \gamma\left((x,y)\begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}\right) \\
&= \gamma(x+y(q-1), x-y) \\
&= (x-y)((x-y)^c - (x+y(q-1))^c) \\
&= (x-y)[\sum_{k=0}^{c}\binom{c}{k}(-1)^k x^{c-k}y^k - \sum_{k=0}^{c}\binom{c}{k}x^{c-k}y^k(q-1)^k] \\
&= (x-y)\sum_{k=0}^{c}\binom{c}{k}x^{c-k}y^k[(-1)^k - (q-1)^k]
\end{aligned}$$

y, como también $\gamma((x,y)\sigma) = \pm\sqrt{q^{c+1}}(y^{c+1} - yx^c)$, entonces debe cumplirse que $\sqrt{q^{c+1}} \in \mathbb{Z}$. Los únicos parámetros que cumplen con esto son $(q,c) = (2,2)$ y $(q,c) = (2,4)$, con los correspondientes λ.

4) Para el tipo 2 se procederá de la misma manera. Entonces, tenemos que

$$\begin{aligned}
\gamma((x,y)\sigma) &= \gamma(x+y, x-y) \\
&= (x^2-y^2)((x-y)^c - (x+y)^c) \\
&= (x^2-y^2)[\sum_{k=0}^{c}\binom{c}{k}x^{c-k}y^k((-1)^k - 1)]
\end{aligned}$$

y, como también $\gamma((x,y)\sigma) = \pm\sqrt{2^{c+2}}(xy^{c+1} - yx^{c+1})$, entonces debe cumplirse que $\sqrt{2^{c+2}} \in \mathbb{Z}$. Ahora, $(q,c) = (2,2)$ y $(q,c) = (2,4)$ son los únicos parámetros que cumplen con esto, con lo que se demuestra la afirmación.

□

Teorema 2.3.3 (Gleason-Pierce) *Sea C un código c-divisible auto-dual de longitud n sobre $\mathbb{F}_q$, con $c > 1$. Entonces,*

$$\begin{array}{ll} \textit{Tipo I} & (q,c) = (2,2), \quad o \\ \textit{Tipo II} & (q,c) = (2,4), \quad o \\ \textit{Tipo III} & (q,c) = (3,3), \quad o \\ \textit{Tipo IV} & (q,c) = (4,2). \end{array}$$

DEMOSTRACIÓN. Ver [7] o [8]. □

No es de extrañar que los únicos casos no triviales para los cuales λ en el lema 2.3.2 es invariante, son también aquellos que están dados mediante el teorema de Gleason-Pierce. La demostración de este teorema en [8] determina, en primer lugar, las condiciones necesarias para que λ sea invariante. Luego, la demostración continua estableciendo cotas para c.

Teorema 2.3.4 *Sea C un código c-divisible, auto-dual, de longitud n y distancia mínima d. Entonces, se verifica que*

$$\textit{(Tipo 1)} \quad d \leq c\lfloor n/c(c+1)\rfloor + c \quad \textit{(auto-dual),}$$

$$\textit{(Tipo 2)} \quad d \leq c\lfloor n/c(c+2)\rfloor + c \quad \textit{(auto-dual).}$$

DEMOSTRACIÓN. Por teorema 2.1.15, sabemos que

$$\text{(Tipo 1)} \quad d + cd^{\perp} \leq n + c(c+1),$$

$$\text{(Tipo 2)} \quad 2d + cd^{\perp} \leq n + c(c+2).$$

Como C es auto-dual, entonces $d = d^{\perp}$ y estas últimas desigualdades quedarían de la forma

$$\text{(Tipo 1)} \quad d + cd \leq n + c(c+1),$$

$$\text{(Tipo 2)} \quad 2d + cd \leq n + c(c+2),$$

o, equivalentemente,

$$\text{(Tipo 1)} \quad d(c+1) \leq n + c(c+1),$$

$$\text{(Tipo 2)} \quad d(c+2) \leq n + c(c+2).$$

Esto implica que

$$\text{(Tipo 1)} \quad d \leq n/(c+1) + c,$$

$$\text{(Tipo 2)} \quad d \leq n/(c+2) + c,$$

o, equivalentemente,

$$\text{(Tipo 1)} \quad d \leq c\lfloor n/c(c+1)\rfloor + c,$$

$$\text{(Tipo 2)} \quad d \leq c\lfloor n/c(c+2)\rfloor + c.$$

Tenga en cuenta que si $x \in \mathbb{Z}$, $a \in \mathbb{N}$ y $ax \leq y$, entonces: $x \leq \lfloor y/a \rfloor$. □

Teorema 2.3.5 *[Cotas de Mallows-Sloane] Sea C un código c-divisible, auto-dual, de longitud n y distancia mínima d sobre $\mathbb{F}_q$, con $c > 1$. Entonces,*

$$\begin{array}{ll} \textit{Tipo I} & d \leq 2\lfloor n/8 \rfloor + 2 \\ \textit{Tipo II} & d \leq 4\lfloor n/24 \rfloor + 4 \\ \textit{Tipo III} & d \leq 3\lfloor n/12 \rfloor + 3 \\ \textit{Tipo IV} & d \leq 2\lfloor n/6 \rfloor + 2, \end{array}$$

donde

$$\begin{array}{ll} \textit{Tipo I} & (q,c) = (2,2) \\ \textit{Tipo II} & (q,c) = (2,4) \\ \textit{Tipo III} & (q,c) = (3,3) \\ \textit{Tipo IV} & (q,c) = (4,2). \end{array}$$

DEMOSTRACIÓN. El teorema de Gleason-Pierce clasifica a los códigos c-divisibles, auto-duales, no triviales en los siguientes cuatro casos:

$$\begin{array}{ll} \text{Tipo I} & (q,c) = (2,2) \\ \text{Tipo II} & (q,c) = (2,4) \\ \text{Tipo III} & (q,c) = (3,3) \\ \text{Tipo IV} & (q,c) = (4,2). \end{array}$$

El resto se sigue utilizando el teorema 2.3.4 y demostrando las cotas de Mallows-Sloane. □

Lema 2.3.6 *Sean C un código c-divisible, auto-dual, de longitud n y distancia mínima d y $A(x,y) \in \mathbb{Z}[x,y]$ su correspondiente polinomio enumerador de pesos. Además, definamos*

$$a(x,y) = (\gamma(x,y))^{d-c-1}$$

y $p(x,y)$ de la siguiente forma:

$$\textit{(Tipo 1)} \quad a(x,y) := y^{d-c-1}(y^c - x^c)^{d-c-1} \qquad p(x,y) := y(y^c - (q-1)^c x^c),$$

$$\textit{(Tipo 2)} \quad a(x,y) := (xy)^{d-c-1}(y^c - x^c)^{d-c-1} \qquad p(x,y) := xy(y^c - x^c).$$

$\widetilde{a}(x,y)$ denotará el factor complementario en

$$a(x,y) \mid p(x,y)(D)A(x,y).$$

Entonces, $\widetilde{a}(x,y)$ es c-divisible e invariante bajo la transformación de MacWilliams

$$\sigma = \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}.$$

DEMOSTRACIÓN. Del lema 2.1.13 y dado que $d = d^{\perp}$ se tiene que

$$a(x,y) \mid p(x,y)(D)A(x,y)$$

y, por tanto,

(Tipo 1) $\quad y^{d-c-1}(y^c - x^c)^{d-c-1} \mid y(y^c - (q-1)^c x^c)(D)A(x,y)$,

(Tipo 2) $\quad (xy)^{d-c-1}(y^c - x^c)^{d-c-1} \mid xy(y^c - x^c)(D)A(x,y)$.

Si $\widetilde{a}(x,y)$ es c-divisible, entonces toda potencia de y con coeficientes no nulos en el polinomio es divisibles por c.

i) Para el tipo 1,

$$\begin{aligned} p(x,y)(D)A(x,y) &= y(y^c - (q-1)^c x^c)(D)A(x,y) \\ &= \partial/\partial y[(\partial/\partial y)^c - (q-1)^c(\partial/\partial x)^c]A(x,y) \\ &= (\partial/\partial y)^{c+1}A(x,y) - (q-1)^c(\partial/\partial x)^c \partial/\partial y A(x,y). \end{aligned}$$

Además, se sabe que el polinomio enumerador de pesos homogéneo $A(x,y)$ para un código c-divisible, de longitud n es de la forma

$$A(x,y) = x^n + \textstyle\sum_{i=0}^{\lambda} A_{d+ic} x^{n-d-ic} y^{d+ic},$$

con $\lambda = \frac{n-d}{c}$. Por tanto,

$$\begin{aligned} (\tfrac{\partial}{\partial y})^{c+1}A(x,y) &= (\tfrac{\partial}{\partial y})^{c+1}(x^n) + \sum_{i=0}^{\lambda}(\tfrac{\partial}{\partial y})^{c+1}(A_{d+ic}x^{n-d-ic}y^{d+ic}) \\ &= \sum_{i=0}^{\lambda} A_{d+ic}x^{n-d-ic}(d+ic)(d+ic-1)\cdots(d+ic-c)y^{d+ic-(c+1)} \\ &= \sum_{i=0}^{\lambda} A_{d+ic}x^{n-d-ic}(d+ic-c)_{c+1}y^{d+ic-c-1} \\ &= \sum_{i=0}^{\lambda} A_{d+ic}(d+ic-c)_{c+1}x^{n-d-ic}y^{d+ic-c-1} \end{aligned}$$

y

$$\begin{aligned} (\tfrac{\partial}{\partial x})^c \tfrac{\partial}{\partial y}A(x,y) &= (\tfrac{\partial}{\partial x})^c \tfrac{\partial}{\partial y}x^n + \sum_{i=0}^{\lambda}(\tfrac{\partial}{\partial x})^c \tfrac{\partial}{\partial y}(A_{d+ic}x^{n-d-ic}y^{d+ic}) \\ &= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(n-d-ic-1)\cdots(n-d-ic-(c-1)) \\ &\quad x^{n-d-ic-c}(d+ic)y^{d+ic-1} \\ &= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-(c-1))_c(d+ic)x^{n-d-ic-c}y^{d+ic-1} \\ &= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c+1)_c(d+ic)x^{n-d-ic-c}y^{d+ic-1}. \end{aligned}$$

Luego,

$$\begin{aligned} p(x,y)(D)A(x,y) &= \sum_{i=0}^{\lambda} A_{d+ic}(d+ic-c)_{c+1}x^{n-d-ic}y^{d+ic-c-1} \\ &\quad -(q-1)^c[\sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c+1)_{c+1}(d+ic)x^{n-d-ic-c}y^{d+ic-1}] \\ &= \sum_{i=0}^{\lambda} A_{d+ic}x^{n-d-ic-c}y^{d+ic-c-1}[(d+ic-c)_{c+1}x^c \\ &\quad -(q-1)^c(n-d-ic-c+1)_c(d+ic)y^c]. \end{aligned}$$

Entonces, en este polinomio, y es de la forma

$$y^{ic-c+d-1} \quad \wedge \quad y^{ic+d-1},$$

donde $i = 0, ..., \lambda$. Ahora, dado que $a(x,y) = (\gamma(x,y))^{d-c-1}$, se tiene que

$$a(x,y) = y^{d-c-1}(y^c - x^c)^{d-c-1}.$$

Entonces,

$$\begin{aligned} a(x,y) &= y^{d-c-1}\sum_{k=0}^{d-c-1}\binom{d-c-1}{k}(-1)^k(y^c)^{(d-c-1)-k}(x^c)^k \\ &= \sum_{k=0}^{d-c-1}\binom{d-c-1}{k}(-1)^k y^{d-c-1}y^{cd-c^2-c-kc}x^{ck} \\ &= \sum_{k=0}^{d-c-1}\binom{d-c-1}{k}(-1)^k y^{cd-c^2-c-kc+d-c-1}x^{ck} \\ &= \sum_{k=0}^{d-c-1}\binom{d-c-1}{k}(-1)^k y^{cd-c^2-2c-kc+d-1}x^{ck} \\ &= \sum_{k=0}^{d-c-1}\binom{d-c-1}{k}(-1)^k y^{c(d-c-2-k)+d-1}x^{ck}. \end{aligned}$$

Luego, en el polinomio $a(x,y)$, y tiene la forma

$$y^{c(d-c-2-k)+d-1},$$

donde $k = 0, ..., d-c-1$. Por lo tanto, permanece un y libre, el cual tiene en la potencia un múltiplo de c, cuando $a(x,y)$ divide al polinomio $p(x,y)$, ya que y^{d-1} se simplifica. En consecuencia, toda potencia de y en $\widetilde{a}(x,y)$ es divisible por c y así se tiene que el polinomio es c-divisible.

ii) Para el tipo 2,

$$\begin{aligned} p(x,y)(D)A(x,y) &= xy(y^c - x^c)(D)A(x,y) \\ &= \frac{\partial}{\partial x}\frac{\partial}{\partial y}[(\frac{\partial}{\partial y})^c - (\frac{\partial}{\partial x})^c]A(x,y) \\ &= \frac{\partial}{\partial x}(\frac{\partial}{\partial y})^{c+1}A(x,y) - (\frac{\partial}{\partial x})^{c+1}\frac{\partial}{\partial y}A(x,y). \end{aligned}$$

$A(x,y)$ es el polinomio enumerador de pesos homogéneo para un código binario, auto-complementario, de longitud n, y por lo tanto de la forma

$$A(x,y) = x^n + \sum_{i=0}^{\lambda} A_{d+ic} x^{n-d-ic} y^{d+ic} + y^n,$$

con $\lambda = \frac{n-2d}{c}$. Entonces,

$$\begin{aligned}
\tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} A(x,y) &= \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} x^n + \sum_{i=0}^{\lambda} \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1}(A_{d+ic} x^{n-d-ic} y^{d+ic}) \\
&\quad + \tfrac{\partial}{\partial x}(\tfrac{\partial}{\partial y})^{c+1} y^n \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic) x^{n-d-ic-1}(d+ic)(d+ic-1)\cdots(d+ic-c) \\
&\quad y^{d+ic-(c+1)} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic) x^{n-d-ic-1}(d+ic-c)_{c+1} y^{d+ic-c-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(d+ic-c)_{c+1} x^{n-d-ic-1} y^{d+ic-c-1}
\end{aligned}$$

y

$$\begin{aligned}
(\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} A(x,y) &= (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} x^n + \sum_{i=0}^{\lambda} (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y}(A_{d+ic} x^{n-d-ic} y^{d+ic}) \\
&\quad + (\tfrac{\partial}{\partial x})^{c+1} \tfrac{\partial}{\partial y} y^n \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(n-d-ic-1)\cdots(n-d-ic-c) \\
&\quad x^{n-d-ic-(c+1)}(d+ic) y^{d+ic-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c)_{c+1}(d+ic) x^{n-d-ic-c-1} y^{d+ic-1}.
\end{aligned}$$

Luego,

$$\begin{aligned}
p(x,y)(D)A(x,y) &= \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic)(d+ic-c)_{c+1} x^{n-d-ic-1} y^{d+ic-c-1} \\
&\quad - \sum_{i=0}^{\lambda} A_{d+ic}(n-d-ic-c)_{c+1}(d+ic) x^{n-d-ic-c-1} y^{d+ic-1} \\
&= \sum_{i=0}^{\lambda} A_{d+ic} x^{n-d-ic-c-1} y^{d+ic-c-1} [(n-d-ic)(d+ic-c)_{c+1} x^c \\
&\quad - (n-d-ic-c)_{c+1}(d+ic) y^c].
\end{aligned}$$

Por ende, en este polinomio, y es de la forma

$$y^{ic-c+d-1} \quad \wedge \quad y^{ic+d-1},$$

donde $i = 0, ..., \lambda$. Además, como

$$a(x,y) = (xy)^{d-c-1}(y^c - x^c)^{d-c-1},$$

entonces

$$\begin{aligned} a(x,y) &= (xy)^{d-c-1} \sum_{k=0}^{d-c-1} \binom{d-c-1}{k} (-1)^k (y^c)^{(d-c-1)-k} (x^c)^k \\ &= \sum_{k=0}^{d-c-1} \binom{d-c-1}{k} (-1)^k (xy)^{d-c-1} y^{cd-c^2-c-kc} x^{d-c-1+ck} \\ &= \sum_{k=0}^{d-c-1} \binom{d-c-1}{k} (-1)^k y^{cd-c^2-c-kc+d-c-1} x^{d-c-1+ck} \\ &= \sum_{k=0}^{d-c-1} \binom{d-c-1}{k} (-1)^k y^{cd-c^2-2c-kc+d-1} x^{d-c-1+ck} \\ &= \sum_{k=0}^{d-c-1} \binom{d-c-1}{k} (-1)^k x^{d-c-1+ck} y^{c(d-c-2-k)+d-1}. \end{aligned}$$

Luego, en el polinomio $a(x,y)$, y tiene la forma

$$y^{c(d-c-2-k)+d-1},$$

donde $k = 0, ..., d-c-1$. Usando el mismo razonamiento que en $i)$, se deduce que para el tipo 2, toda potencia de y en $\widetilde{a}(x,y)$ es divisible por c y, en consecuencia, el polinomio es c-divisible.

iii) En primer lugar, debe tenerse en cuenta que $p(x,y)$ es invariante con respecto a σ^T. Es decir,

$$p((x,y)\sigma^T) = \lambda p(x,y).$$

Del lema 2.3.1, es conocido que

$$\gamma((x,y)\sigma) = \lambda\gamma(x,y) \Leftrightarrow p((x,y)\sigma^T) = \lambda p(x,y)$$

y que $\gamma(x,y)$ es invariante, con respecto a la transformación de Mac-Williams, exactamente para el parámetro (q,c), donde $A(x,y)$ es el polinomio enumerador de pesos homogéneo de un código auto-dual. Dad que $\gamma(x,y)$ es invariante con respecto a la transformación de Mac-Williams σ y como por definición $a(x,y) = [\gamma(x,y)]^{d-c-1}$, entonces

$$\begin{aligned} a((x,y)\sigma) &= [\gamma((x,y)\sigma)]^{d-c-1} \\ &= [\lambda\gamma(x,y)]^{d-c-1} \\ &= \lambda^{d-c-1}[\gamma(x,y)]^{d-c-1} \\ &= \lambda^{d-c-1}a(x,y). \end{aligned}$$

Lo que nos ayuda a concluir que $a(x,y)$ es también invariante con respecto a σ. Además, por el teorema de la dualidad de Mac-Williams y por el hecho de que el código es auto-dual, tenemos que

$$A(x,y) = q^{-n/2}A(x + (q-1)y, x - y)$$

o

$$q^{n/2}A(x,y) = A((x,y)\sigma),$$

pues

$$(x,y)\sigma = (x,y)\begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix} = (x+(q-1)y, x-y).$$

En realidad lo que necesitamos es que

$$p(x,y)(D) = p((u,v)\sigma^T)(D), \tag{2.18}$$

pero esto fue demostrado en el lema 2.1.5.

Recordemos que $\widetilde{a}(x,y)$ se definió como el factor complementario en $a(x,y) \mid p(x,y)(D)A(x,y)$, por lo que

$$\frac{p(u,v)(D)A(u,v)}{a(u,v)} = \widetilde{a}(u,v).$$

Dado que $p((x,y)\sigma^T) = \lambda p(x,y)$, se tiene que $p((x,y)\sigma^T)/\lambda = p(x,y)$. Luego,

$$\frac{p((u,v)\sigma^T)(D)A(u,v)}{\lambda a(u,v)} = \widetilde{a}(u,v).$$

Ahora, usamos el hecho de que $(u,v) = (x,y)\sigma$ y (2.18), para obtener

$$\frac{p(x,y)(D)A((x,y)\sigma)}{\lambda a((x,y)\sigma)} = \widetilde{a}((x,y)\sigma).$$

Teniendo en cuenta que $a((x,y)\sigma) = \lambda^{d-c-1}a(x,y)$ y $q^{n/2}A(x,y) = A((x,y)\sigma)$, se obtiene que

$$\frac{p(x,y)(D)q^{n/2}A(x,y)}{\lambda^{d-c}a(x,y)} = \widetilde{a}((x,y)\sigma)$$

o, equivalentemente,

$$\frac{p(x,y)(D)A(x,y)}{a(x,y)} = \frac{\lambda^{d-c}}{q^{n/2}}\widetilde{a}((x,y)\sigma).$$

Pero como en un principio $\frac{p(u,v)(D)A(u,v)}{a(u,v)} = \widetilde{a}(u,v)$, entonces

$$\widetilde{a}(x,y) = \frac{\lambda^{d-c}}{q^{n/2}}\widetilde{a}((x,y)\sigma).$$

Sea $\widetilde{\lambda} := \frac{q^{n/2}}{\lambda^{d-c}}$, entonces

$$\widetilde{a}((x,y)\sigma) = \widetilde{\lambda}\widetilde{a}(x,y)$$

y se demuestra la invariancia de $\widetilde{a}(x,y)$ con respecto a la transformación de MacWilliams σ.

□

Definición 2.3.7 *Un código auto-dual o un polinomio enumerador de pesos se llama extremal, si cumple alguna de las cotas de Mallows-Sloane. Estos códigos se conocen como extremales, auto-duales.*

Observación 2.3.8 *Resultados como los del teorema 2.2.1 también podrán ser obtenidos para códigos extremales auto-duales. Si se consideran los parámetros n y d puede llegarse a las cotas de Mallows-Sloane:*

$$\begin{array}{ll} \textit{Tipo I} & d = 2\lfloor n/8 \rfloor + 2 \\ \textit{Tipo II} & d = 4\lfloor n/24 \rfloor + 4 \\ \textit{Tipo III} & d = 3\lfloor n/12 \rfloor + 3 \\ \textit{Tipo IV} & d = 2\lfloor n/6 \rfloor + 2, \end{array}$$

o

$$\begin{array}{lll} \textit{Tipo I} & n = 4(d-2) + 2v, & v = 0, 1, 2, 3. \\ \textit{Tipo II} & n = 6(d-4) + 8v, & v = 0, 1, 2. \\ \textit{Tipo III} & n = 4(d-3) + 4v, & v = 0, 1, 2. \\ \textit{Tipo IV} & n = 3(d-2) + 2v, & v = 0, 1, 2. \end{array}$$

Teorema 2.3.9 (Gleason) *Sea C un código auto-dual sobre $\mathbb{F}_q$. Entonces, el polinomio enumerador de pesos homogéneo de C es un polinomio con coeficientes racionales en $y(x-y)$ y $x^2 + (q-1)y^2$.*

DEMOSTRACIÓN. Ver [9], pág. 106. □

Teorema 2.3.10 (Gleason) *Sea C un código binario auto-dual. Entonces, el polinomio enumerador de pesos homogéneo de C es un polinomio con coeficientes racionales en $x^2 + y^2$ y $x^8 + 14x^4y^4 + y^8$.*

DEMOSTRACIÓN. Ver [9], pág. 106. □

Teorema 2.3.11 *Para polinomios enumeradores de pesos de códigos extremales de (Tipo I)-(Tipo IV) se verifican:*

$$\begin{array}{ll} \textit{(Tipo I)} & (xy^3 - x^3y)(D)A(x,y) = (d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}(x^2+y^2)^v, \\ \textit{(Tipo II)} & (xy^5 - x^5y)(D)A(x,y) = (d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}(x^8+14x^4y^4+y^8)^v, \\ \textit{(Tipo III)} & (y^4 - 8x^3y)(D)A(x,y) = (d-3)_4A_d(y^4 - x^3y)^{d-4}(x^4+9xy^3)^v, \\ \textit{(Tipo III)} & (y^3 - 9x^2y)(D)A(x,y) = (d-2)_3A_d(y^3 - x^2y)^{d-3}(x^2+3y^2)^v. \end{array}$$

En cualquier caso, $A_{d+c}/A_d \geq 0$, si

$$\begin{array}{ll} \textit{Tipo I} & (d-3-v)(d-2)_2 \leq (n-d-2)_2, \\ \textit{Tipo II} & (d-5-14v)(d-4)_4 \leq (n-d-4)_4, \\ \textit{Tipo III} & (d-4-8v)(d-3)_3 \leq 8(n-d-2)_3, \\ \textit{Tipo IV} & (d-3-3v)(d-2)_2 \leq 9(n-d-1)_2. \end{array}$$

DEMOSTRACIÓN.

Tipo I. En este caso, $c = 2$ y $d = d^{\perp}$. El objetivo es mostrar que

$$(xy^3 - x^3y)(D)A(x,y) = (d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}(x^2+y^2)^v,$$

con $A_{d+2}/A_d \geq 0$, si $(d-3-v)(d-2)_2 \leq (n-d-2)_2$.

(i) Del lema 2.1.13 se tiene que

$$(xy)^{d-2-1}(x^2-y^2)^{d^{\perp}-2-1} \mid xy(y^2-x^2)(D)A(x,y).$$

Pero, por un lado,

$$\begin{aligned}(xy)^{d-2-1}(x^2-y^2)^{d^{\perp}-2-1} &= (xy)^{d-3}(x^2-y^2)^{d^{\perp}-3} \\ &= (xy)^{d-3}(x^2-y^2)^{d-3} \\ &= [xy(x^2-y^2)]^{d-3} \\ &= (x^3y - xy^3)^{d-3}\end{aligned}$$

y, por otro lado,

$$xy(y^2-x^2) = (xy^3 - x^3y).$$

Por tanto,

$$(x^3y - xy^3)^{d-3} \mid (xy^3 - x^3y)(D)A(x,y).$$

Si escribimos esto último en la forma

$$\frac{(xy^3 - x^3y)(D)A(x,y)}{(x^3y - xy^3)^{d-3}} = B\widetilde{a}(x,y),$$

entonces con el teorema 2.1.15 se obtiene fácilmente la constante B. Esta está dada por

$$B = (d-2)_3(n-d)A_d.$$

Con el lema 2.3.6 y lo anterior, se tiene que

$$(xy^3 - x^3y)(D)A(x,y) = (d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}\widetilde{a}(x,y),$$

donde $\widetilde{a}(x,y)$ es 2-divisible e invariante bajo la transformación de MacWilliams. El polinomio

$$(xy^3 - x^3y)(D)A(x,y)$$

tiene, por supuesto, grado $n-4$, ya que $A(x,y)$ es polinomio de pesos homogéneo de un código de longitud n. Se aplica a n lo que se conoce del Tipo I en la observación 2.3.8: Esto es, que

$$n = 4(d-2) + 2v,$$

donde $v = 0, 1, 2, 3$. Entonces

$$n - 4 = 4(d-2) + 2v - 4 = 4d - 12 + 2v,$$

donde $v = 0, 1, 2, 3$ (o, de otra forma, $n = 4d - 8 + 2v$). El grado de

$$(d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}$$

es $4(d-3)$ y, por lo tanto, se deduce que $\widetilde{a}(x,y)$ debe tener grado $2v$, donde v debe ser igual a $0, 1, 2$ o 3. Ahora, el teorema de Gleasons nos asegura que

$$(x^2 + y^2)^v$$

es el único polinomio homogéneo de grado $2v$ ($v = 0, 1, 2, 3$) que es invariante con respecto a la transformación de MacWilliams. Luego,

$$(xy^3 - x^3y)(D)A(x,y) = (d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}(x^2 + y^2)^v.$$

(ii) Ahora, una vez más, son comparados los coeficientes de $x^{n-d-3}y^{d-1}$ a ambos lados de la igualdad

$$(xy^3 - x^3y)(D)A(x,y) = (d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}(x^2 + y^2)^v. \tag{2.19}$$

Este coeficiente en el lado izquierdo de (2.19) está dado por

$$(d)_{2+1}(n-d-2)A_{d+2} - (n-d-2)_{2+1}dA_d.$$

Es decir,

$$(d)_3(n-d-2)A_{d+2} - (n-d-2)_3dA_d.$$

(Ver demostración del teorema 2.2.1). Por otro lado,

$$\begin{aligned}
(x^3y - xy^3)^{d-3} &= \sum_{k=0}^{d-3} \binom{d-3}{k} (-1)^k (x^3y)^{d-3-k}(xy^3)^k \\
&= \sum_{k=0}^{d-3} \binom{d-3}{k} (-1)^k x^{3(d-3-k)} y^{d-3-k} x^k y^{3k} \\
&= \sum_{k=0}^{d-3} \binom{d-3}{k} (-1)^k x^{3d-9-2k} y^{d-3+2k}
\end{aligned}$$

y

$$\begin{aligned}
(x^2 + y^2)^v &= \sum_{i=0}^{v} \binom{v}{i} (x^2)^{v-i}(y^2)^i \\
&= \sum_{i=0}^{v} \binom{v}{i} x^{2(v-i)} y^{2i} \\
&= \sum_{i=0}^{v} \binom{v}{i} x^{2v-2i} y^{2i}.
\end{aligned}$$

Por tanto,

$$(x^3y - xy^3)^{d-3}(x^2 + y^2)^v = \sum_{k=0}^{d-3} \binom{d-3}{k} (-1)^k x^{3d-9-2k} y^{d-3+2k} \sum_{i=0}^{v} \binom{v}{i} x^{2v-2i} y^{2i}.$$

Luego, el lado derecho de (2.19) se puede escribir como

$$(d-2)_3(n-d)A_d \sum_{k=0}^{d-3}\sum_{i=0}^{v}\binom{d-3}{k}\binom{v}{i}(-1)^k x^{3d-9-2k-2i+2v}y^{d-3+2k+2i}.$$

$x^{n-d-3}y^{d-1}$ se obtiene cuando $i=1$ y $k=0$ o cuando $i=0$ y $k=1$. En efecto, si $i=1$ y $k=0$, el coeficiente de $x^{n-d-3}y^{d-1}$ o $x^{3d-11+2v}y^{d-1}$ (recordemos que $n-d-3 = 4d-8+2v-d-3 = 3d-11+2v$) es

$$(d-2)_3(n-d)A_d v$$

y si $i=0$ y $k=1$, el coeficiente de $x^{n-d-3}y^{d-1}$ es

$$(d-2)_3(n-d)A_d[-(d-3)].$$

En consecuencia, el coeficiente completo de $x^{n-d-3}y^{d-1}$ es

$$(d-2)_3(n-d)A_d[v-(d-3)]$$

o, de otra forma,

$$(d-2)_3(n-d)A_d(v-d+3).$$

(iii) Los coeficientes de ambos lados deben ser iguales. Así que,

$$(d)_3(n-d-2)A_{d+2} - (n-d-2)_3 d A_d = (d-2)_3(n-d)A_d(v-d+3).$$

Es decir,

$$(d)_3(n-d-2)A_{d+2}/A_d = (n-d-2)_3 d + (d-2)_3(n-d)(v-d+3).$$

Si $n-d-2<0$, entonces $A_{d+2}/A_d = 0$. Si $n-d-2=0$, es decir, $n=d+2$, se deduce que $A_{d+2}/A_d = A_n/A_d$ y esto es mayor que cero puesto que $A_n = A_0 = 1$ y $A_d > 0$. Como $(d)_3 > 0$, siempre es cierto que $A_{d+2}/A_d \geq 0$ exactamente si

$$(n-d-2)_3 d + (d-2)_3(n-d)(v-d+3) \geq 0$$

o, equivalentenmente,

$$(d-2)_3(n-d)(d-3-v) \leq (n-d-2)_3 d.$$

Esto proporciona la desigualdad buscada para $n<d$. Si $n-d=0$, es decir $n=d$, entonces se está en presencia del código de repetición trivial, el cual consta del vector nulo y el vector $(1,...,1)$. Considerando que

$$n = 4(d-2)+2v,$$

para $v=0,1,2,3$ y $n=d$, se deduce que

$$4(d-2)+2v \leq d.$$

Esto es,

$$d \leq \frac{8-2v}{3}$$

o $d \leq 2$. Con esto uno puede decir que el único código no vacío para el cual se verifican las hipótesis es el código $C = \{(0,0),(1,1)\}$. El caso $n=d$ se concluye como ya se hizo en el teorema 2.2.1. Lo mismo se cumple también para el tipo II (ambos son códigos de tipo 2).

Tipo II. Para este tipo, $c = 4$ y $d = d^{\perp}$. El objetivo es mostrar que

$$(xy^5 - x^5y)(D)A(x,y) = (d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}(x^8 + 14x^4y^4 + y^8)^v,$$

con $A_{d+4}/A_d \geq 0$, si $(d-5-14v)(d-4)_4 \leq (n-d-4)_4$.

(i) Del lema 2.1.13 es sabido que

$$(xy)^{d-4-1}(x^4 - y^4)^{d^{\perp}-4-1} \mid xy(y^4 - x^4)(D)A(x,y).$$

Pero, por un lado,

$$\begin{aligned}(xy)^{d-4-1}(x^4 - y^4)^{d^{\perp}-4-1} &= (xy)^{d-5}(x^4 - y^4)^{d^{\perp}-5} \\ &= (xy)^{d-5}(x^4 - y^4)^{d-5} \\ &= (x^5y - xy^5)^{d-5}\end{aligned}$$

y, por otro lado,

$$xy(y^4 - x^4) = (xy^5 - x^5y).$$

Por tanto,

$$(x^5y - xy^5)^{d-5} \mid (xy^5 - x^5y)(D)A(x,y).$$

Si escribimos esto último en la forma

$$\frac{(xy^5 - x^5y)(D)A(x,y)}{(x^5y - xy^5)^{d-5}} = B\widetilde{a}(x,y),$$

entonces con el teorema 2.1.15 se obtiene que la constante B está dada por

$$B = (d-4)_5(n-d)A_d.$$

Con el lema 2.3.6 y lo anterior se tiene que

$$(xy^5 - x^5y)(D)A(x,y) = (d-4)_5(n-d)A_d(x^5y - xy^5)^{d-3}\widetilde{a}(x,y),$$

donde $\widetilde{a}(x,y)$ es 4-divisible e invariante bajo la transformación de MacWilliams. El polinomio

$$(xy^5 - x^5y)(D)A(x,y)$$

tiene grado $n-6$, ya que $A(x,y)$ es polinomio de pesos homogéneo de un código de longitud n. Se aplica a n lo que se conoce del Tipo II en la observación 2.3.8, esto es, que

$$n = 6(d-4) + 8v,$$

donde $v = 0, 1, 2$. Entonces,

$$n - 6 = 6(d-4) + 8v - 6 = 6d - 30 + 8v,$$

donde $v = 0, 1, 2$ (o, de otra forma, $n = 6d - 24 + 8v$). El grado de

$$(d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}$$

es $6(d-5) = 6d-30$ y, por lo tanto, se deduce que $\widetilde{a}(x,y)$ tiene grado $8v$, donde v debe ser igual a $0,1,2$.
Ahora, el teorema de Gleasons nos asegura que

$$(x^8 + 14x^4y^4 + y^8)^v$$

es el único polinomio homogéneo de grado $8v$ ($v = 0,1,2$) que es invariante con respecto a la transformación de MacWilliams. Luego,

$$(xy^5 - x^5y)(D)A(x,y) = (d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}(x^8 + 14x^4y^4 + y^8)^v.$$

(ii) Ahora, comparamos los coeficientes de $x^{n-d-5}y^{d-1}$ a ambos lados de la igualdad

$$(xy^5 - x^5y)(D)A(x,y) = (d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}(x^8 + 14x^4y^4 + y^8)^v. \quad (2.20)$$

Este coeficiente en el lado izquierdo de (2.20) está dado por

$$(d)_{4+1}(n-d-4)A_{d+4} - (n-d-4)_{4+1}dA_d.$$

Es decir,

$$(d)_5(n-d-4)A_{d+4} - (n-d-4)_5dA_d.$$

(Ver demostración del teorema 2.2.1). Por otro lado,

$$\begin{aligned}(x^5y - xy^5)^{d-5} &= \sum_{k=0}^{d-5}\binom{d-5}{k}(-1)^k(x^5y)^{d-5-k}(xy^5)^k \\ &= \sum_{k=0}^{d-5}\binom{d-5}{k}(-1)^k x^{5(d-5-k)}y^{d-5-k}x^k y^{5k} \\ &= \sum_{k=0}^{d-5}\binom{d-5}{k}(-1)^k x^{5d-25-4k}y^{d-5+4k}\end{aligned}$$

y

$$(x^8 + 14x^4y^4 + y^8)^v = \sum_{m_1+m_2+m_3=v}\frac{v!}{m_1!m_2!m_3!}x^{8m_1+4m_2}y^{4m_2+8m_3}.???$$

Por tanto,

$$\begin{aligned}(x^5y - xy^5)^{d-5}(x^8 + 14x^4y^4 + y^8)^v &= \sum_{k=0}^{d-5}\binom{d-5}{k}(-1)^k x^{5d-25-4k}y^{d-5+4k} \\ &\quad \sum_{m_1+m_2+m_3=v}\frac{v!}{m_1!m_2!m_3!}x^{8m_1+4m_2}y^{4m_2+8m_3}.\end{aligned}$$

Luego, el lado derecho de (2.20) se puede escribir como

$$(d-4)_5(n-d)A_d\sum_{k=0}^{d-5}\sum_{m_1+m_2+m_3=v}\binom{d-5}{k}\frac{v!}{m_1!m_2!m_3!}(-1)^k x^{5d-25-4k+8m_1+4m_2}y^{d-5+4k+4m_2+8m_3}.$$

$x^{n-d-5}y^{d-1}$ se obtiene cuando $k=0$, $m_1=v-1$, $m_2=1$ y $m_3=0$ o cuando $k=1$, $m_1=v$ y $m_2=m_3=0$. En efecto, si $k=0$, $m_1=v-1$, $m_2=1$ y $m_3=0$, el coeficiente de $x^{n-d-5}y^{d-1}$ o $x^{5d-29+8v}y^{d-1}$ (recordemos que $n-d-5=6d-24+8v-d-5=5d-29+8v$) es

$$(d-4)_5(n-d)A_d(14v)$$

y si $k=1$, $m_1=v$ y $m_2=m_3=0$, el coeficiente de $x^{n-d-5}y^{d-1}$ es

$$(d-4)_5(n-d)A_d[-(d-5)].$$

En consecuencia, el coeficiente completo de $x^{n-d-5}y^{d-1}$ es

$$(d-4)_5(n-d)A_d[(14v)-(d-5)]$$

o, de otra forma,

$$(d-2)_3(n-d)A_d(14v-d+5).$$

(iii) Los coeficientes en ambos lados deben ser iguales. Así que,

$$(d)_5(n-d-4)A_{d+4}-(n-d-4)_5dA_d=(d-4)_5(n-d)A_d(14v-d+5).$$

Es decir,

$$(d)_5(n-d-4)A_{d+4}/A_d=(n-d-4)_5d+(d-4)_5(n-d)(14v-d+5).$$

Si $n-d-4<0$, entonces $A_{d+4}/A_d=0$. Si $n-d-4=0$, es decir, $n=d+4$, se deduce que $A_{d+4}/A_d=A_n/A_d$ y esto es mayor que cero puesto que $A_n=A_0=1$ y $A_d>0$. Como $(d)_5>0$, siempre es cierto que $A_{d+4}/A_d\geq 0$ exactamente si

$$(n-d-4)_5d+(d-4)_5(n-d)(14v-d+5)\geq 0$$

o, equivalentenmente,

$$(d-4)_5(n-d)(d-5-14v)\leq(n-d-4)_5d.$$

Esto proporciona la desigualdad buscada para $n<d$. Si $n-d=0$, es decir $n=d$, entonces se está en presencia del código de repetición trivial. Considerando que

$$n=6(d-4)+8v,$$

para $v=0,1,2$ y $n=d$, se deduce que

$$6(d-4)+8v\leq d.$$

Esto es,

$$d\leq\frac{24-8v}{5}$$

o $d\leq 4$. Con esto uno puede decir que el único código no vacío para el cual se verifican las hipótesis es el código $C=\{(0,0),(1,1)\}$. El caso $n=d$ se concluye como ya se hizo en el teorema 2.2.1. Lo mismo se cumple también para el tipo II.

Tipo III. Para este tipo, $c = 3$, $q = 3$ y $d = d^{\perp}$. El objetivo es mostrar que

$$(y^4 - 8x^3y)(D)A(x,y) = (d-3)_4 A_d (y^4 - x^3y)^{d-4}(x^4 + 9xy^3)^v,$$

con $A_{d+3}/A_d \geq 0$, si $(d-4-8v)(d-3)_3 \leq 8(n-d-2)_3$.

(i) Del lema 2.1.13 es sabido que

$$y^{d-3-1}(x^3 - y^3)^{d^{\perp}-3-1} \mid y(y^3 - (3-1)^3x^3)(D)A(x,y).$$

Pero, por un lado,

$$\begin{aligned} y^{d-3-1}(x^3 - y^3)^{d^{\perp}-3-1} &= y^{d-4}(x^3 - y^3)^{d^{\perp}-4} \\ &= y^{d-4}(x^3 - y^3)^{d-4} \\ &= [y(x^3 - y^3)]^{d-4} \\ &= (x^3y - y^4)^{d-4} \end{aligned}$$

y, por otro lado,

$$y(y^3 - (3-1)^3x^3) = (y^4 - 8x^3y).$$

Por tanto,

$$(x^3y - y^4)^{d-4} \mid (y^4 - 8x^3y)(D)A(x,y).$$

Si escribimos esto último en la forma

$$\frac{(y^4 - 8x^3y)(D)A(x,y)}{(x^3y - y^4)^{d-4}} = B\widetilde{a}(x,y),$$

entonces con el teorema 2.1.15 se obtiene que la constante B está dada por

$$B = (d-3)_4 A_d.$$

Con el lema 2.3.6 y lo anterior se tiene que

$$(y^4 - 8x^3y)(D)A(x,y) = (d-3)_4 A_d (x^3y - y^4)^{d-4}\widetilde{a}(x,y),$$

donde $\widetilde{a}(x,y)$ es 3-divisible e invariante bajo la transformación de MacWilliams.
El polinomio $(y^4 - 8x^3y)(D)A(x,y)$ tiene grado $n-4$.
Se aplica a n lo que se conoce del Tipo III en la observación 2.3.8. Esto es,

$$n = 4(d-3) + 4v,$$

donde $v = 0, 1, 2$. Entonces,

$$n - 4 = 4(d-3) + 4v - 4 = 4d - 16 + 4v,$$

donde $v = 0, 1, 2$ (o, de otra forma, $n = 4d - 12 + 4v$). El grado de

$$(d-3)_4 A_d (x^3y - y^4)^{d-4}$$

es $4(d-4) = 4d-16$ y, por lo tanto, se deduce que $\widetilde{a}(x,y)$ tiene grado $4v$, donde v debe ser igual a $0,1,2$.
Ahora, el teorema de Gleasons nos asegura que

$$(x^4+8xy^3)^v$$

es el único polinomio homogéneo de grado $4v$ ($v=0,1,2$) que es invariante con respecto a la transformación de MacWilliams. Luego,

$$(y^4-8x^3y)(D)A(x,y) = (d-3)_4A_d(x^3y-y^4)^{d-4}(x^4+8xy^3)^v.$$

(ii) Ahora, comparamos los coeficientes de $x^{n-d-3}y^{d-1}$ a ambos lados de la igualdad

$$(y^4-8x^3y)(D)A(x,y) = (d-3)_4A_d(x^3y-y^4)^{d-4}(x^4+8xy^3)^v. \tag{2.21}$$

Este coeficiente en el lado izquierdo de (2.21) está dado por

$$(d)_{3+1}A_{d+3} - (3-1)^3(n-d-3+1)_3dA_d.$$

Es decir,

$$(d)_4A_{d+3} - 8(n-d-2)_3dA_d.$$

(Ver demostración del teorema 2.2.1). Por otro lado,

$$\begin{aligned}(x^3y-y^4)^{d-4} &= \sum_{k=0}^{d-4}\binom{d-4}{k}(-1)^k(x^3y)^{d-4-k}(y^4)^k\\ &= \sum_{k=0}^{d-4}\binom{d-4}{k}(-1)^kx^{3(d-4-k)}y^{d-4-k}y^{4k}\\ &= \sum_{k=0}^{d-4}\binom{d-4}{k}(-1)^kx^{3d-12-3k}y^{d-4+3k}\end{aligned}$$

y

$$\begin{aligned}(x^4+8xy^3)^v &= \sum_{i=0}^{v}\binom{v}{i}(x^4)^{v-i}(8xy^3)^i\\ &= \sum_{i=0}^{v}\binom{v}{i}x^{4(v-i)}8^ix^iy^{3i}\\ &= \sum_{i=0}^{v}\binom{v}{i}8^ix^{4v-3i}y^{3i}.\end{aligned}$$

Por tanto,

$$(x^3y-y^4)^{d-4}(x^4+8xy^3)^v = \sum_{k=0}^{d-4}\binom{d-4}{k}(-1)^kx^{3d-12-3k}y^{d-4+3k}\sum_{i=0}^{v}\binom{v}{i}8^ix^{4v-3i}y^{3i}$$

Luego, el lado derecho de (2.21) se puede escribir como

$$(d-3)_4A_d\sum_{k=0}^{d-4}\sum_{i=0}^{v}\binom{d-4}{k}\binom{v}{i}(-1)^k8^ix^{3d-12-3k+4v-3i}y^{d-4+3k+3i}.$$

$x^{n-d-3}y^{d-1}$ se obtiene cuando $i = 1$ y $k = 0$ o cuando $i = 0$ y $k = 1$. En efecto, si $i = 1$ y $k = 0$, el coeficiente de $x^{n-d-3}y^{d-1}$ o $x^{3d-15+4v}y^{d-1}$ (recordemos que $n-d-3 = 4d-12+4v-d-3 = 3d-15+4v$) es $(d-3)_4A_d(8v)$ y si $i = 0$ y $k = 1$, el coeficiente de $x^{n-d-3}y^{d-1}$ es $(d-3)_4A_d[-(d-4)]$. En consecuencia, el coeficiente completo de $x^{n-d-3}y^{d-1}$ es

$$(d-3)_4A_d[8v-(d-4)]$$

o, de otra forma,

$$(d-3)_4A_d(8v-d+4).$$

(iii) Los coeficientes en ambos lados deben ser iguales. Así que,

$$(d)_4A_{d+3} - 8(n-d-2)_3dA_d = (d-3)_4A_d(8v-d+4).$$

Es decir,

$$(d)_4A_{d+3}/A_d = 8(n-d-2)_3d + (d-3)_4(8v-d+4).$$

Puesto que $(d)_4 > 0$, siempre es cierto que $A_{d+3}/A_d \geq 0$ exactamente si

$$8(n-d-2)_3d + (d-3)_4(8v-d+4) \geq 0$$

o, equivalentenmente,

$$(d-3)_4(d-4-8v) \leq 8(n-d-2)_3d.$$

Luego

$$\frac{(d-3)_4}{d}(d-4-8v) \leq 8(n-d-2)_3.$$

Pero,

$$\begin{aligned}\frac{(d-3)_4}{d} &= \frac{(d-3)(d-3+1)(d-3+2)(d-3+3)}{d}\\ &= \frac{(d-3)(d-3+1)(d-3+2)d}{d}\\ &= (d-3)(d-3+1)(d-3+2)\\ &= (d-3)_3.\end{aligned}$$

Por lo tanto, la última desigualdad quedaría de la forma

$$(d-3)_3(d-4-8v) \leq 8(n-d-2)_3,$$

lo que queríamos probar.

Tipo IV. Para este tipo, $c = 2$, $q = 4$ y $d = d^{\perp}$. El objetivo es mostrar que

$$(y^3-9x^2y)(D)A(x,y) = (d-2)_3A_d(y^3-x^2y)^{d-3}(x^2+3y^2)^v,$$

con $A_{d+2}/A_d \geq 0$, si $(d-3-3v)(d-2)_2 \leq 9(n-d-1)_2$.

(i) Del lema 2.1.13 es sabido que

$$y^{d-2-1}(x^2-y^2)^{d^\perp-2-1} \mid y(y^2-(4-1)^2x^2)(D)A(x,y).$$

Pero, por un lado,

$$\begin{aligned} y^{d-2-1}(x^2-y^2)^{d^\perp-2-1} &= y^{d-3}(x^2-y^2)^{d^\perp-3} \\ &= y^{d-3}(x^2-y^2)^{d-3} \\ &= [y(x^2-y^2)]^{d-3} \\ &= (x^2y-y^3)^{d-3} \end{aligned}$$

y, por otro lado,

$$y(y^2-(4-1)^2x^2) = (y^3-9x^2y).$$

Por tanto,

$$(x^2y-y^3)^{d-3} \mid (y^3-9x^2y)(D)A(x,y).$$

Si escribimos esto último en la forma

$$\frac{(y^3-9x^2y)(D)A(x,y)}{(x^2y-y^3)^{d-3}} = B\widetilde{a}(x,y),$$

entonces con el teorema 2.1.15 se obtiene que la constante B está dada por

$$B = (d-2)_3A_d.$$

Con el lema 2.3.6 y lo anterior se tiene que

$$(y^3-9x^2y)(D)A(x,y) = (d-2)_3A_d(x^2y-y^3)^{d-3}\widetilde{a}(x,y),$$

donde $\widetilde{a}(x,y)$ es 2-divisible e invariante bajo la transformación de MacWilliams.
El polinomio $(y^3-9x^2y)(D)A(x,y)$ tiene grado $n-3$.
Se aplica a n lo que se conoce del Tipo IV en la observación 2.3.8. Esto es, que

$$n = 3(d-2)+2v,$$

donde $v = 0,1,2$. Entonces,

$$n-3 = 3(d-2)+2v-3 = 3d-9+2v,$$

donde $v = 0,1,2$ (o, de otra forma, $n = 3d-6+2v$). El grado de

$$(d-2)_3A_d(x^2y-y^3)^{d-3}$$

es $3(d-3) = 3d-9$ y, por lo tanto, se deduce que $\widetilde{a}(x,y)$ tiene grado $2v$, donde v debe ser igual a $0,1,2$.
Ahora, el teorema de Gleasons nos asegura que

$$(x^2+3y^2)^v$$

es el único polinomio homogéneo de grado $2v$ (para $v = 0,1,2$) que es invariante con respecto a la transformación de MacWilliams. Luego,

$$(y^3-9x^2y)(D)A(x,y) = (d-2)_3A_d(x^2y-y^3)^{d-3}(x^2+3y^2)^v.$$

(ii) Ahora, comparamos los coeficientes de $x^{n-d-2}y^{d-1}$ a ambos lados de la igualdad

$$(y^3 - 9x^2y)(D)A(x,y) = (d-2)_3 A_d (x^2y - y^3)^{d-3}(x^2 + 3y^2)^v. \tag{2.22}$$

Este coeficiente en el lado izquierdo de (2.22) está dado por

$$(d)_{2+1}A_{d+2} - (4-1)^2(n-d-2+1)_2 dA_d.$$

Es decir,

$$(d)_3 A_{d+2} - 9(n-d-1)_2 dA_d.$$

(Ver demostración del teorema 2.2.1). Por otro lado,

$$\begin{aligned}(x^2y - y^3)^{d-3} &= \sum_{k=0}^{d-3}\binom{d-3}{k}(-1)^k(x^2y)^{d-3-k}(y^3)^k \\ &= \sum_{k=0}^{d-3}\binom{d-3}{k}(-1)^k x^{2(d-3-k)}y^{d-3-k}y^{3k} \\ &= \sum_{k=0}^{d-3}\binom{d-3}{k}(-1)^k x^{2d-6-2k}y^{d-3+2k}\end{aligned}$$

y

$$\begin{aligned}(x^2 + 3y^2)^v &= \sum_{i=0}^{v}\binom{v}{i}(x^2)^{v-i}(3y^2)^i \\ &= \sum_{i=0}^{v}\binom{v}{i}x^{2(v-i)}3^i y^{2i} \\ &= \sum_{i=0}^{v}\binom{v}{i}3^i x^{2v-2i}y^{2i}.\end{aligned}$$

Por tanto,

$$(x^2y - y^3)^{d-3}(x^2 + 3y^2)^v = \sum_{k=0}^{d-3}\binom{d-3}{k}(-1)^k x^{2d-6-2k}y^{d-3+2k}\sum_{i=0}^{v}\binom{v}{i}3^i x^{2v-2i}y^{2i}$$

Luego, el lado derecho de (2.22) se puede escribir como

$$(d-2)_3 A_d \sum_{k=0}^{d-3}\sum_{i=0}^{v}\binom{d-3}{k}\binom{v}{i}(-1)^k 3^i x^{2d-6-2k+2v-2i}y^{d-3+2k+2i}.$$

$x^{n-d-2}y^{d-1}$ se obtiene cuando $i = 1$ y $k = 0$ o cuando $i = 0$ y $k = 1$. En efecto, si $i = 1$ y $k = 0$, el coeficiente de $x^{n-d-2}y^{d-1}$ o $x^{3d-15+4v}y^{d-1}$ (recordemos que $n - d - 2 = 3d - 6 + 2v - d - 2 = 2d - 8 + 2v$) es

$$(d-2)_3 A_d (3v)$$

y si $i = 0$ y $k = 1$, el coeficiente de

$$x^{n-d-2}y^{d-1}$$

es $(d-2)_3 A_d[-(d-3)]$. En consecuencia, el coeficiente completo de $x^{n-d-2}y^{d-1}$ es

$$(d-2)_3 A_d[3v-(d-3)]$$

o, de otra forma,

$$(d-2)_3 A_d(3v-d+3).$$

(iii) Los coeficientes de ambos lados deben ser iguales. Así que,

$$(d)_3 A_{d+2} - 9(n-d-1)_2 d A_d = (d-2)_3 A_d(3v-d+3).$$

Es decir,

$$(d)_3 A_{d+2}/A_d = 9(n-d-1)_2 d + (d-2)_3(3v-d+3).$$

Como $(d)_3 > 0$, siempre es cierto que $A_{d+2}/A_d \geq 0$ exactamente si

$$9(n-d-1)_2 d + (d-2)_3(3v-d+3) \geq 0$$

o, equivalentenmente,

$$(d-2)_3(d-3-3v) \leq 9(n-d-1)_2 d.$$

Luego,

$$\frac{(d-2)_3}{d}(d-3-3v) \leq 9(n-d-1)_2.$$

Pero,

$$\begin{aligned}\frac{(d-2)_3}{d} &= \frac{(d-2)(d-2+1)(d-2+2)}{d} \\ &= \frac{(d-2)(d-2+1)d}{d} \\ &= (d-2)(d-2+1) \\ &= (d-2)_2.\end{aligned}$$

Por lo tanto, la última desigualdad quedaría de la forma

$$(d-2)_2(d-3-3v) \leq 9(n-d-1)_2.$$

Eso era justo lo que queríamos probar.

□

Teorema 2.3.12 *[Cotas de Zhang] Para los polinomios enumeradores de pesos de códigos extremales de (Tipo I)-(Tipo IV),* $A_{d+c}/A_d \geq 0$*, si*

	$v=0$	$v=1$	$v=2$	$v=3$
Tipo I	$n \leq 24$	$n \leq 42$	$n \leq 44$	$n \leq 50$
	$d \leq 8$	$d \leq 12$	$d \leq 12$	$d \leq 13$
Tipo II	$n \leq 3690$	$n \leq 3824$	$n \leq 3952$	
	$d \leq 619$	$d \leq 640$	$d \leq 660$	
Tipo III	$n \leq 840$	$n \leq 896$	$n \leq 944$	
	$d \leq 213$	$d \leq 226$	$d \leq 237$	
Tipo IV	$n \leq 102$	$n \leq 119$	$n \leq 136$	
	$d \leq 36$	$d \leq 41$	$d \leq 46$	

DEMOSTRACIÓN.

Tipo I. El teorema 2.3.11 dice que para códigos de este tipo, $A_{d+2}/A_d \geq 0$, si $(d-3-v)(d-2)_2 \leq (n-d-2)_2$. Además, por la observación 2.3.8, se tiene que $n = 4(d-2)+2v$.

(i) Sea $v = 0$. Entonces, $n = 4d-8$ y $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq ((4d-8)-d-2)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq (3d-10)_2.$$

Es decir,

$$(d-3)(d-2)(d-1) \leq (3d-10)(3d-9).$$

Luego,

$$d^3 - 15d^2 + 68d - 96 \leq 0.$$

A continuación, resolveremos esta desigualdad utilizando el software CAS máxima:

```
(%i1) allroots(d^3-15*d^2+68*d-96);
(%o1)   d = 3,0, d = 4, d = 7,999
(%i2) p_1(d):=d^3-15*d^2+68*d-96;
(%o2)   p_1(d) := d^3 - 15 d^2 + 68 d - 96
(%i3) p_1([2,3.5,5,8,8.1]);
(%o3)   [-12, 1,125, -6, 0, 2,091]
```

Entonces, $d \leq 8$. Por tanto, $n = 4d-8 \leq 24$.

(ii) Sea $v = 1$. Entonces, $n = 4d-6$ y $A_{d+2}/A_d \geq 0$, si

$$(d-4)(d-2)_2 \leq ((4d-6)-d-2)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-4)(d-2)_2 \leq (3d-8)_2.$$

Luego,

$$d^3 - 16d^2 + 59d - 64 \leq 0$$

y

```
(%i1) allroots(d^3-16*d^2+59*d-64);
(%o1)  d = 0,286 i + 2,366, d = 2,366 − 0,286 i, d = 11,268
(%i2) p_2(d):=d^3-16*d^2+59*d-64;
(%o2)  p_2 (d) := d^3 − 16 d^2 + 59 d − 64
(%i3) p_2([11,12]);
(%o3)  [−20, 68]
```

Entonces, $d \leq 12$ y $n = 4d - 6 \leq 42$.

(iii) Sea $v = 2$. Entonces, $n = 4d - 4$ y $A_{d+2}/A_d \geq 0$, si

$$(d-5)(d-2)_2 \leq ((4d-4)-d-2)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq (3d-6)_2.$$

Luego,

$$d^3 - 15d^2 + 44d - 36 \leq 0$$

y

```
(%i1) allroots(d^3-15*d^2+44*d-36);
(%o1)  d = 1,575, d = 2,0, d = 11,424
(%i2) p_3(d):=d^3-15*d^2+44*d-36;
(%o2)  p_3 (d) := d^3 − 15 d^2 + 44 d − 36
(%i3) p_3([1,1.8,11,12]);
(%o3)  [−6, 0,432, −36, 60]
```

Entonces, $d \leq 12$ y $n = 4d - 4 \leq 44$.

(iv) Sea $v = 3$. Entonces, $n = 4d - 2$ y $A_{d+2}/A_d \geq 0$, si

$$(d-6)(d-2)_2 \leq ((4d-2)-d-2)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq (3d-4)_2.$$

Luego,

$$d^3 - 15d^2 + 32d - 18 \leq 0$$

y

```
(%i1) allroots(d^3-15*d^2+32*d-18);
(%o1)  d = 1,0, d = 1,432, d = 12,567
(%i2) p_4(d):=d^3-15*d^2+32*d-18;
(%o2)  p_4(d) := d^3 - 15 d^2 + 32 d - 18
(%i3) p_4([0.5,1.2,12,13]);
(%o3)  [-5,625, 0,528, -66, 60]
```

Entonces, $d \leq 13$ y $n = 4d - 2 \leq 50$.

Tipo II. El teorema 2.3.11 dice que para códigos de este tipo, $A_{d+4}/A_d \geq 0$, si $(d - 5 - 14v)(d-4)_4 \leq (n-d-4)_4$. Además, por la observación 2.3.8, se tiene que $n = 6(d-4) + 8v$.

(i) Sea $v = 0$. Entonces, $n = 6d - 24$ y $A_{d+4}/A_d \geq 0$, si

$$(d-5)(d-4)_4 \leq ((6d-24) - d - 4)_4.$$

Esto es, $A_{d+4}/A_d \geq 0$, si

$$(d-5)(d-4)_4 \leq (5d-28)_4.$$

Esto es,

$$(d-5)(d-4)(d-3)(d-2)(d-1) \leq (5d-28)(5d-27)(5d-26)(5d-25).$$

Luego,

$$d^5 - 640d^4 + 13335d^3 - 105500d^2 + 371804d - 491520 \leq 0$$

y

```
(%i1) allroots(d^5-640*d^4+13335*d^3-105500*d^2+371804*d-491520);
(%o1)  d = 5, d = 0,261 i + 5,139, d = 5,139 - 0,261 i, d = 5,999, d = 618,721]
(%i2) p_5(d):=d^5-640*d^4+13335*d^3-105500*d^2+371804*d-491520;
```

```
(%o2)  p_5(d) := d^5 - 640 d^4 + 13335 d^3 + (-105500) d^2 + 371804 d - 491520
(%i3) p_5([4,5.5,618,619]);
(%o3)  [-1680, 30,46875, -101667276000, 39497527080]
```

Entonces, $d \leq 619$ y $n = 6d - 24 \leq 3690$.

(ii) Sea $v = 1$. Entonces, $n = 6d - 16$ y $A_{d+4}/A_d \geq 0$, si

$$(d-19)(d-4)_4 \leq ((6d-16)-d-4)_4.$$

Esto es, $A_{d+4}/A_d \geq 0$, si

$$(d-19)(d-4)_4 \leq (5d-20)_4.$$

Luego,

$$d^5 - 654d^4 + 9475d^3 - 51990d^2 + 127144d - 116736 \leq 0$$

y

```
(%i1) allroots(d^5-654*d^4+9475*d^3-51990*d^2+127144*d-116736);
(%o1)  d = 3,278, d = 0,419 i + 3,707, d = 3,707 - 0,419 i, d = 4, d = 639,306]
(%i2) p_6(d):=d^5-654*d^4+9475*d^3-51990*d^2+127144*d-116736;
(%o2)  p_6(d) := d^5 - 654 d^4 + 9475 d^3 + (-51990) d^2 + 127144 d - 116736
(%i3) p_6([3,3.5,639,640]);
(%o3)  [-120, 15,46875, -49848363600, 113790311424]
```

Entonces, $d \leq 640$ y $n = 6d - 16 \leq 3824$.

(iii) Sea $v = 2$. Entonces, $n = 6d - 8$ y $A_{d+4}/A_d \geq 0$, si

$$(d-33)(d-4)_4 \leq ((6d-8)-d-4)_4.$$

Esto es, $A_{d+4}/A_d \geq 0$, si

$$(d-33)(d-4)_4 \leq (5d-12)_4.$$

Luego,

$$d^5 - 668d^4 + 5615d^3 - 17680d^2 + 24564d - 12672 \leq 0$$

y

```
(%i1) allroots(d^5-668*d^4+5615*d^3-17680*d^2+24564*d-12672);
(%o1)  d = 1,593, d = 2, d = 0,275 i + 2,439, d = 2,439 − 0,275 i, d = 659,526]
(%i2) p_7(d):=d^5-668*d^4+5615*d^3-17680*d^2+24564*d-12672;
(%o2)  p_7 (d) := d^5 − 668 d^4 + 5615 d^3 + (−17680) d^2 + 24564 d − 12672
(%i3) p_7([1,1.8,659,660]);
(%o3)  [−840, 13,178, −98098325640, 88625951568]
```

Entonces, $d \leq 660$ y $n = 6d - 8 \leq 3952$.

Tipo III. El teorema 2.3.11 dice que para códigos de este tipo, $A_{d+3}/A_d \geq 0$ si y sólo si $(d-4-8v)(d-3)_3 \leq 8(n-d-2)_3$. Además, por la observación 2.3.8, se tiene que $n = 4(d-3)+4v$.

(i) Sea $v = 0$. Entonces, $n = 4d-12$ y $A_{d+3}/A_d \geq 0$, si

$$(d-4)(d-3)_3 \leq 8((4d-12)-d-2)_3.$$

Esto es, $A_{d+3}/A_d \geq 0$, si

$$(d-4)(d-3)_3 \leq 8(3d-14)_3.$$

Esto es,

$$(d-4)(d-3)(d-2)(d-1) \leq 8(3d-14)(3d-13)(3d-12).$$

Luego,

$$d^4 - 226d^3 + 2843d^2 - 12194d + 17496 \leq 0$$

y

```
(%i1) allroots(d^4-226*d^3+2843*d^2-12194*d+17496);
(%o1)  d = 3,999, d = 4,236, d = 4,848, d = 212,914]
(%i2) p_8(d):=d^4-226*d^3+2843*d^2-12194*d+17496;
(%o2)  p_8 (d) := d^4 − 226 d^3 + 2843 d^2 + (−12194) d + 17496
(%i3) p_8([3,4,4.5,212,213]);
(%o3)  [480, 0, 9,5625, −8185632, 777480]
```

Entonces, $d \leq 213$ y $n = 4d - 12 \leq 840$.

(ii) Sea $v = 1$. Entonces, $n = 4d - 8$ y $A_{d+3}/A_d \geq 0$, si

$$(d-12)(d-3)_3 \leq 8((4d-8)-d-2)_3.$$

Esto es, $A_{d+3}/A_d \geq 0$, si

$$(d-12)(d-3)_3 \leq 8(3d-10)_3.$$

Luego,

$$d^4 - 234d^3 + 2027d^2 - 5946d + 5832 \leq 0$$

y

```
(%i1) allroots(d^4-234*d^3+2027*d^2-5946*d+5832);
(%o1)   d = 2,770, d = 3, d = 3,117, d = 225,112]
(%i2) p_9(d):=d^4-234*d^3+2027*d^2-5946*d+5832;
(%o2)   p_9 (d) := d^4 − 234 d^3 + 2027 d^2 + (−5946) d + 5832
(%i3) p_9([2,2.9,3.1,225,226]);
(%o3)   [192, −0,628, 0,128, −1230768, 9847680]
```

Entonces, $d \leq 226$ y $n = 4d - 8 \leq 896$.

(iii) Sea $v = 2$. Entonces, $n = 4d - 4$ y $A_{d+3}/A_d \geq 0$, si

$$(d-20)(d-3)_3 \leq 8((4d-4)-d-2)_3.$$

Esto es, $A_{d+3}/A_d \geq 0$, si

$$(d-20)(d-3)_3 \leq 8(3d-6)_3.$$

Luego,

$$d^4 - 242d^3 + 1211d^2 - 2002d + 1080 \leq 0$$

y

```
(%i1) allroots(d^4-242*d^3+1211*d^2-2002*d+1080);
(%o1)   d = 1,244, d = 1,830, d = 2, d = 236,924]
(%i2) p_10(d):=d^4-242*d^3+1211*d^2-2002*d+1080;
```

```
(%o2)  p_10(d) := d^4 - 242*d^3 + 1211*d^2 + (-2002)*d + 1080
(%i3) p_10([1,1.5,1.9,236,237]);
(%o3)  [48, -9,9375, 1,064, -11889072, 987000]
```

Entonces, $d \leq 237$ y $n = 4d - 4 \leq 944$.

Tipo IV. El teorema 2.3.11 dice que para códigos de este tipo, $A_{d+2}/A_d \geq 0$, si $(d - 3 - 3v)(d-2)_2 \leq 9(n-d-1)_2$. Además, por la observación 2.3.8, se tiene que $n = 3(d-2) + 2v$.

(i) Sea $v = 0$. Entonces, $n = 3d - 6$ y $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq 9((3d-6) - d - 1)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-3)(d-2)_2 \leq 9(2d-7)_2.$$

Luego,

$$d^3 - 42d^2 + 245d - 384 \leq 0$$

y

```
(%i1) allroots(d^3-42*d^2+245*d-384);
(%o1)  d = 2,999, d = 3,617, d = 35,382]
(%i2) p_11(d):=d^3-42*d^2+245*d-384;
(%o2)  p_11(d) := d^3 - 42*d^2 + 245*d - 384
(%i3) p_11([2,3.2,35,36]);
(%o3)  [-54, 2,688, -384, 660]
```

Entonces, $d \leq 36$ y $n = 3d - 6 \leq 102$.

(ii) Sea $v = 1$. Entonces, $n = 3d - 4$ y $A_{d+2}/A_d \geq 0$, si

$$(d-6)(d-2)_2 \leq 9((3d-4) - d - 1)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-6)(d-2)_2 \leq 9(2d-5)_2.$$

Luego,

$$d^3 - 45d^2 + 182d - 192 \leq 0$$

y

```
(%i1) allroots(d^3-45*d^2+182*d-192);
(%o1)  d = 1,999, d = 2,362, d = 40,637]
(%i2) p_12(d):=d^3-45*d^2+182*d-192;
(%o2)  p_12 (d) := d^3 − 45 d^2 + 182 d − 192
(%i3) p_12([1,2.1,40,41]);
(%o3)  [−54, 1,011, −912, 546]
```

Entonces, $d \leq 41$ y $n = 3d - 4 \leq 119$.

(iii) Sea $v = 2$. Entonces, $n = 3d - 2$ y $A_{d+2}/A_d \geq 0$, si

$$(d-9)(d-2)_2 \leq 9((3d-2)-d-1)_2.$$

Esto es, $A_{d+2}/A_d \geq 0$, si

$$(d-9)(d-2)_2 \leq 9(2d-3)_2.$$

Luego,

$$d^3 - 48d^2 + 119d - 72 \leq 0$$

y

```
(%i1) allroots(d^3-48*d^2+119*d-72);
(%o1)  d = 1,0, d = 1,585, d = 45,414]
(%i2) p_13(d):=d^3-48*d^2+119*d-72;
(%o2)  p_13 (d) := d^3 − 48 d^2 + 119 d − 72
(%i3) p_13([0.5,1.4,45,46]);
(%o3)  [−24,375, 3,264, −792, 1170]
```

Entonces, $d \leq 46$ y $n = 3d - 2 \leq 136$.

□

Bibliografía

[1] I. M. DUURSMA, *Extremal weight enumerators and ultraspherical polynomials,* Discrete mathematics, 268, pp. 103 - 127, 2003.

[2] A. M. GLEASON, *Weight polynomials of self-dual codes an the MacWilliams identities*, Actes Congres Internal de Mathematique, vol 3. Paris: Gauthier-Villars, 1971, pp. 211-215.

[3] R. HILL, *A First Course in Coding Theory,* Oxford Applied Mathematics and Computing Science Series, 1990.

[4] F.J. MACWILLIAMS AND N.J.A. SLOANE, *The theory of error-correcting codes,* North Holland, Amsterdam 1977.

[5] C.L. MALLOWS, AND N.J.A. SLOANE, *An upper bound for self-dual codes*. Inform. and Control. v22. 188-200.

[6] E.M. RAINS, *Shadow Bounds for Self-Dual Codes,* IEEE Trans. Info. Theory, 44, pp. 134 - 139, 1998.

[7] E.M. RAINS AND N. J. A. SLOANE, *Self-Dual Codes,* Handbook of coding theory, v. I, II, pp. 177 - 294. North Holland, Amsterdam, 1998.

[8] N. J. A. SLOANE, *Self-Dual Codes and lattices,* Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978), pp. 273 - 308. Amer. math. Soc., Providence, R. I., 1979.

[9] W. WILLEMS, *Codierungstheorie*. De Gruyter Lehrbuch, 1999.

[10] S. ZHANG, *On the nonexsitence of extremal self-dual codes*, Discrete Applied Mathematics, v.91 n.1-3, pp. 277-286, 1999.