

UNIVERSIDAD DEL VALLE

FACULTAD DE CIENCIAS NATURALES Y EXACTAS

DEPARTAMENTO DE MATEMÁTICAS

Cotas en teoría de códigos y la función de Manin

TRABAJO DE GRADO

PARA OPTAR AL TÍTULO DE:

Matemática

Autora:

Luz Angélica PÉREZ GUZMÁN

Director:

Dr. Horacio NAVARRO OYOLA

17 de marzo de 2021



No hay en todo el mundo un triunfo verdadero que pueda separarse de la dignidad en el vivir.

David Starr Jordan

RESUMEN

La teoría de códigos es un área de estudio de las matemáticas que se encarga de detectar y corregir los errores producidos al transmitir mensajes a través de ciertos canales de comunicación con ruido. Dicha teoría se emplea en el intercambio de información a través de dispositivos electrónicos y en el almacenamiento de datos en medios magnéticos; en este último caso el medio de almacenamiento hace las veces de canal de comunicación y el ruido puede deberse, por ejemplo, a imperfecciones en el equipo.

En esta monografía realizaremos un estudio detallado de la teoría básica de códigos, de las distintas cotas para los parámetros de un código y para la función de Manin.

PALABRAS CLAVE: teoría de códigos, cuerpos finitos, matriz generadora, matriz de chequeo de paridad, códigos duales, equivalencia de códigos, códigos perforados, extensión de códigos, codificación, decodificación de máxima verosimilitud, Hamming, Plotkin, Singleton, Elias, Griesmer, Gilbert, Varshamov, Manin, cotas, cotas asintóticas.

ÍNDICE GENERAL

resumen	I
Agradecimientos	IV
Introducción	v
1. Preliminares	1
1.1. Nociones básicas de cuerpos finitos	1
2. Introducción a la teoría de códigos	9
2.1. Definición de códigos y códigos lineales	9
2.2. Matriz generadora y matriz de chequeo de paridad	9
2.3. Códigos duales	13
2.4. Peso y distancia de Hamming	18
2.5. Equivalencia de códigos	28
2.5.1. Códigos equivalentes por permutación	28
2.5.2. Códigos monomialmente equivalentes	30
2.6. Construcción de nuevos códigos a partir de otros ya existentes	31
2.6.1. Códigos perforados	31
2.6.2. Extensión de códigos	35
2.7. Codificación y decodificación	38
2.7.1. Codificación	38
2.7.2. Decodificación de máxima verosimilitud	41
3. Cotas en el tamaño de los códigos	45
3.1. El principal problema en la teoría de códigos	45
3.2. $A_q(n, d)$ y $B_q(n, d)$	46
3.3. Cota de Hamming	51
3.4. Cota de Plotkin	53
3.5. Cota de Elias	58
3.6. Cota de Singleton	62
3.7. Cota de Griesmer	64
3.8. Cota de Gilbert	66
3.9. Cota de Varshamov	67

4. Cotas asintóticas	71
4.1. El principal problema asintótico y la función de Manin	71
4.2. Cota asintótica de Singleton	73
4.3. Cota asintótica de Plotkin	74
4.4. La función de entropía de Hilbert	77
4.5. Cota asintótica de Hamming	81
4.6. Cota asintótica de Elias	83
4.7. Cota asintótica de Gilbert-Varshamov	85
4.8. Resultados sobre la función de Manin	87
Bibliografía	95

AGRADECIMIENTOS

Quiero manifestar mis más sinceros agradecimientos:

A mis padres Elda Lucy y Adolfo que con su inmenso amor y entrega hicieron que esto fuera posible al educarme en valores e inculcarme la importancia del estudio.

A mi hermano Alexánder, mi adoración, por escucharme y ayudarme con varias de las pruebas aquí presentadas. Espero que este trabajo lo motive a seguir estudiando y a trazarse grandes metas.

Al profesor Horacio por aceptarme como su estudiante sin conocerme, por la confianza y la disposición que tuvo para orientar, supervisar y leer este trabajo y, sobre todo, por impulsarme a dar lo mejor de mí.

A Andrés por creer en mí y sentir este proyecto como suyo, en su amor y apoyo incondicional encontré muchas veces la tranquilidad y la fuerza que me hacía falta para seguir adelante.

A mis compañeros, en especial a Daniel, Kevin y Giankarlo, por el cariño brindado y los gratos momentos vividos a lo largo de estos años. Su amistad fue fundamental en mi formación personal.

INTRODUCCIÓN

Lograr que el intercambio de datos desde y hacia el espacio sea confiable es uno de los desafíos a los que se enfrentan agencias espaciales como la NASA, ya que la radiación de algunas misiones espaciales, del sol y otros cuerpos celestes pueden interferir en la comunicación entre los centros de operaciones en la Tierra y astronautas o vehículos robotizados en el espacio, al distorsionar la información que se transmite. Por ello, a fin de que el intercambio de datos sea lo más preciso posible, las agencias espaciales utilizan métodos de detección y corrección de errores, en otras palabras, trabajan con teoría de códigos.

La teoría de códigos es un área de estudio de las matemáticas que se encarga de detectar y corregir los errores producidos al transmitir mensajes a través de ciertos canales de comunicación con ruido. Dicha teoría se emplea en el intercambio de información a través de dispositivos electrónicos y en el almacenamiento de datos en medios magnéticos; en este último caso el medio de almacenamiento hace las veces de canal de comunicación y el ruido puede deberse, por ejemplo, a imperfecciones en el equipo.

La *Figura 1* muestra el proceso que tiene lugar cuando se transmite un mensaje a través de un dispositivo electrónico o magnético. Este proceso se estudiará con detalle más adelante, por ahora ilustraremos cómo funciona mediante un ejemplo. Supongamos que en la fuente hay dos mensajes: SI y NO, y que el codificador establece la siguiente relación: SI=1 y NO=0. Así las cosas, si desde la fuente se envía el mensaje SI, el codificador transmite el vector 1 a través del canal de comunicación; el ruido en el canal puede alterar la información, en tal caso el decodificador recibiría el vector 0 y, por lo tanto, el mensaje que llegaría al receptor es NO. En este ejemplo, el código es {0, 1}, los vectores 0 y 1 se conocen como *palabras código* o simplemente palabras.

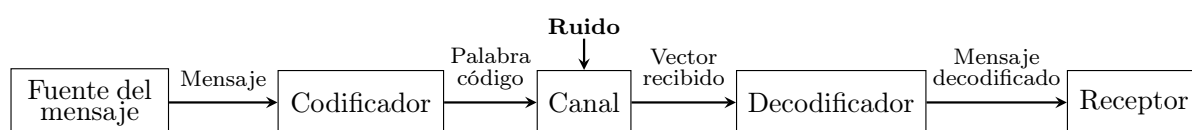


Figura 1: El esquema de comunicación digital.

Una alternativa para detectar y corregir este error es la retransmisión. En tal proceso la fuente enviaría varias veces el mensaje SI y el receptor aceptaría como mensaje original el que haya recibido un mayor número de veces. Sin embargo, este método resulta poco eficiente, ya que puede ser demorado e implica la inversión de muchos recursos. La solución usual consiste en enviar a través del canal más información de la que realmente se requiere. Por ejemplo, en lugar de usar el código {0, 1}, el codificador podría establecer la relación SI=11111 y NO=00000; en esta ocasión si durante la transmisión del mensaje SI se produce un error, por decir algo, si se recibe 10111, la decodificación establecería que la palabra enviada fue la “más cercana” a 10111, es decir 11111, por lo tanto, el mensaje entregado al receptor sería el mensaje SI. La información que se envía de más se conoce como *redundancia* y se usa para proteger, en la medida de lo posible, los mensajes del ruido.

El objetivo de la teoría de códigos es encontrar códigos que permitan transmitir información de manera confiable y eficiente, esto es, códigos que detecten y corrijan muchos errores y que, además, transmitan de manera rápida una amplia variedad de datos. Ante la necesidad de encontrar códigos con estas características, o *buenos códigos*, surge el *principal problema* de la teoría de códigos, el cual estudiaremos a profundidad más adelante. A grandes rasgos, su solución consiste en proporcionar cotas para lo que conoceremos como *parámetros* del código. La búsqueda de buenos códigos también da origen al *principal problema asintótico* de la teoría de códigos, el cual consiste en “pasar a infinito” algunas consideraciones del problema anterior, en cuya solución juega un papel fundamental la función que estableció Manin en [6]; dado que se desconoce el valor exacto de la función de Manin en algunos puntos de su dominio es vital el estudio de cotas para dicha función.

En esta monografía realizaremos un estudio detallado de la teoría básica de códigos, de las distintas cotas para los parámetros de un código y para la función de Manin.

1

PRELIMINARES

En este capítulo presentaremos los conceptos y resultados básicos de la teoría de cuerpos finitos, tomando como referencia [4].

1.1 NOCIONES BÁSICAS DE CUERPOS FINITOS

Sea n un entero positivo. Diremos que dos enteros a y b son *congruentes módulo n* o que a es *congruente con b módulo n* si n divide a $a - b$ y lo denotaremos por $a \equiv b \pmod{n}$.

Sea

$$R = \{(a, b) : a \equiv b \pmod{n}\} \subseteq \mathbb{Z} \times \mathbb{Z},$$

se puede verificar que R es una relación de equivalencia sobre $\mathbb{Z}$ ¹, en este sentido, decimos que la congruencia módulo n es una relación de equivalencia sobre $\mathbb{Z}$. Ahora bien, toda relación de equivalencia sobre un conjunto induce una partición del mismo, por ende, la congruencia módulo n induce una partición de $\mathbb{Z}$ mediante clases de equivalencia.

Dados n, k enteros con $n > 0$, llamaremos *clase residual de k módulo n* , a

$$[k] := \{x \in \mathbb{Z} : x \equiv k \pmod{n}\}.$$

Note que la clase residual de k módulo n

$$[k] = \{nh + k : h \in \mathbb{Z}\} = \{\dots, -2n + k, -n + k, k, n + k, 2n + k, \dots\},$$

es el conjunto de enteros que difieren de k por un múltiplo de n . Es claro que

$$\mathbb{Z} = \bigcup_{k \in \mathbb{Z}} [k].$$

Veamos cuáles son las clases residuales con las que la congruencia módulo n particiona a $\mathbb{Z}$. Por el algoritmo de la división en $\mathbb{Z}$, dado un entero k existen enteros únicos q, r tales que

$$k = nq + r,$$

¹Suponemos que el lector tiene conocimientos en teoría de anillos y cuerpos, de todas maneras [4] presenta un resumen por si el lector desea consultar algún tema.

con $0 \leq r < n$. En términos de congruencias, esto equivale a que $k \equiv r \pmod{n}$, donde r es solo uno de n enteros posibles, de aquí se sigue que todo entero es congruente módulo n a exactamente uno de los siguientes enteros: $0, 1, \dots, n-1$, es decir, $k \in [r]$ para un único entero r tal que $0 \leq r < n$, luego

$$\mathbb{Z} \subseteq \bigcup_{r=0}^{n-1} [r].$$

Por lo tanto,

$$\mathbb{Z} = \bigcup_{r=0}^{n-1} [r].$$

Al conjunto formado por las n clases residuales módulo n que particionan a $\mathbb{Z}$ lo denotaremos por $\mathbb{Z}/(n)$, esto es

$$\mathbb{Z}/(n) := \{[0], [1], \dots, [n-1]\}.$$

Sobre $\mathbb{Z}/(n)$ se definen una suma y una multiplicación a través de aritmética modular, como sigue

$$\begin{aligned} + : \mathbb{Z}/(n) \times \mathbb{Z}/(n) &\rightarrow \mathbb{Z}/(n) & \cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) &\rightarrow \mathbb{Z}/(n) \\ ([a], [b]) &\mapsto +([a], [b]) := [a+b] & ([a], [b]) &\mapsto \cdot([a], [b]) := [ab], \end{aligned}$$

ambas operaciones están bien definidas, es decir, no dependen de los representantes de clase.

Ejemplo 1.1. Sea $n = 5$. La congruencia módulo 5 particiona a $\mathbb{Z}$ a través de 5 clases residuales:

$$\begin{aligned} [0] &= \{\dots, -10, -5, 0, 5, 10, 15, \dots\} \\ [1] &= \{\dots, -14, -9, -4, 1, 6, 11, \dots\} \\ [2] &= \{\dots, -13, -8, -3, 2, 7, 12, \dots\} \\ [3] &= \{\dots, -12, -7, -2, 3, 8, 13, \dots\} \\ [4] &= \{\dots, -11, -6, -1, 4, 9, 14, \dots\}. \end{aligned}$$

Si $x \in [r]$ con $0 \leq r < 5$ entonces $x = 5h + r$ para algún $h \in \mathbb{Z}$; del algoritmo de la división tenemos que r no es más que el residuo que resulta al dividir x por 5. Por lo tanto, si $0 \leq r < 5$ decimos que $[r]$ es el conjunto de enteros que dejan residuo r cuando se dividen por 5; aquí el porqué del nombre clases residuales. En $\mathbb{Z}/(5)$

$$[2] + [4] = [7 + 9] = [16] = [1],$$

puesto que $16 \equiv 1 \pmod{5}$. ■

Observación 1.2. De teoría de anillos sabemos que $(\mathbb{Z}/(n), +, \cdot)$ tiene estructura de anillo y que coincide con el anillo cociente de $\mathbb{Z}$ módulo el ideal principal (n) .

A $(\mathbb{Z}/(n), +, \cdot)$ lo llamaremos el *anillo de enteros módulo n* .

Proposición 1.3. El anillo de enteros módulo n es un cuerpo si y solo si n es un entero primo.

Demostración. Si $(\mathbb{Z}/(n), +, \cdot)$ es un cuerpo, entonces es un dominio entero. Luego, (n) es un ideal primo de $\mathbb{Z}$, es decir, n o es 0 o es un entero primo, como n es un entero positivo concluimos que n es un entero primo.

Si n es un entero primo, entonces (n) es un ideal primo de $\mathbb{Z}$, así el anillo de clases residuales de $\mathbb{Z}$ módulo el ideal principal (n) es un dominio entero, por lo tanto $(\mathbb{Z}/(n), +, \cdot)$ es un cuerpo puesto que todo dominio entero finito es un cuerpo. □

Sea $\mathbb{Z}_n := \{0, 1, \dots, n-1\} \subseteq \mathbb{Z}$. Consideremos

$$\begin{aligned} \psi : \mathbb{Z}/(n) &\rightarrow \mathbb{Z}_n \\ [r] &\mapsto r, \end{aligned} \tag{1.1}$$

con $r = 0, 1, \dots, n-1$, la unicidad del residuo en el algoritmo de la división garantiza que ψ es una función. Veamos que ψ es una biyección, basta con verificar solo la inyectividad pues $|\mathbb{Z}/(n)| = |\mathbb{Z}_n| = n$, supongamos que $\psi([r_1]) = \psi([r_2])$, así $r_1 = r_2$ con $r_1, r_2 \in \mathbb{Z}_n$; como todo entero no nulo divide a cero tenemos que $n|r_1 - r_2$, luego $r_1 \equiv r_2 \pmod{n}$, y por lo tanto $[r_1] = [r_2]$.

Mediante ψ podemos dotar a $\mathbb{Z}_n$ de estructura de anillo. En efecto, por ser ψ una función biyectiva se cumple que para cada par ordenado $(r_1, r_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$ existe un único par ordenado $([r_1], [r_2])$ en $\mathbb{Z}/(n) \times \mathbb{Z}/(n)$ tal que $\psi([r_1]) = r_1$ y $\psi([r_2]) = r_2$; por ende, podemos considerar una suma y una multiplicación sobre $\mathbb{Z}_n$ a partir de la suma y la multiplicación sobre $\mathbb{Z}/(n)$, de la siguiente manera

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n & \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n \\ (r_1, r_2) &\mapsto +(r_1, r_2) := \psi([r_1] + [r_2]) & (r_1, r_2) &\mapsto \cdot(r_1, r_2) := \psi([r_1][r_2]), \end{aligned}$$

se puede verificar que $\mathbb{Z}_n$ junto a estas operaciones binarias hereda la estructura de $(\mathbb{Z}/(n), +, \cdot)$. Por lo tanto, decimos que $\mathbb{Z}_n$ tiene estructura de anillo inducida por ψ , quién por su parte pasa a ser un isomorfismo de anillos.

Proposición 1.4. $\mathbb{Z}_n$ es un cuerpo si y solo si n es un entero primo.

Demostración. Es consecuencia de la Proposición 1.3 y de que los anillos $\mathbb{Z}_n$ y $\mathbb{Z}/(n)$ sean isomorfos. $\square$

Dado un entero primo p , llamaremos a $\mathbb{F}_p := \mathbb{Z}_p$ el *cuerpo de Galois de orden p* .

Así las cosas, $\mathbb{F}_p$ constituye nuestro primer ejemplo de un cuerpo finito. Ahora bien, existen cuerpos finitos cuyo cardinal no es un primo, tal y como muestra el Ejemplo 1.6.

Proposición 1.5. Sea $f \in \mathbb{F}_p[x]$. El anillo cociente $\mathbb{F}_p[x]/(f)$ es un cuerpo si y solo si f es irreducible sobre $\mathbb{F}_p$.

Demostración. $\mathbb{F}_p[x]$ con la norma el grado es un dominio euclídeo puesto que $\mathbb{F}_p$ es un cuerpo, esto implica que $\mathbb{F}_p[x]$ es un DIP y por ende los conceptos de ideal primo y maximal en $\mathbb{F}_p[x]$, coinciden, al igual que los conceptos de polinomio primo e irreducible. Así, el anillo cociente $\mathbb{F}_p[x]/(f)$ es un cuerpo si y solo si (f) es un ideal primo de $\mathbb{F}_p[x]$; por su parte, (f) es un ideal primo de $\mathbb{F}_p[x]$ si y solo si f es irreducible sobre $\mathbb{F}_p$. Por lo tanto, $\mathbb{F}_p[x]/(f)$ es un cuerpo si y solo si f es irreducible sobre $\mathbb{F}_p$. $\square$

Ejemplo 1.6. Sea $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Como $f(0) = 1$ y $f(1) = 1$, tenemos que f no tiene raíces en $\mathbb{F}_2$, así f es irreducible en $\mathbb{F}_2[x]$ ya que además $\mathbb{F}_2$ es un cuerpo. Luego, por la Proposición 1.5, $\mathbb{F}_2[x]/(x^2 + x + 1)$ con las operaciones definidas sobre un anillo cociente es un cuerpo.

$$\mathbb{F}_2[x]/(x^2 + x + 1) = \{g + (f) : g \in \mathbb{F}_2[x]\}.$$

Sea $g \in \mathbb{F}_2[x]$. Por el algoritmo de la división en $\mathbb{F}_2[x]$ existen polinomios q y r en $\mathbb{F}_2[x]$ tales que

$$g = fq + r,$$

con $\partial r < 2$ o $r = 0$, donde ∂f denota el grado del polinomio f . Más aún, por tratarse del anillo de polinomios sobre un cuerpo tenemos que q y r son únicos, Luego, por la absorción del ideal (f)

$$g + (f) = fq + r + (f) = r + (f),$$

con $\partial r < 2$ o $r = 0$, de aquí que

$$\{g + (f) : g \in \mathbb{F}_2[x]\} \subseteq \{0 + (f), 1 + (f), x + (f), 1 + x + (f)\}.$$

Por lo tanto,

$$\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1) = \{0 + (f), 1 + (f), x + (f), 1 + x + (f)\}.$$

Es claro que $\mathbb{F}_4$ no es isomorfo a $\mathbb{Z}_4$. Sean $\omega := x + (f)$ y $\bar{\omega} := x + 1 + (f)$, si además $0 := 0 + (f)$ y $1 := 1 + (f)$, entonces las operaciones en el cuerpo cociente $\mathbb{F}_4$ se pueden resumir de la siguiente manera

+	0	1	ω	$\bar{\omega}$		*	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$		0	0	0	0	
1	1	0	$\bar{\omega}$	ω		1	0	1	ω	$\bar{\omega}$
ω	ω	$\bar{\omega}$	0	1		ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0		$\bar{\omega}$	0	$\bar{\omega}$	1	ω

■

Observación 1.7. El cuerpo finito $\mathbb{F}_4$ se construyó al partir $\mathbb{F}_2[x]$ por un polinomio de segundo grado irreducible sobre $\mathbb{F}_2$, a saber $x^2 + x + 1$. En general, si f es un polinomio de grado n irreducible sobre $\mathbb{F}_p$, con p primo, entonces $\mathbb{F}[x]/(f)$ es un cuerpo con p^n elementos. Esto se sigue de la *Proposición 1.5* y del algoritmo de la división en $\mathbb{F}_p[x]$, tal y como se hizo en el ejemplo anterior, para $p = 2$ y $f = x^2 + x + 1$.

Para $a \in \mathbb{F}_p$ definimos

$$pa := \overbrace{a + \cdots + a}^{p\text{-veces}} \in \mathbb{F}_p.$$

Sea ψ el isomorfismo de $\mathbb{Z}/(p)$ a $\mathbb{F}_p$ dado por (1.1), entonces existe una única clase $[pa]$ en $\mathbb{Z}/(p)$ tal que $\psi([pa]) = pa$, claramente $pa \equiv 0 \pmod{p}$, por consiguiente $[pa] = [0]$ y esto implica que $pa = 0$. Es más, p es el menor entero positivo para el cual esto ocurre. En efecto, si existiera $0 < q < p$ tal que $qa = 0$ tendríamos que $qa \equiv 0 \pmod{p}$, luego, del Lema de Euclides, p divide a a o a q pero en cualquier caso llegamos a una contradicción puesto que a y q son enteros positivos menores a p . Esta propiedad es lo que conocemos como característica de un cuerpo.

La *característica* de un cuerpo F es el menor entero positivo n tal que

$$na := \underbrace{a + \cdots + a}_{n\text{-veces}} = 0_F,$$

para todo $a \in F$; en caso de que dicho entero no exista, decimos que F tiene característica 0.

Teorema 1.8. Todo cuerpo finito tiene característica prima.

Demostración. Sea F un cuerpo finito. En primer lugar, veamos que existe un entero positivo h tal que $ha = 0_F$ para todo $a \in F$. Definamos la función $\phi : \mathbb{Z}^+ \rightarrow F$ por $\phi(k) = k1_F$ para todo entero positivo k , si ϕ fuese una función inyectiva tendríamos que $\phi : \mathbb{Z}^+ \rightarrow \text{Im}(\phi)$ es una biyección y por ende $|\mathbb{Z}^+| = |\text{Im}(\phi)| \leq |F|$, lo que contradice la finitud de F , por lo tanto existen $l, m \in \mathbb{Z}^+$, digamos $l > m$, tales que $l1_F = \phi(l) = \phi(m) = m1_F$, luego

$$0_F = l1_F - m1_F = \underbrace{1_F + \cdots + 1_F}_{l\text{-veces}} - \underbrace{(1_F + \cdots + 1_F)}_{m\text{-veces}} = \underbrace{1_F + \cdots + 1_F}_{(l-m)\text{-veces}} = (l-m)1_F.$$

Sea $h = l - m \in \mathbb{Z}^+$, entonces para cada $a \in F$ se cumple que

$$ha = (l-m)a = \underbrace{a + \cdots + a}_{(l-m)\text{-veces}} = a \underbrace{(1_F + \cdots + 1_F)}_{(l-m)\text{-veces}} = a0_F = 0_F.$$

Por ende, F tiene característica positiva n con $n \leq h$ y como $1 \neq 0$ tenemos que $n \geq 2$. Resta verificar que n es un entero primo, supongamos lo contrario, así $n = st$ con $1 < s, t < n$, luego

$$0_F = n1_F = (st)1_F = \underbrace{1_F + \cdots + 1_F}_{st\text{-veces}} = \underbrace{(1_F + \cdots + 1_F)}_{s\text{-veces}} \underbrace{(1 + \cdots + 1)}_{t\text{-veces}} = (s1_F)(t1_F),$$

de aquí que $s1_F = 0_F$ o $t1_F = 0_F$ lo que contradice la minimalidad de n , por lo tanto F tiene característica prima. $\square$

Corolario 1.9. Sea F un cuerpo finito con característica p . Entonces

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{y} \quad (a - b)^{p^n} = a^{p^n} - b^{p^n},$$

donde $a, b \in F$ y n es un entero positivo.

Demostración. Dado que el Teorema del binomio es válido para cualquier anillo conmutativo, tenemos que

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k},$$

donde $\binom{p}{k}$ es un entero positivo. Si $0 < k < p$ entonces $p - k < p$ y claramente p no divide a $p - k$. Ahora,

$$p \binom{p-1}{k} = \frac{p(p-1)!}{k!(p-1-k)!} = \frac{p!(p-k)}{k!(p-1-k)!(p-k)} = (p-k) \frac{p!}{k!(p-k)!} = (p-k) \binom{p}{k},$$

por lo tanto, p divide $\binom{p}{k}$. Así, para todo $0 < k < p$

$$\binom{p}{k} = s_k p,$$

con s_k un entero positivo, dado que p es la característica de F y $\binom{p}{0} = \binom{p}{p} = 1$ se sigue que

$$(a + b)^p = a^p + b^p + p \sum_{k=1}^{p-1} s_k a^k b^{p-k} = a^p + b^p.$$

Mediante inducción sobre n se puede verificar que $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. La segunda parte se prueba análogamente. $\square$

Corolario 1.10. Sea F es un cuerpo finito. Entonces F contiene un subcuerpo isomorfo a $\mathbb{F}_p$, donde p es la característica de F .

Demostración. Sea $\psi : \mathbb{Z} \rightarrow F$ la función dada por

$$\psi(z) = \begin{cases} \phi(z) & \text{si } z \in \mathbb{Z}^+ \\ 0_F & \text{si } z = 0 \\ -\phi(-z) & \text{si } -z \in \mathbb{Z}^+ \end{cases}$$

donde ϕ es la función de $\mathbb{Z}^+$ a F definida en el Teorema 1.8, se puede verificar que ψ es un homomorfismo de anillos. Si p es la característica de F y $z \in \mathbb{Z}$ entonces

$$\psi(zp) = \psi(z)\psi(p) = \psi(z)0_F = 0_F,$$

así $(p) \subseteq \text{Nu}(\psi)$, donde $\text{Nu}(\psi)$ denota al espacio nulo de ψ . Por otra parte sea $0 \neq b \in \text{Nu}(\psi)$, por la propiedad arquimediana de los números reales, existe $h \in \mathbb{Z}^+$ tal que $ph > |b|$, luego

$$\{h \in \mathbb{Z}^+ : ph > |b|\} \neq \emptyset,$$

así, el principio del buen orden garantiza que este conjunto tiene elemento mínimo, digamos k , como p es la característica de F se cumple que $|b| \geq p$ así que $k \geq 2$ y, por lo tanto, $p(k-1) \leq |b|$; si $p(k-1) < |b|$ tendríamos que

$$p(k-1) < |b| < pk,$$

o de manera equivalente

$$0 < |b| - p(k-1) < p,$$

pero esto sumado al hecho de que

$$\psi(|b| - p(k-1)) = \psi(|b|) + \psi(p)\psi(1-k) = \psi(|b|) = 0_F,$$

contradice la minimalidad de p , por ende $|b| = p(k-1)$, es decir, b es un múltiplo de p . Así las cosas,

$$\text{Nu}(\psi) = (p).$$

Por lo tanto, por el primer Teorema de isomorfía para anillos, el anillo cociente $\mathbb{Z}/(p)$ es isomorfo a $\text{Im}(\psi) \subseteq F$, siendo $\text{Im}(\psi)$ la imagen de ψ , como p es un entero primo concluimos que $\text{Im}(\psi)$ es un subcuerpo de F isomorfo a $\mathbb{F}_p$. $\square$

Sea F un cuerpo con característica p llamaremos *subcuerpo primo* de F al subcuerpo de F isomorfo a $\mathbb{F}_p$.

Observación 1.11. Dado un cuerpo F con característica p , el *Corolario 1.10* garantiza la existencia del subcuerpo primo de F , la unicidad se tiene por la siguiente observación.

Observación 1.12. Existen diferentes maneras de definir el subcuerpo primo de un cuerpo finito F (en general, de un cuerpo), todas ellas equivalentes. Por ejemplo, si

$$\mathcal{K} = \{K \subseteq F : K \text{ es un subcuerpo de } F\},$$

entonces

$$\text{Im}(\psi) = \bigcap_{K \in \mathcal{K}} K,$$

siendo ψ el homomorfismo de anillos de $\mathbb{Z}$ a F definido en el *Corolario 1.10*. En efecto, sea $a \in \text{Im}(\psi)$ y $K \in \mathcal{K}$; por ser K un subcuerpo de F tenemos que $0_F, 1_F \in K$ y dado que K es cerrado bajo la suma y la diferencia concluimos que $a \in K$. Por lo tanto,

$$\text{Im}(\psi) \subseteq \bigcap_{K \in \mathcal{K}} K.$$

La otra inclusión es inmediata. Por esto decimos que el subcuerpo primo de F es el subcuerpo más pequeño de F , en el sentido de que no contiene subcuerpos propios.

Por el *Corolario 1.10*, un cuerpo finito F puede verse como una extensión del cuerpo de Galois de orden p , siendo p la característica de F . Este resultado es muy importante en la caracterización de cuerpos finitos ya que, entre otras cosas, nos brinda una condición necesaria acerca del número de elementos de F .

Teorema 1.13. Sea F un cuerpo finito. Entonces F tiene p^m elementos, donde p es la característica de F y m es el grado de la extensión de F sobre su subcuerpo primo.

Demostración. Sea K el subcuerpo primo de F , al ser F/K una extensión de cuerpos se sigue que F es un espacio vectorial sobre K . Sea $\beta = \{v_1, \dots, v_m\} \subseteq F$ una base de F/K , entonces

$$\alpha_1 v_1 + \dots + \alpha_m v_m \in F,$$

para cualquier elección de escalares $\alpha_1, \dots, \alpha_m$ en K . Puesto que p es la característica de F el número de elementos de K es p , luego, por el principio de la multiplicación, existen p^m posibles elecciones de m elementos de K , no necesariamente distintos, y por ende hay a lo más p^m combinaciones lineales distintas. La unicidad en la representación de un vector en una base nos permite concluir que las p^m combinaciones lineales son distintas, por lo tanto F tiene p^m elementos. $\square$

Ahora bien, dado un primo p y un entero positivo n , ¿siempre es posible encontrar un cuerpo con p^n elementos? Para responder esta pregunta usaremos la noción de cuerpo de descomposición de un polinomio sobre un cuerpo dado.

Sea F un cuerpo y sea $f \in F[x]$ de grado positivo. Diremos que f se *descompone* en L si L es un cuerpo que contiene una copia de F y f puede ser escrito como producto de factores lineales en $L[x]$; esto es, si existen elementos $\alpha_1, \dots, \alpha_m \in L$ tales que

$$f(x) = a \prod_{i=1}^m (x - \alpha_i),$$

donde a es el coeficiente principal de f . El cuerpo L es un *cuerpo de descomposición* de f sobre F si f se descompone en L y $L = K(\alpha_1, \dots, \alpha_m)$, siendo K el subcuerpo de L isomorfo a F .

Observación 1.14. De la teoría de anillos sabemos que dados un cuerpo F y un polinomio $f \in F[x]$ de grado positivo, existe un cuerpo de descomposición de f sobre F y que este es único salvo isomorfismos.

Si L es un cuerpo de descomposición de f sobre F , con $f \in F[x]$ un polinomio de grado positivo y F un cuerpo, diremos que L es el *cuerpo de descomposición* de f sobre F y lo denotaremos por $\text{CDD}_F(f)$.

Teorema 1.15. (Existencia de Cuerpos Finitos) Para cada primo p y cada entero positivo n existe un cuerpo finito con p^n elementos.

Demostración. Consideremos el polinomio $x^q - x$ en $\mathbb{F}_p[x]$ con $q = p^n$. Sean $F = \text{CDD}_{\mathbb{F}_p}(x^q - x)$ y $S = \{a \in F : a^q = a\} \subseteq F$. S es un subcuerpo de F . En efecto,

i) $0_F, 1_F \in S$.

ii) Sean $a, b \in S$. Entonces, por el Corolario 1.9 $(a - b)^q = a^q - b^q = a - b$, así $a - b \in S$.

iii) Sean $a, b \in S$ y $b \neq 0$. Entonces

$$(ab^{-1})^q = a^q(b^{-1})^q = a^q(b^q)^{-1} = ab^{-1},$$

por lo tanto, $ab^{-1} \in S$.

El polinomio $qx^{q-1} - 1$ no tiene raíces en $\mathbb{F}_p$ pues al ser p la característica de $\mathbb{F}_p$ y q una potencia de p se cumple que $qa^{q-1} - 1 = -1$ para todo $a \in \mathbb{F}_p$, por consiguiente el polinomio $x^q - x$ y su derivada $qx^{q-1} - 1$ no tienen raíces en común en $\mathbb{F}_p$. Por lo tanto, $x^q - x$ no tiene raíces múltiples en F , así $|S| = q$.

Sea K el subcuerpo de F isomorfo a $\mathbb{F}_p$. Si K/S entonces K tendría las q raíces de $x^q - x$, pero K solo tiene p elementos, por lo tanto $K \subseteq S \subseteq F$. Así, S tiene todas las raíces de $x^q - x$ y contiene una copia isomorfa a $\mathbb{F}_p$, esto implica que $F \subseteq S$, y por ende $S = F$. Por lo tanto, F es un cuerpo finito con q elementos. $\square$

Lema 1.16. Sean F un cuerpo finito con q elementos y K el subcuerpo primo de F . Entonces el polinomio $x^q - x \in K[x]$ se descompone en F como

$$x^q - x = \prod_{a \in F} (x - a),$$

y F es el cuerpo de descomposición de $x^q - x$ sobre K .

Demostración. Como F es un cuerpo, el grupo multiplicativo F^* formado por las unidades de F es $F \setminus \{0\}$, así $|F^*| = q - 1$ y, por el Teorema de Lagrange, si $u \in F^*$ entonces el orden de u divide a $q - 1$, lo cual implica que $u^{q-1} = 1_F$, por ende $a^q = a$ para todo $a \in F$. En otras palabras, todo elemento de F es raíz del polinomio $x^q - x \in K[x]$. Así, y dado que este polinomio tiene a lo más q raíces distintas en F concluimos que él se factoriza por completo como producto de factores lineales en $F[x]$ de la siguiente manera

$$x^q - x = \prod_{a \in F} (x - a),$$

y que $\text{CDD}_K(x^q - x) \subseteq F$. La otra inclusión se tiene porque todo elemento de F es raíz de $x^q - x$. Por lo tanto, $F = \text{CDD}_K(x^q - x)$. $\square$

Teorema 1.17. (Unicidad de los Cuerpos Finitos) Sean n un entero positivo y p un primo. Entonces cualquier cuerpo finito con $q = p^n$ elementos es isomorfo a $\text{CDD}_{\mathbb{F}_p}(x^q - x)$.

Demostración. Sea F un cuerpo finito con $q = p^n$ elementos y sea K su subcuerpo primo. En primer lugar, veamos que p es la característica de F . Por el Teorema 1.13, $q = (p')^m$, con $m = [F : K]$ y p' la característica de F , así $pp^{n-1} = (p')^m$ y, por el Lema de Euclides, p divide a p' , como ambos son primos, el único chance es que $p = p'$.

En resumen, K es isomorfo a $\mathbb{F}_p$, luego, por el Lema 1.16, $F = \text{CDD}_K(x^q - x)$. Así las cosas, F es un cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$. Por la unicidad en los cuerpos de descomposición concluimos que F es isomorfo a $\text{CDD}_{\mathbb{F}_p}(x^q - x)$. $\square$

Observación 1.18. Dados un primo p y un entero positivo n , denotaremos por $\mathbb{F}_q$ al cuerpo finito con $q = p^n$ elementos.

2

INTRODUCCIÓN A LA TEORÍA DE CÓDIGOS

En este capítulo presentaremos los conceptos y resultados básicos de la teoría de códigos, nuestra referencia principal será el primer capítulo de [2], para algunos ejemplos y resultados seguiremos [1].

2.1 DEFINICIÓN DE CÓDIGOS Y CÓDIGOS LINEALES

Un conjunto finito A es llamado un *alfabeto*. Un *código* q -ario de longitud n es subconjunto no vacío $\mathcal{C} \subseteq A^n$, donde n es un entero positivo, $A^n = A \times \cdots \times A$ y q es la cardinalidad de A . Un (n, M) código $\mathcal{C}$ sobre A es un código de longitud n y de cardinalidad M . Un *subcódigo* de $\mathcal{C}$ es un subconjunto de $\mathcal{C}$. El alfabeto que se considera a lo largo de este trabajo es el cuerpo finito con q elementos, $\mathbb{F}_q$. En este caso, $\mathbb{F}_q^n$ denota al espacio vectorial formado por las n -uplas sobre $\mathbb{F}_q$. Una n -upla $(a_1, a_2, \dots, a_n)$ de un código $\mathcal{C}$ se denomina *palabra código* o simplemente *palabra* y por simplicidad se denota por $a_1 a_2 \cdots a_n$. Un *código binario* (resp. *ternario*, *cuaternario*) es un código sobre $\mathbb{F}_2$ (resp. $\mathbb{F}_3$, $\mathbb{F}_4$).

Un $[n, k]$ código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$ (o un $[n, k]_q$ código lineal $\mathcal{C}$) es un subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k . En ocasiones, nos referiremos a $\mathcal{C}$ omitiendo el término, lineal. Un *subcódigo* de un código lineal $\mathcal{C}$ es un subconjunto de $\mathcal{C}$ que también es lineal. En otras palabras, un subcódigo de $\mathcal{C}$ es un subespacio de $\mathcal{C}$.

Observación 2.1. Como todo espacio vectorial sobre $\mathbb{F}_q$ de dimensión k es isomorfo a $\mathbb{F}_q^k$, un $[n, k]_q$ código es un (n, q^k) código sobre $\mathbb{F}_q$.

Una ventaja de trabajar con un $[n, k]_q$ código $\mathcal{C}$ se presenta al momento de conocer sus palabras; basta con tener una base de $\mathcal{C}$ para saber qué vectores de $\mathbb{F}_q^n$ son palabras código. De aquí, surge la noción de matriz generadora.

2.2 MATRIZ GENERADORA Y MATRIZ DE CHEQUEO DE PARIDAD

Una *matriz generadora* para un $[n, k]_q$ código $\mathcal{C}$ es una matriz G de $k \times n$ con entradas en $\mathbb{F}_q$ cuyas filas forman una base para $\mathcal{C}$. En general, existen tantas matrices generadoras para un código lineal como bases para él. Una matriz generadora para el código lineal $\mathbb{F}_q^n$ es la matriz identidad de $n \times n$; más aún, todo vector de $\mathbb{F}_q^n$ resulta ser, trivialmente, una palabra código de $\mathbb{F}_q^n$.

Para determinar si un vector $\mathbf{x} \in \mathbb{F}_q^n$ es una palabra de un código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$ simplemente debemos verificar si $\mathbf{x}$ es combinación lineal, o no, de las k filas de una matriz generadora G para $\mathcal{C}$. Otra alternativa para determinar si $\mathbf{x}$ está en $\mathcal{C}$ o no, se tiene como consecuencia de la definición de matriz de chequeo de paridad.

Observación 2.2. Si A es una matriz denotaremos por A^T a su matriz transpuesta.

Se llama *matriz de chequeo de paridad* de un $[n, k]$ código $\mathcal{C}$ sobre $\mathbb{F}_q$ ($k < n$), y se denota por H , a una matriz no nula de $(n - k) \times n$ con entradas en $\mathbb{F}_q$ que satisface

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

Para el código lineal $\mathbb{F}_q^n$ no se define el concepto de matriz de chequeo de paridad.

La siguiente proposición garantiza que cada código lineal tiene por lo menos una matriz de chequeo de paridad.

Proposición 2.3. Para un $[n, k]$ código sobre $\mathbb{F}_q$ dado, existe una matriz H de chequeo de paridad.

Demostración. Sea $\mathcal{B}_{\mathcal{C}} = \{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ una base para $\mathcal{C}$. Como $k < n$, $\mathcal{B}_{\mathcal{C}}$ no es una base para $\mathbb{F}_q^n$; sin embargo, podemos completarlo a una. Sean $\mathbf{v}_{k+1}, \dots, \mathbf{v}_n$ en $\mathbb{F}_q^n$ tales que $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{v}_{k+1}, \dots, \mathbf{v}_n\}$ es una base de $\mathbb{F}_q^n$. Es claro que $\mathcal{B}_W = \{\mathbf{v}_{k+1}, \dots, \mathbf{v}_n\}$ es una base para el subespacio vectorial $W = \text{Gen}\{\mathbf{v}_{k+1}, \dots, \mathbf{v}_n\}$. Como $\mathcal{B} = \mathcal{B}_{\mathcal{C}} \cup \mathcal{B}_W$ se sigue que $\mathbb{F}_q^n = \mathcal{C} \oplus W$, donde $\oplus$ denota la suma directa de $\mathcal{C}$ y W .

Ahora, consideremos la función $\varphi : \mathbb{F}_q^n \rightarrow W$, que a cada $\mathbf{v} = \mathbf{x} + \mathbf{y} \in \mathbb{F}_q^n$ con $\mathbf{x} \in \mathcal{C}$ y $\mathbf{y} \in W$ le asigna su componente en W , es decir, $\mathbf{y}$. La unicidad de $\mathbf{x}$ e $\mathbf{y}$ garantiza que φ es una función. Se puede verificar que φ es una transformación lineal que tiene como espacio nulo a $\mathcal{C}$. Dado que W es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión $n - k$, tenemos que W es isomorfo a $\mathbb{F}_q^{n-k}$; más aún, un isomorfismo entre W y $\mathbb{F}_q^{n-k}$ está dado por la función $\phi : W \rightarrow \mathbb{F}_q^{n-k}$ que a cada elemento de W le asigna su vector de coordenadas con respecto a la base $\mathcal{B}_W$. Así,

$$T = \phi \circ \varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-k},$$

es una transformación lineal y $\text{Nu}(T) = \mathcal{C}$, siendo $\text{Nu}(T)$ el espacio nulo de T . En efecto, si $\mathbf{v} = \mathbf{x} + \mathbf{y} \in \mathcal{C} \oplus W$ está en el espacio nulo de $\phi \circ \varphi$ entonces

$$\mathbf{0} = \phi \circ \varphi(\mathbf{v}) = \phi(\varphi(\mathbf{v})) = \phi(\varphi(\mathbf{x} + \mathbf{y})) = \phi(\mathbf{y}) = [\mathbf{y}]_{\mathcal{B}_W},$$

donde $[\mathbf{y}]_{\mathcal{B}_W}$ denota al vector de coordenadas de $\mathbf{y}$ en la base $\mathcal{B}_W$. De aquí que $\mathbf{y} = \mathbf{0}$ y por ende $\mathbf{v} \in \mathcal{C}$. La otra contención es inmediata.

Sea A_T la matriz de $(n - k) \times n$ asociada a T respecto a las bases $\mathcal{B}$ y $\mathcal{B}_0$, donde $\mathcal{B}_0$ es la base canónica de $\mathbb{F}_q^{n-k}$. Entonces

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n : A_T[\mathbf{x}]_{\mathcal{B}}^T = \mathbf{0}\},$$

Si C es la matriz de cambio de base $\mathcal{B}'_0$ a $\mathcal{B}_0$, siendo $\mathcal{B}'_0$ la base canónica de $\mathbb{F}_q^n$, se sigue que

$$\mathcal{C} = \left\{ \mathbf{x} \in \mathbb{F}_q^n : A_T \left(C[\mathbf{x}]_{\mathcal{B}'_0}^T \right) = \mathbf{0} \right\} = \left\{ \mathbf{x} \in \mathbb{F}_q^n : (A_T C) \mathbf{x}^T = \mathbf{0} \right\}.$$

Así, la matriz $H = A_T C$ de tamaño $(n - k) \times n$ es tal que

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

□

Observación 2.4. Hasta el momento, hemos usado $\text{Nu}(\cdot)$ para denotar el espacio nulo de un homomorfismo (de anillos o de espacios vectoriales). En adelante, también lo usaremos para denotar el espacio nulo de una matriz. Así las cosas, si $\mathcal{C}$ es un código lineal y H es una matriz de chequeo de paridad para $\mathcal{C}$ entonces $\mathcal{C} = \text{Nu}(H)$.

Como la elección de los elementos tomados de $\mathbb{F}_q^n$ para completar una base de $\mathbb{F}_q^n$ a partir de una base dada para $\mathcal{C}$ no es única, tenemos que la matriz H de la *Proposición 2.3* no es única. Por lo tanto, $\mathcal{C}$ tiene varias matrices generadoras y de chequeo de paridad. Es por esto que decimos una matriz generadora de $\mathcal{C}$ (resp. una matriz de chequeo de paridad de $\mathcal{C}$), y no, la matriz generadora de $\mathcal{C}$ (resp. la matriz de chequeo de paridad de $\mathcal{C}$).

Otra característica común entre matrices generadoras y de chequeo de paridad para un código lineal es que, en ambos casos, sus filas forman un conjunto linealmente independiente.

Proposición 2.5. El conjunto formado por las filas de una matriz de chequeo de paridad es linealmente independiente.

Demostración. Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y sea H una matriz de chequeo de paridad para $\mathcal{C}$. Esto es, $\mathcal{C} = \text{Nu}(H)$. Por ende, $\nu(H) = \dim(\mathcal{C}) = k$, donde $\nu(H)$ denota la nulidad de H . Por el Teorema de la dimensión,

$$n = \nu(H) + \rho(H) = k + \rho(H),$$

siendo $\rho(H)$ el rango de H . Como el rango de cualquier matriz es igual a la dimensión de su espacio fila, se sigue H tiene $n - k$ filas linealmente independientes. Al ser $n - k$ la cantidad total de filas de H , concluimos que el conjunto formado por las filas de H es linealmente independiente. $\square$

Corolario 2.6. Sean $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$, G una matriz generadora para $\mathcal{C}$ y H una matriz de chequeo de paridad para $\mathcal{C}$. Entonces, $\rho(G) = k$ y $\rho(H) = n - k$.

Demostración. Es claro que las filas de G forman un conjunto linealmente independiente. El resultado buscado es consecuencia de este hecho y de la *Proposición 2.5*. $\square$

Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y H una matriz de chequeo de paridad para $\mathcal{C}$. Para determinar rápidamente si un vector $\mathbf{y}$ de $\mathbb{F}_q^n$ es una palabra código de $\mathcal{C}$ debemos verificar si $H\mathbf{y}^T = \mathbf{0}$. Ahora bien, este proceso no resulta eficiente si nuestro interés es conocer o enlistar las q^k palabras de $\mathcal{C}$. En este caso, es mejor considerar el hecho de que $\mathcal{C}$ es el espacio nulo de H .

Observación 2.7. En adelante denotaremos por I_n a la matriz identidad de tamaño $n \times n$.

Ejemplo 2.8. (Código de repetición) Sea $n > 1$. El $[n, 1]$ código $\mathcal{C}$ sobre $\mathbb{F}_q$ con matriz de chequeo de paridad

$$H = [-\mathbf{1}^T | I_{n-1}],$$

con $\mathbf{1} \in \mathbb{F}_q^{n-1}$, es llamado el *código de repetición q-ario* de longitud n . Sea $\mathbf{x} = x_1 \cdots x_n \in \text{Nu}(H)$. Así

$$\mathbf{0} = \left[\begin{array}{c|cccc} -1 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & 0 & 0 & \cdots & 1 \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} -x_1 + x_2 \\ -x_1 + x_3 \\ \vdots \\ -x_1 + x_n \end{bmatrix},$$

de aquí que $x_1 = \cdots = x_n$. Por lo tanto,

$$\mathcal{C} = \{ \mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_q^n : x_1 = \cdots = x_n \}.$$

Esto implica que una matriz generadora para $\mathcal{C}$ es

$$G = [1 | 1 \cdots 1].$$

■

Decimos que una matriz generadora para un $[n, k]_q$ código está en *forma estándar* si es de la forma $[I_k | A]$, donde A es una matriz de $k \times (n - k)$ con entradas en $\mathbb{F}_q$.

La matriz G del ejemplo anterior está en forma estándar. ¿Todo código lineal tiene una matriz generadora en forma estándar? La respuesta a esta pregunta la da el *Teorema 2.54*.

La prueba de la *Proposición 2.3* es constructiva, esto es, dado un código lineal $\mathcal{C}$, la prueba no solo permite garantizar la existencia de por lo menos una matriz de chequeo de paridad para $\mathcal{C}$, sino que además da la pauta para construir una. El problema radica en que tal vez habría que hacer varios cálculos primero. El siguiente teorema da una matriz de chequeo de paridad para $\mathcal{C}$, de manera inmediata, siempre que se tenga una matriz generadora para $\mathcal{C}$ en forma estándar.

Teorema 2.9. Sea $G = [I_k | A]$ una matriz generadora de un $[n, k]$ código $\mathcal{C}$. Entonces $H = [-A^T | I_{n-k}]$ es una matriz de chequeo de paridad para $\mathcal{C}$.

Demostración. Por la multiplicación de matrices en bloque se tiene que

$$HG^T = -A^T I_k + I_{n-k} A^T = -A^T + A^T = \mathbf{0}_{(n-k) \times n}.$$

Así, si $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ es la base de $\mathcal{C}$ formada por las filas de la matriz G dada en forma estándar, entonces $H\mathbf{v}_i^T = \mathbf{0}$, para todo $1 \leq i \leq k$. Dado $\mathbf{c} \in \mathcal{C}$ existen escalares únicos $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$, tales que $\mathbf{c} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k$. Luego,

$$H\mathbf{c}^T = H(\alpha_1 \mathbf{v}_1^T + \dots + \alpha_k \mathbf{v}_k^T) = \alpha_1 H\mathbf{v}_1^T + \dots + \alpha_k H\mathbf{v}_k^T = \mathbf{0}.$$

Por ende, $\mathcal{C} \subseteq \text{Nu}(H)$. Como H es una matriz de tamaño $(n - k) \times n$ y $\rho(H)$ es igual a la dimensión del espacio fila de H tenemos que $\rho(H) \leq n - k$. Por otra parte, dado que las últimas $n - k$ columnas de H forman un conjunto linealmente independiente tenemos que $\rho(H) \geq n - k$. Por lo tanto, $\rho(H) = n - k$. Luego, por el Teorema de la dimensión

$$\nu(H) = n - \rho(H) = n - (n - k) = k = \dim(\mathcal{C}).$$

Por lo tanto, $\mathcal{C} = \text{Nu}(H)$ y concluimos que H es una matriz de chequeo de paridad para $\mathcal{C}$. □

Ejemplo 2.10. La matriz

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right]$$

es una matriz generadora en forma estándar para el $[7, 4]$ código binario conocido como el $[7, 4]$ *código Hamming*. Por el *Teorema 2.9*, una matriz de chequeo de paridad para este código es

$$H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right].$$

■

Finalizamos esta sección presentando un resultado que será muy importante al momento de estudiar las cotas asintóticas en el último capítulo.

Proposición 2.11. Sean n un entero positivo y q una potencia prima. Entonces, el conjunto

$$\{\mathcal{C} : \mathcal{C} \text{ es un código lineal sobre } \mathbb{F}_q \text{ de longitud } n\},$$

es finito.

Demostración. Observe que

$$\{\mathcal{C} : \mathcal{C} \text{ es un código lineal sobre } \mathbb{F}_q \text{ de longitud } n\} = \prod_{k=0}^n \{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\}.$$

Luego,

$$\left| \{\mathcal{C} : \mathcal{C} \text{ es un código lineal sobre } \mathbb{F}_q \text{ de longitud } n\} \right| = 1 + \sum_{k=1}^n \left| \{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\} \right|.$$

Resta verificar que para todo $1 \leq k \leq n$ el conjunto $\{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\}$ es finito. Sean $1 \leq k \leq n$ y

$$A = \{M : M \text{ es una matriz de tamaño } k \times n \text{ con entradas en } \mathbb{F}_q\}.$$

Es claro que $|A| = q^{nk}$. Sea $B = \{M \in A : \rho(M) = k\}$, si $M \in B$ entonces existe un único $[n, k]_q$ código generado por las filas de M . Por otra parte, dado un $[n, k]_q$ código $\mathcal{C}$ existe por lo menos una matriz generadora para $\mathcal{C}$. Si G es una matriz generadora para $\mathcal{C}$ entonces, por el Corolario 2.6 $G \in B$, y por lo tanto

$$\begin{aligned} B &\rightarrow \{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\} \\ M &\mapsto \mathcal{C} \text{ es el } [n, k]_q \text{ código generado por las filas de } M. \end{aligned} \quad (2.1)$$

es una función sobreyectiva. Así

$$\left| \{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\} \right| \leq |B|,$$

y por transitividad $\left| \{\mathcal{C} : \mathcal{C} \text{ es un } [n, k]_q \text{ código}\} \right| \leq q^{nk}$, lo que concluye la prueba. $\square$

2.3 CÓDIGOS DUALES

Una matriz generadora G de un $[n, k]$ código $\mathcal{C}$ es una matriz cuyas filas son linealmente independientes y generan el código. Las filas de una matriz de chequeo de paridad H son linealmente independientes; por lo tanto, H es una matriz generadora de algún código, llamado el *código dual u ortogonal* de $\mathcal{C}$ y denotado por $\mathcal{C}^\perp$. Una manera alternativa para definir $\mathcal{C}^\perp$ se obtiene a partir de la siguiente forma bilineal.¹

Sea $\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ la función dada por

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i,$$

para cada $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n$ en $\mathbb{F}_q^n$. Se puede verificar que $\cdot$ es una forma bilineal. Sea

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

El siguiente lema establece que $\mathcal{H} = \{\mathbf{x} \in \mathbb{F}_q^n : G\mathbf{x}^T = \mathbf{0}\}$.

Lema 2.12. Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y G una matriz generadora para $\mathcal{C}$. Entonces, un vector $\mathbf{v}$ de $\mathbb{F}_q^n$ pertenece a $\mathcal{H}$ si y solo si $\mathbf{v}$ es ortogonal a todas las filas de G . Es decir, $\mathbf{v} \in \mathcal{H}$ si y solo si $\mathbf{v}G^T = \mathbf{0}$.

¹Si el lector desea puede consultar la definición de forma bilineal en la página 249 de [3].

Demostración. ($\Rightarrow$) (Inmediato).

($\Leftarrow$) Supongamos que $\mathbf{g}_1, \dots, \mathbf{g}_k$ son las filas de G , entonces $\mathbf{v} \cdot \mathbf{g}_i = 0$ para todo $1 \leq i \leq k$. Si $\mathbf{c} \in \mathcal{C}$, entonces existen escalares únicos $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$, tales que $\mathbf{c} = \alpha_1 \mathbf{g}_1 + \dots + \alpha_k \mathbf{g}_k$. Así,

$$\mathbf{v} \cdot \mathbf{c} = \sum_{i=1}^k \alpha_i (\mathbf{v} \cdot \mathbf{g}_i) = 0.$$

De aquí que, $\mathbf{v}$ es ortogonal a todo elemento de $\mathcal{C}$, y por lo tanto, está en $\mathcal{H}$. $\square$

Proposición 2.13. Sean $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y G una matriz generadora para $\mathcal{C}$. Entonces $\mathcal{H}$ es un $[n, n - k]_q$ código y G es una matriz de chequeo de paridad para $\mathcal{H}$.

Demostración. Por el Lema 2.12, $\mathcal{H} = \text{Nu}(G)$, por ende, $\mathcal{H}$ es lineal y G es una matriz de chequeo de paridad para $\mathcal{H}$. Por el Corolario 2.6, $\dim(\mathcal{H}) = n - \rho(G) = n - k$. $\square$

El siguiente teorema muestra que una matriz de chequeo de paridad para $\mathcal{C}$ es una matriz generadora para $\mathcal{H}$. Lo cual implica que $\mathcal{H} = \mathcal{C}^\perp$.

Proposición 2.14. Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y H una matriz de chequeo de paridad para $\mathcal{C}$. Entonces H es una matriz generadora para $\mathcal{H}$.

Demostración. Sean $\mathbf{h}_1, \dots, \mathbf{h}_{n-k}$ las filas de H . Al ser $\mathcal{H}$ es un espacio vectorial de dimensión $n - k$, es suficiente mostrar que $\{\mathbf{h}_1, \dots, \mathbf{h}_{n-k}\}$ es un subconjunto de $\mathcal{H}$ linealmente independiente. Más aún, por la Proposición 2.5, basta con verificar que $\{\mathbf{h}_1, \dots, \mathbf{h}_{n-k}\} \subseteq \mathcal{H}$. Como $\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n : H\mathbf{x}^T = \mathbf{0}\}$, tenemos que $\mathbf{h}_i \cdot \mathbf{c} = 0$ para todo $\mathbf{c} \in \mathcal{C}$ y para todo $1 \leq i \leq n - k$. $\square$

Corolario 2.15. Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$. Entonces $\mathcal{C}^\perp$ es un $[n, n - k]$ código sobre $\mathbb{F}_q$ y

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

Así las cosas, si G y H son matrices generadora y de chequeo de paridad, respectivamente, para un código lineal $\mathcal{C}$, entonces H y G son matrices generadora y de chequeo de paridad, respectivamente, para $\mathcal{C}^\perp$.

Un código $\mathcal{C}$ es *auto ortogonal* siempre que $\mathcal{C} \subseteq \mathcal{C}^\perp$ y es *auto dual* siempre que $\mathcal{C} = \mathcal{C}^\perp$.

Observación 2.16. $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Ejemplo 2.17. El *tetracódigo* es el $[4, 2]$ código ternario generado por

$$G = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right].$$

Veamos que el tetracódigo es auto dual. Por el Teorema 2.9, una matriz de chequeo de paridad para el tetracódigo es

$$H = \left[\begin{array}{cc|cc} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array} \right].$$

Por lo tanto, H es una matriz generadora para el dual del tetracódigo. Como ambos códigos tienen la misma dimensión, resta verificar que uno sea un subconjunto del otro. Dado que

- $1011 = 1(2210) + 1(2101)$
- $0112 = 1(2210) + 2(2101),$

tenemos que, $\text{Gen}\{1011, 0112\} \subseteq \text{Gen}\{2210, 2101\}$. Esto es, el tetracódigo está contenido en su dual. ■

Proposición 2.18. Un código auto dual tiene longitud par n y dimensión $n/2$.

Demostración. Sea $\mathcal{C}$ un $[n, k]$ código auto dual. Así, $n = \dim(\mathcal{C}) = \dim(\mathcal{C}^\perp) = n - k$. Por lo tanto, $n = 2k$. □

Ejemplo 2.19. El dual del $[7, 4]$ código Hamming (*Ejemplo 2.10*) es el $[7, 3]$ código binario con matriz generadora

$$\left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right].$$

Se puede verificar que cada fila de esta matriz se puede escribir como combinación lineal de las filas de la matriz generadora para $[7, 4]$ el código Hamming dada en el *Ejemplo 2.10*. Por lo tanto, el dual del $[7, 4]$ código Hamming es auto ortogonal. Por la *Proposición 2.18*, no es auto dual. ■

Cuando usamos códigos que tienen como alfabeto a $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ (ver *Ejemplo 1.6*) a menudo es útil considerar otra forma bilineal, llamada *forma bilineal hermitiana*. Para $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n$ en $\mathbb{F}_4^n$ la forma bilineal hermitiana $\langle \cdot, \cdot \rangle$ está dada por

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x} \cdot \bar{\mathbf{y}} := \sum_{i=1}^n x_i * \bar{y}_i,$$

donde $\bar{\cdot} : \mathbb{F}_4 \rightarrow \mathbb{F}_4$ llamada conjugación, es tal que: $\bar{0} = 0, \bar{1} = 1, \bar{\omega} = \omega, \bar{\bar{\omega}} = \omega$. La *Proposición 2.21* permite, entre otras cosas, verificar que $\langle \cdot, \cdot \rangle$ es en efecto una forma bilineal.

Lema 2.20. Para $x, y \in \mathbb{F}_4$, se cumple que $\overline{x + y} = \bar{x} + \bar{y}$ y $\overline{x * y} = \bar{x} * \bar{y}$.

Demostración. Sea $x = \omega$ y $y = \bar{\omega}$. Por las operaciones de $\mathbb{F}_4$ y la definición de conjugación

$$\overline{\omega + \bar{\omega}} = \bar{1} = (1 + \omega) + \omega = \bar{\omega} + \bar{\bar{\omega}}, \quad \text{y} \quad \overline{\omega * \bar{\omega}} = \bar{1} = (1 + \omega) * \omega = \bar{\omega} * \bar{\bar{\omega}}.$$

Los otros casos son análogos. □

Proposición 2.21. Para $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_4^n$ y $\alpha \in \mathbb{F}_4$ se cumple que

- i) $\langle \mathbf{x}, \mathbf{x} \rangle \in \{0, 1\}$.
- ii) $\langle \mathbf{x}, \mathbf{y} + \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle$.
- iii) $\langle \mathbf{x} + \mathbf{y}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{z} \rangle + \langle \mathbf{y}, \mathbf{z} \rangle$.
- iv) $\overline{\langle \mathbf{x}, \mathbf{y} \rangle} = \langle \mathbf{y}, \mathbf{x} \rangle$.
- v) $\langle \alpha \mathbf{x}, \mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$
- vi) $\langle \mathbf{x}, \alpha \mathbf{y} \rangle = \bar{\alpha} \langle \mathbf{x}, \mathbf{y} \rangle$.

Demostración. Sean $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n$ y $\mathbf{z} = z_1 \cdots z_n$ en $\mathbb{F}_4^n$ y $\alpha \in \mathbb{F}_4$

- i) Observe que $0 * \bar{0} = 0, 1 * \bar{1} = 1, \omega * \bar{\omega} = \omega * (\omega + 1) = 1, \bar{\omega} * \bar{\bar{\omega}} = (\omega + 1) * \omega = 1$.
- ii) $\langle \mathbf{x}, \mathbf{y} + \mathbf{z} \rangle = \sum_{i=1}^n x_i * \overline{(y_i + z_i)} = \sum_{i=1}^n x_i * (\bar{y}_i + \bar{z}_i) = \sum_{i=1}^n x_i * \bar{y}_i + \sum_{i=1}^n x_i * \bar{z}_i = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle$.
- iii) Análogo a ii).

$$\text{iv) } \overline{\langle \mathbf{x}, \mathbf{y} \rangle} = \overline{\sum_{i=1}^n x_i * \overline{y_i}} = \sum_{i=1}^n \overline{x_i} * \overline{\overline{y_i}} = \sum_{i=1}^n y_i * \overline{x_i} = \langle \mathbf{y}, \mathbf{x} \rangle, \text{ pues } \overline{\overline{y_i}} = y_i, \text{ para todo } y_i \in \mathbb{F}_4.$$

$$\text{v) } \langle \alpha \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n (\alpha * x_i) * \overline{y_i} = \sum_{i=1}^n \alpha * (x_i * \overline{y_i}) = \alpha * \sum_{i=1}^n (x_i * \overline{y_i}) = \alpha \langle \mathbf{x}, \mathbf{y} \rangle.$$

vi) Análogo a v).

□

Para un código lineal $\mathcal{C} \subseteq \mathbb{F}_4^n$, definimos el *dual Hermitiano* de $\mathcal{C}$ como

$$\mathcal{C}^{\perp_H} = \{ \mathbf{x} \in \mathbb{F}_4^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0, \text{ para todo } \mathbf{c} \in \mathcal{C} \},$$

y definimos el *conjugado* de $\mathcal{C}$ como

$$\overline{\mathcal{C}} = \{ \overline{\mathbf{c}} : \mathbf{c} \in \mathcal{C} \},$$

donde $\overline{\mathbf{c}} = \overline{c_1} \cdots \overline{c_n}$ y $\mathbf{c} = c_1 \cdots c_n$. Por el Lema 2.20, $\overline{\alpha \mathbf{x} + \mathbf{y}} = \overline{\alpha} \overline{\mathbf{x}} + \overline{\mathbf{y}}$ para todo $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ y para todo $\alpha \in \mathbb{F}_4$.

Proposición 2.22. Sea $\mathcal{C}$ un $[n, k]$ código cuaternario. Entonces $\overline{\mathcal{C}}$ es un $[n, k]$ código cuaternario.

Demostración. Como $\overline{\mathbf{0}} = \mathbf{0}$, se tiene que $\mathbf{0} \in \overline{\mathcal{C}}$. Supongamos que $\mathbf{v}_1, \mathbf{v}_2 \in \overline{\mathcal{C}}$ y $\alpha \in \mathbb{F}_4$. Luego, existen $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ tales que $\mathbf{v}_1 = \overline{\mathbf{c}_1}, \mathbf{v}_2 = \overline{\mathbf{c}_2}$. Así

$$\alpha \mathbf{v}_1 + \mathbf{v}_2 = \lambda \overline{\mathbf{c}_1} + \overline{\mathbf{c}_2} = \overline{\lambda \mathbf{c}_1 + \mathbf{c}_2},$$

con $\lambda \mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$. Por lo tanto, $\overline{\mathcal{C}}$ es lineal. Ahora, sea $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ una base para $\overline{\mathcal{C}}$. Veamos que $\{\overline{\mathbf{v}_1}, \dots, \overline{\mathbf{v}_k}\}$ es una base para $\mathcal{C}$. Sean $\alpha_1, \dots, \alpha_k \in \mathbb{F}_4$ tales que $\mathbf{0} = \alpha_1 \overline{\mathbf{v}_1} + \dots + \alpha_k \overline{\mathbf{v}_k}$. Luego

$$\mathbf{0} = \overline{\mathbf{0}} = \overline{\alpha_1 \overline{\mathbf{v}_1} + \dots + \alpha_k \overline{\mathbf{v}_k}} = \overline{\alpha_1} \mathbf{v}_1 + \dots + \overline{\alpha_k} \mathbf{v}_k.$$

Esto implica, por ser $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ linealmente independiente, que $\overline{\alpha_1} = \dots = \overline{\alpha_k} = 0$. Así, $\alpha_i = \overline{\alpha_i} = \overline{0} = 0$, para todo $i = 1, \dots, k$. Por lo que $\{\overline{\mathbf{v}_1}, \dots, \overline{\mathbf{v}_k}\}$ es un conjunto linealmente independiente.

Sea $\mathbf{v} \in \overline{\mathcal{C}}$, entonces existe $\mathbf{c} \in \mathcal{C}$ tal que $\mathbf{v} = \overline{\mathbf{c}}$. Como $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ genera a $\overline{\mathcal{C}}$, existen escalares únicos $\alpha_1, \dots, \alpha_k \in \mathbb{F}_4$ tales que $\mathbf{c} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k$. Luego,

$$\mathbf{v} = \overline{\mathbf{c}} = \overline{\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k} = \overline{\alpha_1} \overline{\mathbf{v}_1} + \dots + \overline{\alpha_k} \overline{\mathbf{v}_k}.$$

De aquí que, $\mathbf{v} \in \text{gen}\{\overline{\mathbf{v}_1}, \dots, \overline{\mathbf{v}_k}\}$, esto es, $\overline{\mathcal{C}} \subseteq \text{gen}\{\overline{\mathbf{v}_1}, \dots, \overline{\mathbf{v}_k}\}$, la otra inclusión es inmediata, por lo tanto, $\overline{\mathcal{C}} = \text{gen}\{\overline{\mathbf{v}_1}, \dots, \overline{\mathbf{v}_k}\}$. □

Proposición 2.23. Sea $\mathcal{C}$ un código cuaternario de longitud n . Entonces $\overline{\mathcal{C}}^{\perp} = \mathcal{C}^{\perp_H}$.

Demostración. Por el Corolario 2.15, $\overline{\mathcal{C}}^{\perp} = \{ \mathbf{x} \in \mathbb{F}_4^n : \mathbf{x} \cdot \overline{\mathbf{c}} = 0, \text{ para todo } \mathbf{c} \in \mathcal{C} \}$. Como $\mathbf{x} \cdot \overline{\mathbf{c}} = \langle \mathbf{x}, \mathbf{c} \rangle$, se sigue que

$$\overline{\mathcal{C}}^{\perp} = \{ \mathbf{x} \in \mathbb{F}_4^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0, \text{ para todo } \mathbf{c} \in \mathcal{C} \} = \mathcal{C}^{\perp_H}.$$

□

Corolario 2.24. Sea $\mathcal{C}$ un $[n, k]$ código cuaternario. Entonces $\mathcal{C}^{\perp_H}$ es un $[n, n - k]$ código cuaternario.

Demostración. Es consecuencia de las Proposiciones 2.22 y 2.23 y el Corolario 2.15. □

Al saber que, dado un código lineal cuaternario $\mathcal{C}$, los conjuntos $\overline{\mathcal{C}}$ y $\mathcal{C}^{\perp_H}$ son códigos lineales, es natural preguntarse, ¿cómo se caracterizan las matrices generadoras y de chequeo de paridad para estos códigos lineales?, y ¿cómo se relacionan con las de $\mathcal{C}$? La *Proposición 2.26* permite responder estas preguntas.

Observación 2.25. Si M es una matriz de $m \times n$ con entradas en $\mathbb{F}_4$, denotaremos por $\overline{M}$ a la matriz de $m \times n$ que resulta al conjugar cada componente de M .

Proposición 2.26. Sea $\mathcal{C}$ un $[n, k]$ código sobre cuaternario y G una matriz generadora para $\mathcal{C}$. Entonces $\overline{G}$ es una matriz generadora para $\overline{\mathcal{C}}$; más aún, si G está en forma estándar, es decir, si es de la forma $[I_k | A]$ entonces

- i) $[I_k | \overline{A}]$ es una matriz generadora para $\overline{\mathcal{C}}$ en forma estándar.
- ii) $\begin{bmatrix} -\overline{A}^T \\ I_{n-k} \end{bmatrix}$ es una matriz de chequeo de paridad para $\overline{\mathcal{C}}$.
- iii) $\begin{bmatrix} -\overline{A}^T \\ I_{n-k} \end{bmatrix}$ es una matriz generadora para $\mathcal{C}^{\perp_H}$.
- iv) $[I_k | \overline{A}]$ es una matriz de chequeo de paridad para $\mathcal{C}^{\perp_H}$.

Demostración. La prueba de la *Proposición 2.22* garantiza que $\overline{G}$ es una matriz generadora para $\overline{\mathcal{C}}$.

- i) Se sigue de que $\overline{I_k} = I_k$.
- ii) Es consecuencia de i) y del *Teorema 2.9*.
- iii) y iv) Son consecuencia de i) y ii), junto a las *Proposiciones 2.13* y *2.14*.

□

Decimos que un código lineal cuaternario $\mathcal{C}$ es *auto ortogonal Hermitiano* si $\mathcal{C} \subseteq \mathcal{C}^{\perp_H}$ y *auto dual Hermitiano* si $\mathcal{C} = \mathcal{C}^{\perp_H}$.

Ejemplo 2.27. El *hexacódigo* $\mathcal{G}_6$ es el $[6, 3]$ código cuaternario generado por

$$G = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{array} \right].$$

$\mathcal{G}_6$ es auto dual Hermitiano. En efecto, por la *Proposición 2.26* iii) una matriz generadora para $\mathcal{G}_6^{\perp_H}$ es

$$G^{\perp_H} = \left[\begin{array}{ccc|ccc} -\overline{1} & -\overline{\omega} & -\overline{\omega} & 1 & 0 & 0 \\ -\overline{\omega} & -\overline{1} & -\overline{\omega} & 0 & 1 & 0 \\ -\overline{\omega} & -\overline{\omega} & -\overline{1} & 0 & 0 & 1 \end{array} \right].$$

Por las operaciones de $\mathbb{F}_4$ y la definición de conjugación,

$$G^{\perp_H} = \left[\begin{array}{ccc|ccc} 1 & \overline{\omega} & \overline{\omega} & 1 & 0 & 0 \\ \overline{\omega} & 1 & \overline{\omega} & 0 & 1 & 0 \\ \overline{\omega} & \overline{\omega} & 1 & 0 & 0 & 1 \end{array} \right].$$

Así, $\{1\overline{\omega}\overline{\omega}100, \overline{\omega}1\overline{\omega}010, \overline{\omega}\overline{\omega}1001\}$ es una base para $\mathcal{G}_6^{\perp_H}$. Como

- $1\overline{\omega}\overline{\omega}100 = 1(1001\omega\omega) + \overline{\omega}(010\omega1\omega) + \overline{\omega}(001\omega\omega1)$
- $\overline{\omega}1\overline{\omega}010 = \overline{\omega}(1001\omega\omega) + 1(010\omega1\omega) + \overline{\omega}(001\omega\omega1)$
- $\overline{\omega}\overline{\omega}1001 = \overline{\omega}(1001\omega\omega) + \overline{\omega}(010\omega1\omega) + 1(001\omega\omega1),$

tenemos que, $\mathcal{G}_6^{\perp_H} \subseteq \mathcal{G}_6$. Por *Corolario 2.24*, $\dim(\mathcal{G}_6^{\perp_H}) = \dim(\mathcal{G}_6) = 3$. Por lo tanto, $\mathcal{G}_6^{\perp_H} = \mathcal{G}_6$. ■

2.4 PESO Y DISTANCIA DE HAMMING

Ejemplo 2.28. Supongamos que los soldados A y B están situados en el mapa cuadriculado como muestra la *Figura 2.1*, y que solo B conoce la ruta indicada: la ruta que evita territorio enemigo y le permite a A llegar a salvo donde B .

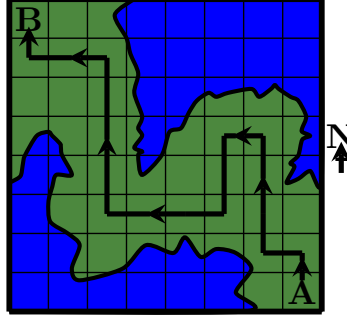


Figura 2.1: Ejemplo mapa coordenado.

B desea enviar la ruta NONNNOSSOOONNNNOON. Para ello piensa usar un código binario. El código binario más rápido, es decir, el de menor longitud, que podría ser usado es

$$\mathcal{C}_1 = \{N = 00, O = 01, E = 10, S = 11\}.$$

$\mathcal{C}_1$ identifica los mensajes N, S, E, O con los cuatro vectores de $\mathbb{F}_2^2$. Si B envía, por ejemplo, 00 y el ruido en el canal hace que A reciba el vector 10 entonces, por ser 10 una palabra código de $\mathcal{C}_1$, A no tiene manera de detectar que ha ocurrido un error durante la transmisión. En este caso, la confiabilidad es más importante que la rapidez. Por lo que B debe considerar otro código para enviar la ruta. Sea $\mathcal{C}_2$ el código binario de longitud 3 que se obtiene al añadir una componente a las palabras de $\mathcal{C}_1$. Esta nueva componente es la suma de las dos anteriores y es llamada la componente de chequeo de paridad.

$$\mathcal{C}_2 = \{N = 000, O = 011, E = 101, S = 110\}.$$

Se puede verificar manualmente, que si se produce solo un error durante la transmisión entonces A no recibe una palabra código de $\mathcal{C}_2$. Así, si por ejemplo, B envía 011 y A recibe 001 , entonces A es capaz de reconocer que ha ocurrido un error. Si A tiene manera de comunicarse con B , debe pedirle que le envíe de nuevo la ruta.

Supongamos que B no puede hacer retransmisión, es decir, que el canal es en un solo sentido. Sea $\mathcal{C}_3$ el código que se obtiene al repetir dos veces el procedimiento usado para construir $\mathcal{C}_2$ a partir de $\mathcal{C}_1$. Esto es,

$$\mathcal{C}_3 = \{c_1 = 00000, c_2 = 01101, c_3 = 10110, c_4 = 11011\}.$$

Si ocurre un solo error durante la transmisión, entonces A es capaz no solo de detectarlo sino también de corregirlo. Por ejemplo, supongamos que B envía 01101 y A recibe $y = 11101 \notin \mathcal{C}_3$. Si A compara el vector recibido y con cada palabra de $\mathcal{C}_3$ se dará cuenta que y difiere de c_1, c_2, c_3 y c_4 en 4, 1, 3, 2 componentes, respectivamente. Al no poder comunicarse con B , A puede asumir que B envió la palabra de $\mathcal{C}_3$ más “cercana”, la que difiere en menos componentes con y , a saber 01101 . ■

Para formalizar la noción de cercanía del ejemplo anterior introduciremos una métrica sobre el espacio vectorial $\mathbb{F}_q^n$, llamada la distancia Hamming. Los *Ejemplos 2.90 y 2.96* muestran que si durante la transmisión ocurre un error entonces $\mathcal{C}_3$ lo detecta y lo corrige.

La *distancia (Hamming)* $d(\mathbf{x}, \mathbf{y})$ entre dos vectores $\mathbf{x} = x_1 \cdots x_n$ y $\mathbf{y} = y_1 \cdots y_n$ en $\mathbb{F}_q^n$ es el número de componentes en las que difieren. Esto es,

$$d(\mathbf{x}, \mathbf{y}) := |\{i : x_i \neq y_i\}| = n - |\{i : x_i = y_i\}|.$$

Por brevedad omitimos $1 \leq i \leq n$ en la definición anterior. El siguiente teorema muestra que, en efecto, la función distancia es una métrica sobre $\mathbb{F}_q^n$.

Teorema 2.29. La función distancia $d(\mathbf{x}, \mathbf{y})$ satisface las siguientes propiedades:

- i) (No negatividad) $d(\mathbf{x}, \mathbf{y}) \geq 0$, para todo $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$.
- ii) $d(\mathbf{x}, \mathbf{y}) = 0$ si y solo si $\mathbf{x} = \mathbf{y}$.
- iii) (Simetría) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$, para todo $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$.
- iv) (Desigualdad triangular) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$, para todo $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$.

Demostración. Los incisos i), ii) y iii) se siguen de la definición de distancia. Sean $\mathbf{x} = x_1 \cdots x_n$, $\mathbf{y} = y_1 \cdots y_n$ y $\mathbf{z} = z_1 \cdots z_n \in \mathbb{F}_q^n$. Consideremos los siguientes conjuntos

$$A = \{i : x_i = y_i\}, \quad B = \{i : x_i = z_i\} \quad \text{y} \quad C = \{i : z_i = y_i\}.$$

Es claro que $B \cap C \subseteq A$. Luego, $|B \cap C| \leq |A|$. Dado que $|B \cap C| = |B| + |C| - |B \cup C|$ y $|B \cup C| \leq n$, concluimos que

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= n - |A| \\ &\leq n - |B| - |C| + |B \cup C| \\ &\leq n - |B| + n - |C| \\ &= d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y}). \end{aligned}$$

□

El *peso (Hamming)* de un vector $\mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_q^n$, denotado por $wt(\mathbf{x})$, es el número de componentes no nulas de $\mathbf{x}$. En otras palabras,

$$wt(\mathbf{x}) := |\{i : x_i \neq 0\}|.$$

Observación 2.30. $wt(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$.

Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código con al menos dos palabras. La *distancia mínima* de $\mathcal{C}$, denotada por $d(\mathcal{C})$, es

$$d(\mathcal{C}) := \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$

El *peso mínimo* de $\mathcal{C}$, denotado por $wt(\mathcal{C})$, es

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

El peso mínimo de un código con una sola palabra (no nula) se define de la misma manera. Si $\mathcal{C} = \{\mathbf{0}\}$ decimos que $d(\mathcal{C}) = wt(\mathcal{C}) = 0$. Veremos más adelante, que la distancia mínima de un código se relaciona con su capacidad para corregir errores. La relación entre distancia y peso está dada por el siguiente teorema.

Teorema 2.31. Si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ entonces $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. Si $\mathcal{C}$ es un código lineal, entonces

$$d(\mathcal{C}) = wt(\mathcal{C}).$$

Demostración. El vector $\mathbf{x} - \mathbf{y}$ tiene componentes no nulas en los lugares donde $\mathbf{x}$ e $\mathbf{y}$ difieren. En efecto,

$$wt(\mathbf{x} - \mathbf{y}) = d(\mathbf{x} - \mathbf{y}, \mathbf{0}) = n - |\{i : x_i - y_i = 0\}| = n - |\{i : x_i = y_i\}| = d(\mathbf{x}, \mathbf{y}).$$

Resta verificar que $d(\mathcal{C}) = wt(\mathcal{C})$. Si $\mathcal{C} = \{\mathbf{0}\}$, no hay nada que probar. Supongamos que $\mathcal{C}$ no es el código lineal trivial de $\mathbb{F}_q^n$. Sean $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ distintos tales que $d(\mathbf{x}, \mathbf{y}) = d(\mathcal{C})$. Luego, $d(\mathcal{C}) = wt(\mathbf{x} - \mathbf{y})$. Como $\mathcal{C}$ es lineal, $\mathbf{x} - \mathbf{y} \in \mathcal{C}$ y por ende $wt(\mathbf{x} - \mathbf{y}) \geq wt(\mathcal{C})$. Por lo tanto, $d(\mathcal{C}) \geq wt(\mathcal{C})$. Por otra parte, sea $\mathbf{z} \in \mathcal{C}$ tal que $wt(\mathcal{C}) = wt(\mathbf{z})$. Como $\mathbf{0} \in \mathcal{C}$ tenemos que $wt(\mathbf{z}) = d(\mathbf{z}, \mathbf{0}) \geq d(\mathcal{C})$. Así, $wt(\mathcal{C}) \geq d(\mathcal{C})$. $\square$

Observación 2.32. En ocasiones, denotaremos la distancia mínima de un código $\mathcal{C}$ por d .

Si $\mathcal{C}$ es un (n, M) código sobre $\mathbb{F}_q$ con distancia mínima d , diremos que $\mathcal{C}$ es un (n, M, d) código sobre $\mathbb{F}_q$. Como resultado del teorema anterior, para códigos lineales la distancia mínima es también llamada el peso mínimo. Si $\mathcal{C}$ es un $[n, k]$ código sobre $\mathbb{F}_q$ con peso mínimo d , diremos que $\mathcal{C}$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$.

Sea $\mathcal{C}$ un código de longitud n con M palabras (dimensión k en el caso lineal) y distancia mínima d , los valores n, M (k en el caso lineal) y d son llamados los *parámetros* de $\mathcal{C}$.

Sean $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathbb{F}_q^n$, denotamos por $\mathbf{x} \cap \mathbf{y}$ al vector $x_1 y_1 \cdots x_n y_n \in \mathbb{F}_q^n$. Cuando se trata de códigos sobre $\mathbb{F}_2, \mathbb{F}_3$ o $\mathbb{F}_4$, hay algunos resultados elementales sobre pesos que resultan ser útiles.

Teorema 2.33.

- i) $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$, para todo $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$.
- ii) $wt(\mathbf{x} \cap \mathbf{y}) \equiv \mathbf{x} \cdot \mathbf{y} \pmod{2}$, para todo $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$.
- iii) $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x} \pmod{2}$, para todo $\mathbf{x} \in \mathbb{F}_2^n$.
- iv) $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x} \pmod{3}$, para todo $\mathbf{x} \in \mathbb{F}_3^n$.
- v) $wt(\mathbf{x}) \equiv \langle \mathbf{x}, \mathbf{x} \rangle \pmod{2}$, para todo $\mathbf{x} \in \mathbb{F}_4^n$.

Demostración.

- i) Sean $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathbb{F}_2^n$

$$A = \{i : x_i = 1, y_i = 0\}, \quad B = \{i : x_i = 0, y_i = 1\} \quad \text{y} \quad C = \{i : x_i = 1, y_i = 1\}.$$

Claramente, estos conjuntos son disjuntos dos a dos. Además, $A \cup C = \{i : x_i \neq 0\}$ y $B \cup C = \{i : y_i \neq 0\}$. De aquí que

$$wt(\mathbf{x}) = |A| + |C| \quad \text{y} \quad wt(\mathbf{y}) = |B| + |C|.$$

Dado que en $\mathbb{F}_2$ cada vector es su propio inverso aditivo, tenemos que $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. Por ende, $wt(\mathbf{x} + \mathbf{y})$ es la cantidad de componentes en las que $\mathbf{x}$ e $\mathbf{y}$ difieren. Así,

$$wt(\mathbf{x} + \mathbf{y}) = |\{i : x_i \neq y_i\}| = |A \cup B| = |A| + |B|.$$

Como además

$$wt(\mathbf{x} \cap \mathbf{y}) = wt(x_1 y_1 \cdots x_n y_n) = |\{i : x_i y_i \neq 0\}| = |C|,$$

concluimos que $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$.

ii) Sean $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathbb{F}_2^n$ y $A = \{i : x_i = y_i = 1\} = \{i : x_i y_i \neq 0\}$. Entonces

$$wt(\mathbf{x} \cap \mathbf{y}) = wt(x_1 y_1 \cdots x_n y_n) = |\{i : x_i y_i \neq 0\}| = |A| \equiv \begin{cases} 0 \pmod{2} & \text{si } |A| \text{ es par} \\ 1 \pmod{2} & \text{en otro caso} \end{cases}.$$

Por otra parte,

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i = \sum_{i \in A} x_i y_i = \sum_{i \in A} 1 = |A|1 = \begin{cases} 0 & \text{si } |A| \text{ es par} \\ 1 & \text{en otro caso} \end{cases}.$$

puesto que $\mathbb{F}_2$ es un cuerpo de característica 2. Por lo tanto, $|A| \equiv |A|1 \pmod{2}$.

iii) Es un caso particular del ítem anterior puesto que $\mathbf{x} \cap \mathbf{x} = \mathbf{x}$, para todo $\mathbf{x} \in \mathbb{F}_2^n$.

iv) Sean $\mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_3^n$ y $A = \{i : x_i \neq 0\}$. Entonces $wt(\mathbf{x}) = |A|$. En $\mathbb{F}_3$, $a^2 = 1$ si y solo si $a \neq 0$, luego

$$\mathbf{x} \cdot \mathbf{x} = \sum_{i=1}^n x_i^2 = \sum_{i \in A} x_i^2 = \sum_{i \in A} 1 = |A|1 \equiv |A| \pmod{3} = wt(\mathbf{x}) \pmod{3},$$

ya que $\mathbb{F}_3$ es un cuerpo de característica 3.

v) Sean $\mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_4^n$ y $A = \{i : x_i \neq 0\}$. Entonces $wt(\mathbf{x}) = |A|$. Por el *Ejemplo 1.6*, $a * \bar{a} = 1$, para todo $a \in \mathbb{F}_4$ con $a \neq 0$, luego por ser 2 la característica de $\mathbb{F}_4$, obtenemos

$$\langle \mathbf{x}, \mathbf{x} \rangle = \sum_{i=1}^n x_i * \bar{x}_i = \sum_{i \in A} x_i * \bar{x}_i = \sum_{i \in A} 1 = |A|1 \equiv |A| \pmod{2} = wt(\mathbf{x}) \pmod{2}.$$

□

Sea A_i , también denotado $A_i(\mathcal{C})$, el número de palabras de peso i en un código $\mathcal{C}$. Esto es,

$$A_i := \{\mathbf{x} \in \mathcal{C} : wt(\mathbf{x}) = i\}.$$

Si la longitud de $\mathcal{C}$ es n , la lista A_i para $1 \leq i \leq n$ es llamada la *distribución de pesos* o el *espectro de pesos* de $\mathcal{C}$.

Ejemplo 2.34. Sea $\mathcal{C}$ un código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$\mathcal{C}$ tiene $2^3 = 8$ palabras código de longitud 6, a saber

$$000000 \quad 110000 \quad 001100 \quad 000011 \quad 111100 \quad 110011 \quad 001111 \quad 111111.$$

La distribución de pesos de $\mathcal{C}$ es $A_0 = 1, A_1 = 0, A_2 = 3, A_3 = 0, A_4 = 3, A_5 = 0, A_6 = 1$. Por lo general, solo los A_i no nulos son listados, por lo que la distribución de pesos de $\mathcal{C}$ es presentada de la siguiente manera:

$$A_0 = A_6 = 1, A_2 = A_4 = 3.$$

■

Teorema 2.35. Sea $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Entonces

- i) $A_0(\mathcal{C}) + A_1(\mathcal{C}) + \cdots + A_n(\mathcal{C}) = q^k$.
- ii) $A_0(\mathcal{C}) = 1$ y $A_1(\mathcal{C}) = A_2(\mathcal{C}) = \cdots = A_{d-1}(\mathcal{C}) = 0$.
- iii) Si $\mathcal{C}$ es un código binario y $\mathbf{1} \in \mathcal{C}$ entonces $A_i(\mathcal{C}) = A_{n-i}(\mathcal{C})$ para $i = 0, \dots, n$.
- iv) Si $\mathcal{C}$ es un código binario auto ortogonal, entonces el peso de cada palabra código es par y $\mathbf{1} \in \mathcal{C}^\perp$.
- v) Si $\mathcal{C}$ es un código ternario auto ortogonal, entonces el peso de cada palabra código es divisible por 3.
- vi) Si $\mathcal{C}$ es un código cuaternario auto ortogonal Hermitiano, entonces el peso de cada palabra código es par.

Demostración.

- i) Note que

$$\mathcal{C} = \bigsqcup_{i=0}^n \{\mathbf{x} \in \mathcal{C} : wt(\mathbf{x}) = i\}.$$

Por lo tanto,

$$q^k = |\mathcal{C}| = \left| \bigsqcup_{i=0}^n \{\mathbf{x} \in \mathcal{C} : wt(\mathbf{x}) = i\} \right| = A_0(\mathcal{C}) + A_1(\mathcal{C}) + \cdots + A_n(\mathcal{C}).$$

- ii) Como $\mathcal{C}$ es lineal, $\mathbf{0} \in \mathcal{C}$. Luego, $A_0(\mathcal{C}) \geq 1$. Si $\mathbf{b} \in \mathcal{C}$ es tal que $wt(\mathbf{b}) = 0$ tenemos que $d(\mathbf{b}, \mathbf{0}) = wt(\mathbf{b} - \mathbf{0}) = wt(\mathbf{b}) = 0$. Esto implica, por ser d una métrica sobre $\mathbb{F}_q^n$, que $\mathbf{b} = \mathbf{0}$. Por lo tanto, $A_0(\mathcal{C}) = 1$. Dado que $\mathcal{C}$ es lineal tenemos que $d = wt(\mathcal{C})$. Por lo tanto, no existe una palabra código no nula con peso menor a d .
- iii) Sean $\mathbf{x} \in \mathcal{C}$ tal que $wt(\mathbf{x}) = i$ y $\mathbf{y} = \mathbf{x} + \mathbf{1}$. Como $\mathbf{1} \in \mathcal{C}$ y el código es lineal, $\mathbf{y} \in \mathcal{C}$. Veamos que $wt(\mathbf{y}) = n - i$. Dado que $\mathbf{x} \cap \mathbf{1} = \mathbf{x}$ entonces, por el Teorema 2.33 i) tenemos

$$\begin{aligned} wt(\mathbf{y}) &= wt(\mathbf{x} + \mathbf{1}) = wt(\mathbf{x}) + wt(\mathbf{1}) - 2wt(\mathbf{x} \cap \mathbf{1}) \\ &= i + n - 2i \\ &= n - i. \end{aligned}$$

Para cada $0 \leq i \leq n$, sean $A = \{\mathbf{x} \in \mathcal{C} : wt(\mathbf{x}) = i\}$ y $B = \{\mathbf{x} \in \mathcal{C} : wt(\mathbf{x}) = n - i\}$ y sea $f_i : A \rightarrow B$ dada por $f_i(\mathbf{x}) = \mathbf{x} + \mathbf{1}$, para todo $\mathbf{x} \in A$. Es claro que f_i es inyectiva. Sea $\mathbf{y} \in B$ entonces $wt(\mathbf{y}) = n - i$. Luego, $wt(\mathbf{y} + \mathbf{1}) = i$. Así, y por ser $\mathcal{C}$ un código binario, $\mathbf{y} = f_i(\mathbf{y} + \mathbf{1})$. De aquí que, f_i es sobreyectiva. Por lo tanto

$$A_i(\mathcal{C}) = |A| = |B| = A_{n-i}(\mathcal{C}).$$

- iv) Sea $\mathbf{x} \in \mathcal{C}$. Como $\mathcal{C}$ es auto ortogonal $\mathbf{x} \cdot \mathbf{c} = 0$ para todo $\mathbf{c} \in \mathcal{C}$. En particular, $\mathbf{x} \cdot \mathbf{x} = 0$. Por el Teorema 2.33 iii) $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x} \pmod{2}$. Por consiguiente, $wt(\mathbf{x})$ es par. Resta mostrar que $\mathbf{1} \in \mathcal{C}^\perp$. Si $\mathbf{x}$ es de la forma $x_1 \cdots x_n$, tenemos que

$$\mathbf{x} \cdot \mathbf{1} = \sum_{i=1}^n x_i = \sum_{i=1}^n x_i^2 = \mathbf{x} \cdot \mathbf{x} = 0.$$

Por lo tanto, $\mathbf{1} \in \mathcal{C}^\perp$.

v) y vi) Los argumentos son análogos a los del ítem anterior.

□

Ejemplo 2.36. Sea $\mathcal{C}$ el tetracódigo. En el *Ejemplo 2.17* vimos $\mathcal{C}$ es un código ternario auto dual, y por ende auto ortogonal. Luego, por el *Teorema 2.35 v)*, el peso de cada palabra de $\mathcal{C}$ es divisible por 3. Como $1011 \in \mathcal{C}$ y $wt(1011) = 3$, tenemos que el tetracódigo es un $[4, 2, 3]$ código ternario. ■

La siguiente proposición muestra que el recíproco de los ítems v) y vi) del *Teorema 2.35* es cierto.

Proposición 2.37. Sea $\mathcal{C}$ un código sobre $\mathbb{F}_q$, con $q = 3$ o 4 .

- i) Cuando $q = 3$, el peso de cada palabra código de $\mathcal{C}$ es divisible por tres si y solo si $\mathcal{C}$ es auto ortogonal.
- ii) Cuando $q = 4$, el peso de cada palabra código de $\mathcal{C}$ es par si y solo si $\mathcal{C}$ es auto ortogonal Hermitiano.

Demostración.

- i) Si $\mathcal{C}$ es auto ortogonal entonces, por el *Teorema 2.35 v)* el peso de cada palabra de $\mathcal{C}$ es divisible por tres. Resta verificar el recíproco. Sean $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathcal{C}$. Debemos mostrar que $\mathbf{x} \cdot \mathbf{y} = 0$. Sean

$$B_1 = \{i : x_i = 0, y_i = 1\} \quad B_2 = \{i : x_i = 0, y_i = 2\} \quad B_3 = \{i : x_i = 1, y_i = 0\} \quad B_4 = \{i : x_i = 1, y_i = 1\} \\ B_5 = \{i : x_i = 1, y_i = 2\} \quad B_6 = \{i : x_i = 2, y_i = 0\} \quad B_7 = \{i : x_i = 2, y_i = 1\} \quad B_8 = \{i : x_i = 2, y_i = 2\}.$$

Estos conjuntos son disjuntos dos a dos. Note que

$$\{i : x_i + y_i \neq 0\} = \bigcup_{i=1}^8 B_i \setminus (B_5 \cup B_7), \quad \{i : x_i - y_i \neq 0\} = \bigcup_{i=1}^8 B_i \setminus (B_4 \cup B_8).$$

Luego,

$$wt(\mathbf{x} + \mathbf{y}) = \sum_{i=1}^8 |B_i| - |B_5| - |B_7|, \quad wt(\mathbf{x} - \mathbf{y}) = \sum_{i=1}^8 |B_i| - |B_4| - |B_8|.$$

Como $\mathcal{C}$ es lineal y el peso de cada palabra código es divisible por 3, tenemos que

$$\sum_{i=1}^8 |B_i| - |B_5| - |B_7| \equiv \sum_{i=1}^8 |B_i| - |B_4| - |B_8| \pmod{3}.$$

De aquí que

$$|B_4| + |B_8| \equiv |B_5| + |B_7| \pmod{3}.$$

Por otra parte, dado que la característica de $\mathbb{F}_3$ es 3, obtenemos

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \sum_{i=1}^n x_i y_i = \sum_{i \in B_4} x_i y_i + \sum_{i \in B_5} x_i y_i + \sum_{i \in B_7} x_i y_i + \sum_{i \in B_8} x_i y_i \\ &= \sum_{i \in B_4} 1 + \sum_{i \in B_5} 2 + \sum_{i \in B_7} 2 + \sum_{i \in B_8} 1 \\ &\equiv |B_4| + |B_8| + 2(|B_5| + |B_7|) \pmod{3}. \end{aligned}$$

Por lo tanto, $\mathbf{x} \cdot \mathbf{y} \equiv 3(|B_5| + |B_7|) \pmod{3} \equiv 0 \pmod{3}$. En otras palabras $\mathbf{x} \cdot \mathbf{y} = 0$.

- ii) Si $\mathcal{C}$ es auto ortogonal Hermitiano entonces, por el *Teorema 2.35 vi)* el peso de cada palabra de $\mathcal{C}$ es divisible por dos. Resta verificar el recíproco.

En primer lugar, dado $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}$, veamos que $\mathbf{x} \in \mathcal{C}^\perp$, es decir que $\langle \mathbf{x}, \mathbf{x} \rangle = 0$. Sea $A = \{i : x_i \neq 0\}$. Entonces $wt(\mathbf{x}) = |A|$. Por ende, $|A|$ es par. Por el *Ejemplo 1.6*, $a * \bar{a} = 1$, para todo $a \in \mathbb{F}_4$ con $a \neq 0$. Luego,

$$\langle \mathbf{x}, \mathbf{x} \rangle = \sum_{i=1}^n x_i * \bar{x}_i = \sum_{i \in A} x_i * \bar{x}_i = \sum_{i \in A} 1 = |A| \cdot 1 \in \mathbb{F}_4.$$

Como $|A|$ es par y la característica de $\mathbb{F}_4$ es 2, se sigue que $\langle \mathbf{x}, \mathbf{x} \rangle = 0$. Ahora, sean $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Como $\mathcal{C}$ es lineal, tenemos que $\mathbf{x} + \mathbf{y}$ y $\omega\mathbf{x} + \mathbf{y}$ están en $\mathcal{C}$. Luego, $\langle \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} \rangle = 0$ y $\langle \omega\mathbf{x} + \mathbf{y}, \omega\mathbf{x} + \mathbf{y} \rangle = 0$. Así, por la *Proposición 2.21*,

$$\begin{aligned} 0 &= \langle \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle, \\ 0 &= \langle \omega\mathbf{x} + \mathbf{y}, \omega\mathbf{x} + \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle + \omega\langle \mathbf{x}, \mathbf{y} \rangle + \bar{\omega}\langle \mathbf{y}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle = \omega\langle \mathbf{x}, \mathbf{y} \rangle + \bar{\omega}\langle \mathbf{y}, \mathbf{x} \rangle. \end{aligned}$$

Por ende,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle \quad \text{y} \quad \omega\langle \mathbf{x}, \mathbf{y} \rangle = \bar{\omega}\langle \mathbf{y}, \mathbf{x} \rangle.$$

Por lo tanto,

$$0 = (\bar{\omega} + \omega)\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle.$$

□

El recíproco del *Teorema 2.35 iv)* en general no es cierto, como muestra el *Ejemplo 2.39*.

Proposición 2.38. Sean $\mathcal{C}$ un código binario y G una matriz generadora para $\mathcal{C}$ tal que el peso de cada una de las filas de G es par. Entonces el peso de cada palabra código es par.

Demostración. La suma de dos palabras de $\mathcal{C}$ con peso par es una palabra código con peso par. En efecto, sean $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ con peso par. Entonces $wt(\mathbf{x}) + wt(\mathbf{y}) \equiv 0 \pmod{2}$. Luego, por el *Teorema 2.33 i)*

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{2}.$$

Sea G una matriz generadora para $\mathcal{C}$ tal que el peso de cada una de sus filas es par. Toda palabra de $\mathcal{C}$ es combinación lineal de las filas de G . Como los escalares son tomados sobre $\mathbb{F}_2$, cada palabra de $\mathcal{C}$ es la suma de determinadas filas de G . Por lo tanto, el peso de cada palabra de $\mathcal{C}$ es par. □

Ejemplo 2.39. Sea $\mathcal{C}$ el $[6, 3]$ código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Dado que cada una de las filas de G tiene peso par tenemos, por el *Teorema 2.38*, que el peso de cada palabra de $\mathcal{C}$ es par. $\mathcal{C}$ no es auto ortogonal. En efecto, mediante operaciones elementales por fila llevamos G a su forma estándar

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right]$$

Luego, una matriz generadora de $\mathcal{C}^\perp$ es

$$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right]$$

De aquí que $\mathbf{1} \in \mathcal{C}^\perp$. Como no existen escalares tales que 011000 se pueda escribir como combinación lineal de las filas de H , tenemos que $\mathcal{C} \not\subseteq \mathcal{C}^\perp$. ■

El ítem iv) del *Teorema 2.35* establece que todas las palabras en un código binario auto ortogonal $\mathcal{C}$ tienen peso par. Si consideramos el subconjunto de $\mathcal{C}$ formado por las palabras de peso divisible por 4, obtendremos un subcódigo de $\mathcal{C}$. Esto es, el subconjunto de palabras código de peso divisible por 4 es un subespacio de $\mathcal{C}$.

Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$ de longitud n y sea $\mathbf{x}$ cualquier vector en $\mathbb{F}_q^n$, entonces el conjunto $\mathbf{x} + \mathcal{C}$ es definido como

$$\mathbf{x} + \mathcal{C} = \{\mathbf{x} + \mathbf{c} : \mathbf{c} \in \mathcal{C}\},$$

y es llamado una clase lateral de $\mathcal{C}$.

Teorema 2.40. Sean $\mathcal{C}$ un $[n, k]$ código binario auto ortogonal y $\mathcal{C}_0$ el conjunto de todas las palabras de $\mathcal{C}$ cuyo peso es divisible por 4. Entonces

- i) $\mathcal{C}_0 = \mathcal{C}$, o
- ii) $\mathcal{C}_0$ es un $[n, k-1]$ subcódigo de $\mathcal{C}$ y $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1$, donde $\mathcal{C}_1 = \mathbf{x} + \mathcal{C}_0$, para cualquier $\mathbf{x} \notin \mathcal{C}_0$. Más aún, $\mathcal{C}_1$ está conformado por todas las palabras de $\mathcal{C}$ cuyo peso no es divisible por 4.

Demostración. Por el *Teorema 2.35* iv) todas las palabras código de $\mathcal{C}$ tienen peso par. Por lo tanto, i) se cumple o existe $\mathbf{x} \in \mathcal{C}$ con peso par y no divisible por 4. Supongamos lo segundo.

Sea $\mathbf{y} \in \mathcal{C}$ con $\mathbf{y} \neq \mathbf{x}$ tal que $wt(\mathbf{y})$ es par pero no múltiplo de 4. La existencia de algún $\mathbf{y}$ con estas características se garantiza por ser $\mathcal{C}$ lineal. Si $wt(\mathbf{x}) = 4k + 2$ y $wt(\mathbf{y}) = 4m + 2$, con k, m enteros no negativos. Entonces

$$wt(\mathbf{x}) + wt(\mathbf{y}) = 4(k + m + 1) \equiv 0 \pmod{4}.$$

Por el *Teorema 2.33* ii) y por ser $\mathcal{C}$ auto ortogonal tenemos que $wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{2}$. Luego, $2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{4}$. Por lo tanto, del *Teorema 2.33* i)

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{4}.$$

De aquí que, $\mathbf{x} + \mathbf{y} \in \mathcal{C}_0$. Así, existe $\mathbf{c}_0 \in \mathcal{C}_0$ tal que $\mathbf{x} + \mathbf{y} = \mathbf{c}_0$. Esto implica, por ser $\mathcal{C}$ binario, que $\mathbf{y} = \mathbf{x} + \mathbf{c}_0$. Por ende, $\mathbf{y} \in \mathcal{C}_1$. Por lo tanto, $\mathcal{C} \subseteq \mathcal{C}_0 \cup \mathcal{C}_1$ y toda palabra de $\mathcal{C}$ cuyo peso no es múltiplo de 4 está en $\mathcal{C}_1$. La otra inclusión es inmediata.

Por otra parte, sea $\mathbf{z} \in \mathcal{C}_1$. Luego, existe $\mathbf{c}'_0 \in \mathcal{C}_0$ tal que $\mathbf{z} = \mathbf{x} + \mathbf{c}'_0$. Si $wt(\mathbf{c}'_0) = 4t$ con t un entero no negativo. Entonces,

$$wt(\mathbf{z}) = wt(\mathbf{x}) + wt(\mathbf{c}'_0) - 2wt(\mathbf{x} \cap \mathbf{c}'_0) = 4(k + t) + 2 - 2wt(\mathbf{x} \cap \mathbf{c}'_0) \equiv 2 \pmod{4}.$$

De aquí que, toda palabra en $\mathcal{C}_1$ tiene peso no divisible por 4. Así las cosas, $\mathcal{C}_1$ está formado por todas las palabras de $\mathcal{C}$ cuyo peso no es divisible por 4. Esto implica, a su vez, que $\mathcal{C} = \mathcal{C}_0 \sqcup \mathcal{C}_1$.

Es fácil verificar que $\mathcal{C}_0$ es lineal. Sea $r = \dim(\mathcal{C}_0)$. Veamos que $r = k - 1$. Sea $f : \mathcal{C}_0 \rightarrow \mathcal{C}_1$ tal que $f(\mathbf{c}_0) = \mathbf{x} + \mathbf{c}_0$, para todo $\mathbf{c}_0 \in \mathcal{C}_0$. Es inmediato que f es una biyección. Por lo tanto,

$$2^k = |\mathcal{C}| = |\mathcal{C}_0| + |\mathcal{C}_1| = 2^r + 2^r = 2^{r+1}.$$

Así, $k = r + 1$. □

En el teorema anterior, la hipótesis de auto ortogonalidad es fundamental para garantizar que el conjunto formado por las palabras código con peso divisible por 4 es un código.

Ejemplo 2.41. Sea $\mathcal{C}$ el código binario no auto ortogonal del *Ejemplo 2.39*. El subconjunto de $\mathcal{C}$ formado por las palabras cuyo peso es divisible por 4 no es un subcódigo de $\mathcal{C}$ puesto no es cerrado para la suma. En efecto, 100111 y 010111 tienen peso 4 pero su suma 110000, no. ■

Si consideramos el subconjunto de un código binario formado por todas las palabras código que tienen peso par, sin exigir auto ortogonalidad, se tiene el siguiente resultado.

Teorema 2.42. Sean $\mathcal{C}$ un $[n, k]$ código binario y $\mathcal{C}_p$ el conjunto de todas las palabras de $\mathcal{C}$ cuyo peso es par. Entonces

- i) $\mathcal{C} = \mathcal{C}_p$, o
- ii) $\mathcal{C}_p$ es un $[n, k-1]$ subcódigo de $\mathcal{C}$ y $\mathcal{C} = \mathcal{C}_p \cup \mathcal{C}_i$, donde $\mathcal{C}_i = \mathbf{x} + \mathcal{C}_p$, para cualquier palabra $\mathbf{x}$ con peso impar. Más aún, $\mathcal{C}_i$ consiste de todas las palabras de $\mathcal{C}$ cuyo peso es impar.

Demostración. La prueba es análoga a la del *Teorema 2.40*. □

En la prueba del *Teorema 2.40* supusimos que i). no se daba y mostramos que debía ocurrir ii). Ahora bien, ¿en realidad puede suceder que todas las palabras de un código binario auto ortogonal tengan peso divisible por 4? si es así, ¿cómo determinar cuándo esto ocurre sin necesidad de conocer el peso de todas las palabras código? La primera parte del siguiente teorema da respuesta a estas preguntas.

Teorema 2.43. Sea $\mathcal{C}$ un código lineal binario.

- i) Si $\mathcal{C}$ es auto ortogonal y tiene una matriz generadora tal que el peso de cada una de sus filas es divisible por 4, entonces el peso de cada palabra de $\mathcal{C}$ es divisible por 4.
- ii) Si el peso de cada palabra de $\mathcal{C}$ es divisible por 4, entonces $\mathcal{C}$ es auto ortogonal.

Demostración.

- i) La suma de dos palabras de $\mathcal{C}$ con peso divisible por 4 es una palabra código con peso divisible por 4. En efecto, sean $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ con peso divisible por 4. Si $wt(\mathbf{x}) = 4k$ y $wt(\mathbf{y}) = 4m$, con k, m enteros no negativos. Entonces

$$wt(\mathbf{x}) + wt(\mathbf{y}) = 4(k + m) \equiv 0 \pmod{4}.$$

Por el *Teorema 2.33 ii)* y por ser $\mathcal{C}$ auto ortogonal tenemos que $wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{2}$. Luego, $2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{4}$. Por lo tanto, del *Teorema 2.33 i)*

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 \pmod{4}.$$

Sea G una matriz generadora para $\mathcal{C}$ tal que el peso de cada una de sus filas es divisible por 4. Toda palabra de $\mathcal{C}$ es combinación lineal de las filas de G . Como los escalares son tomados sobre $\mathbb{F}_2$, cada palabra de $\mathcal{C}$ es la suma de determinadas filas de G . Por lo tanto, el peso de cada palabra de $\mathcal{C}$ es divisible por 4.

- ii) Para verificar que $\mathcal{C}$ es auto ortogonal, debemos mostrar que $\mathbf{x} \cdot \mathbf{y} = 0$, para todo $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Por el *Teorema 2.33 ii)* $\mathbf{x} \cdot \mathbf{y} \equiv wt(\mathbf{x} \cap \mathbf{y}) \pmod{2}$. Así y dado que $\mathcal{C}$ es lineal y que el peso de cada palabra código es divisible por 4, tenemos que

$$\begin{aligned} 2(\mathbf{x} \cdot \mathbf{y}) &\equiv 2wt(\mathbf{x} \cap \mathbf{y}) - wt(\mathbf{x}) - wt(\mathbf{y}) \pmod{4} \\ &\equiv -wt(\mathbf{x} + \mathbf{y}) \pmod{4} \\ &\equiv 0 \pmod{4}. \end{aligned}$$

Por lo tanto, $\mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod{2}$.

□

Ejemplo 2.44. Sea $\mathcal{C}$ el dual del $[7, 4]$ código Hamming. En el *Ejemplo 2.19* vimos que $\mathcal{C}$ es un código binario auto ortogonal y que una matriz generadora $\mathcal{C}$ es

$$\left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right]$$

Como el peso de cada fila es 4, por el *Teorema 2.43 i)* tenemos que el peso de cada palabra de $\mathcal{C}$ es divisible por 4. Esto implica, que $d(\mathcal{C}) = 4$. ■

Diremos que un código lineal binario es un *código par* si el peso de cada una de sus palabras es divisible por 2. El siguiente ejemplo muestra que los códigos pares no son auto ortogonales.

Ejemplo 2.45. Sea $n > 2$ y sea $\mathcal{C}$ el dual del $[n, 1]$ código de repetición binario (*Ejemplo 2.8*). Si $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}$ entonces

$$0 = \mathbf{x} \cdot \mathbf{1} = \sum_{i=1}^n x_i = \mathbf{x} \cdot \mathbf{x}.$$

Por el *Teorema 2.33 iii)* $\mathbf{x} \cdot \mathbf{x} \equiv wt(\mathbf{x}) \pmod{2}$. Por lo tanto, $\mathcal{C}$ es un código par. $\mathcal{C}^\perp$ es el $[n, 1]$ código de repetición binario. Si $\mathcal{C} \subseteq \mathcal{C}^\perp$ entonces $n - 1 = \dim(\mathcal{C}) \leq \dim(\mathcal{C}^\perp) = 1$. Esto no puede ser, por lo tanto, $\mathcal{C}$ no es auto ortogonal. ■

Existe una relación entre una matriz de chequeo de paridad para un código lineal y su distancia mínima.

Teorema 2.46. Un código lineal $\mathcal{C}$ tiene distancia mínima $d > 0$ si y solo si de cualquier matriz de chequeo de paridad para $\mathcal{C}$ se puede extraer un conjunto de d columnas linealmente dependientes y además todo conjunto formado por $d - 1$ columnas es linealmente independiente.

Demostración. Sean $\mathbf{c} = c_1 \cdots c_n \in \mathcal{C}$ una palabra no nula, $A = \{i : c_i \neq 0\}$ y $\mathbf{h}_1, \dots, \mathbf{h}_n$ las columnas de una matriz de chequeo de paridad H para $\mathcal{C}$. Luego,

$$\mathbf{0} = \mathbf{c}H^T = c_1\mathbf{h}_1 + \cdots + c_n\mathbf{h}_n = \sum_{i \in A} c_i\mathbf{h}_i.$$

Por ende, $\{\mathbf{h}_i : i \in A\}$ es linealmente dependiente y $|\{\mathbf{h}_i : i \in A\}| = wt(\mathbf{c})$. Sea $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}$ tal que $wt(\mathbf{x}) = d$ y sea $B = \{i : x_i \neq 0\}$ entonces $\{\mathbf{h}_i : i \in B\}$ es linealmente dependiente y $|\{\mathbf{h}_i : i \in B\}| = d$. Si existiese un conjunto $C \subseteq \{1, \dots, n\}$ con $|C| = d - 1$ tal que $\{\mathbf{h}_i : i \in C\}$ sea linealmente dependiente tendríamos que existen $d - 1$ escalares, no todos cero, tales que

$$\mathbf{0} = \sum_{i \in C} \alpha_i \mathbf{h}_i,$$

de aquí que el vector $\mathbf{y} = y_1 \cdots y_n$ con

$$y_i = \begin{cases} \alpha_i & \text{si } i \in C \\ 0 & \text{en caso contrario} \end{cases}$$

para todo $1 \leq i \leq n$ está en $\mathcal{C}$ y $0 < wt(\mathbf{y}) \leq d - 1$ pero esto contradice que $d(\mathcal{C}) = d$.

Resta verificar el recíproco. Sea $D \subseteq \{1, \dots, n\}$ con $|D| = d$ tal que $\{\mathbf{h}_i : i \in D\}$ es linealmente dependiente. Dado que además todo conjunto formado por $d - 1$ columnas de H es linealmente independiente, tenemos que existen exactamente d escalares no nulos, tales que

$$\mathbf{0} = \sum_{i \in D} \alpha_i \mathbf{h}_i.$$

Entonces, por el mismo argumento anterior, existe $\mathbf{y} \in \mathcal{C}$ tal que $0 < wt(\mathbf{y}) = d$. Así, $d(\mathcal{C}) \leq d$. Supongamos que $d(\mathcal{C}) < d$. Sea $\mathbf{z} \in \mathcal{C}$ tal que $wt(\mathbf{z}) = d(\mathcal{C})$. Entonces existe un conjunto formado por $wt(\mathbf{z})$ columnas de H , linealmente dependiente. Agregando $d - wt(\mathbf{z}) - 1$ columnas de H a este conjunto, obtenemos un conjunto de $d - 1$ columnas de H linealmente dependiente. Esto no puede ser. Por lo tanto, $d(\mathcal{C}) = d$. $\square$

Ejemplo 2.47. El hexacódigo $\mathcal{G}_6$ (Ejemplo 2.27) es un $[6, 3]$ código cuaternario auto dual Hermitiano, y por ende auto ortogonal Hermitiano. Una matriz de chequeo de paridad para $\mathcal{G}_6$ es

$$H = \left[\begin{array}{ccc|ccc} 1 & \bar{\omega} & \bar{\omega} & 1 & 0 & 0 \\ \bar{\omega} & 1 & \bar{\omega} & 0 & 1 & 0 \\ \bar{\omega} & \bar{\omega} & 1 & 0 & 0 & 1 \end{array} \right]$$

Por el Teorema 2.35 vi) el peso de cada palabra de $\mathcal{G}_6$ es par. Como $\bar{\omega}1\bar{\omega}010 \in \mathcal{G}_6$ tenemos que $d(\mathcal{G}_6) \leq 4$. Supongamos que $d(\mathcal{G}_6) = 2$. Entonces, por el Teorema 2.46, existe un conjunto formado por dos columnas de H que es linealmente dependiente. Sin embargo, ninguna columna de H es un múltiplo de otra. Por lo tanto, $d(\mathcal{G}_6) = 4$. $\blacksquare$

2.5 EQUIVALENCIA DE CÓDIGOS

En esta sección vamos a establecer cuándo dos códigos son equivalentes, es decir cuándo son “esencialmente” el mismo. Algunos de los códigos con los que hemos trabajado han sido lineales, por ello es natural pensar que dos códigos lineales (tomados sobre el mismo cuerpo finito) son “esencialmente” el mismo si ellos son isomorfos como espacios vectoriales. Sin embargo, no es así. Lo que nos interesa al establecer el concepto de equivalencia entre dos códigos es que estos tengan los mismos parámetros.

2.5.1 Códigos equivalentes por permutación. Sea S_n el grupo simétrico de orden n . Sean $\sigma \in S_n$ y $\mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_q^n$, al vector $y_1 \cdots y_n \in \mathbb{F}_q^n$ tal que $y_i = x_{\sigma^{-1}(i)}$ para todo $1 \leq i \leq n$ lo denotaremos por $\mathbf{x}\sigma$.

Ejemplo 2.48. Sean $\sigma = (1, 2, 3) \in S_3$ y $\mathbf{x} = 10\bar{\omega} \in \mathbb{F}_4^3$. Entonces, $\sigma^{-1}(1) = 3$, $\sigma^{-1}(2) = 1$ y $\sigma^{-1}(3) = 2$. Por lo tanto, $\mathbf{x}\sigma = \bar{\omega}10$. $\blacksquare$

Proposición 2.49. Si $\sigma \in S_n$ y P es la matriz de $n \times n$ definida por

$$P_{ij} = \begin{cases} 1 & \text{si } j = \sigma(i) \\ 0 & \text{si } j \neq \sigma(i) \end{cases}$$

Entonces, $\mathbf{x}\sigma = \mathbf{x}P$, para todo $\mathbf{x} \in \mathbb{F}_q^n$.

Demostración. Sean $\mathbf{x} = x_1 \cdots x_n$ y $\mathbf{z} = z_1 \cdots z_n \in \mathbb{F}_q^n$ tales que $\mathbf{z} = \mathbf{x}P$. Veamos quién es z_i , para cada i . Para $i \in \{1, \dots, n\}$ sea r tal que $r = \sigma^{-1}(i)$, luego, $z_i = x_r$. Por lo tanto, $z_i = x_{\sigma^{-1}(i)}$, para todo $1 \leq i \leq n$ y por ende $\mathbf{z} = \mathbf{x}\sigma$. $\square$

Con la notación de la proposición anterior, decimos que P es la matriz de permutación asociada a σ . Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos de longitud n , sobre el mismo cuerpo $\mathbb{F}_q$. Decimos que $\mathcal{C}_1$ es *equivalente por permutación* a $\mathcal{C}_2$ si existe $\sigma \in S_n$ tal que

$$\mathcal{C}_2 = \{\mathbf{x}\sigma : \mathbf{x} \in \mathcal{C}_1\}.$$

Si P es la matriz de permutación asociada a σ , entonces $\mathcal{C}_1$ es equivalente por permutación a $\mathcal{C}_2$ si

$$\mathcal{C}_2 = \{\mathbf{x}P : \mathbf{x} \in \mathcal{C}_1\}.$$

Sea S el conjunto de todos los códigos sobre $\mathbb{F}_q$ de longitud n y sea

$$R = \{(\mathcal{C}_1, \mathcal{C}_2) : \mathcal{C}_1 \text{ es equivalente por permutación a } \mathcal{C}_2\} \subseteq S \times S.$$

Se puede verificar que R es una relación de equivalencia sobre S . Por esto decimos que dos códigos son *equivalentes por permutación* si uno de ellos es equivalente por permutación al otro.

Teorema 2.50. Sea $\mathcal{C}_1$ un (n, M, d) código sobre $\mathbb{F}_q$. Si $\mathcal{C}_1$ es equivalente por permutación a $\mathcal{C}_2$. Entonces $\mathcal{C}_2$ es un (n, M, d) código sobre $\mathbb{F}_q$.

Demostración. Sea $\sigma \in S_n$ tal que $\mathcal{C}_2 = \{\mathbf{x}\sigma : \mathbf{x} \in \mathcal{C}_1\}$. Note que si $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}_1$ entonces $\mathbf{x}\sigma = x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(n)}$ y $(\mathbf{x}\sigma)\sigma^{-1} = x_{\sigma(\sigma^{-1}(1))} \cdots x_{\sigma(\sigma^{-1}(n))} = \mathbf{x}$. Sea $f : \mathcal{C}_1 \rightarrow \mathcal{C}_2$ la función dada por $f(\mathbf{x}) = \mathbf{x}\sigma$, para todo $\mathbf{x} \in \mathcal{C}_1$. Es inmediato que f es sobreyectiva. Supongamos que existen $\mathbf{x}, \mathbf{y} \in \mathcal{C}_1$ tales que $\mathbf{x}\sigma = \mathbf{y}\sigma$. Luego, $(\mathbf{x}\sigma)\sigma^{-1} = (\mathbf{y}\sigma)\sigma^{-1}$, y por ende, $\mathbf{x} = \mathbf{y}$. Por lo tanto f es una biyección. Luego, $|\mathcal{C}_2| = |\mathcal{C}_1| = M$.

Consideremos $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathcal{C}_1$ e $i \in \{1, \dots, n\}$ tal que $x_i = y_i$. Luego $x_{\sigma(\sigma^{-1}(i))} = y_{\sigma(\sigma^{-1}(i))}$. Sea $j = \sigma(i)$. Como $\sigma(\sigma^{-1}(i)) = \sigma^{-1}(\sigma(i))$ tenemos que $x_{\sigma^{-1}(j)} = y_{\sigma^{-1}(j)}$. Así, si $A = \{i : x_i = y_i\}$ entonces $\sigma(A) = \{j : x_{\sigma^{-1}(j)} = y_{\sigma^{-1}(j)}\}$. De aquí que, $\sigma|_A : A \rightarrow \{j : x_{\sigma^{-1}(j)} = y_{\sigma^{-1}(j)}\}$ es sobreyectiva. Más aún, por ser σ una función biyectiva, en particular inyectiva, tenemos que $\sigma|_A$ es inyectiva. Luego, $|A| = |\{j : x_{\sigma^{-1}(j)} = y_{\sigma^{-1}(j)}\}|$. Por lo tanto,

$$d(\mathbf{x}\sigma, \mathbf{y}\sigma) = n - |\{j : x_{\sigma^{-1}(j)} = y_{\sigma^{-1}(j)}\}| = n - |\{i : x_i = y_i\}| = d(\mathbf{x}, \mathbf{y}).$$

Si $\mathbf{x}, \mathbf{y}$ son tales que $d(\mathbf{x}, \mathbf{y}) = d$, entonces $d(\mathbf{x}\sigma, \mathbf{y}\sigma) = d$. Por ende, $d(\mathcal{C}_2) \leq d$. Si $d(\mathcal{C}_2) < d$ tendríamos que existen $\mathbf{z}, \mathbf{w} \in \mathcal{C}_2$ tales que $d(\mathbf{w}, \mathbf{z}) = d(\mathcal{C}_2)$, si $\mathbf{u}, \mathbf{v} \in \mathcal{C}_1$ son tales que $\mathbf{z} = \mathbf{u}\sigma$ y $\mathbf{w} = \mathbf{v}\sigma$ entonces $0 < d(\mathbf{u}, \mathbf{v}) = d(\mathbf{w}, \mathbf{z}) < d$ pero esto contradice la minimalidad de d , por lo tanto $d(\mathcal{C}_2) = d$. $\square$

Proposición 2.51. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos de longitud n , sobre el mismo cuerpo $\mathbb{F}_q$, tales que $\mathcal{C}_2 = \{\mathbf{x}\sigma : \mathbf{x} \in \mathcal{C}_1\}$. Sea P la matriz de permutación asociada a σ . Si $\mathcal{C}_1$ es lineal y G es una matriz generadora para $\mathcal{C}_1$ entonces $\mathcal{C}_2$ es lineal y GP es una matriz generadora para $\mathcal{C}_2$.

Demostración. Sean $k = \dim(\mathcal{C}_1)$ y $\mathbf{g}_1, \dots, \mathbf{g}_k$ las filas de G . Entonces las filas de GP son $\mathbf{g}_1P, \dots, \mathbf{g}_kP$. Es claro $\{\mathbf{g}_1P, \dots, \mathbf{g}_kP\} \subseteq \mathcal{C}_2$, esto implica que $\text{Gen}\{\mathbf{g}_1P, \dots, \mathbf{g}_kP\} \subseteq \mathcal{C}_2$. Sea $\mathbf{x} \in \mathcal{C}_2$. Luego, existe $\mathbf{y} \in \mathcal{C}_1$ tal que $\mathbf{x} = \mathbf{y}P$. Sean $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$ tales que $\mathbf{y} = \alpha_1\mathbf{g}_1 + \cdots + \alpha_k\mathbf{g}_k$. Así,

$$\mathbf{x} = (\alpha_1\mathbf{g}_1 + \cdots + \alpha_k\mathbf{g}_k)P = \alpha_1\mathbf{g}_1P + \cdots + \alpha_k\mathbf{g}_kP.$$

De aquí que $\mathcal{C}_2 \subseteq \text{Gen}\{\mathbf{g}_1P, \dots, \mathbf{g}_kP\}$. Así, $\mathcal{C}_2 = \text{Gen}\{\mathbf{g}_1P, \dots, \mathbf{g}_kP\}$. Por el Teorema 2.50, $|\mathcal{C}_2| = q^k$, lo que concluye la prueba. $\square$

Corolario 2.52. Sea $\mathcal{C}_1$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Si $\mathcal{C}_1$ es equivalente por permutación a $\mathcal{C}_2$ entonces $\mathcal{C}_2$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$.

Demostración. Es consecuencia del Teorema 2.50 y la Proposición 2.51. $\square$

Ejemplo 2.53. Sea $\mathcal{C}_1$ el código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Por la *Proposición 2.38* y dado que $110000 \in \mathcal{C}_1$ tenemos que $d(\mathcal{C}_1) = 2$. Así, $\mathcal{C}_1$ es un $[6, 3, 2]$ código binario. Sea $\sigma = (2, 6) \in S_6$. Luego,

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{y} \quad GP = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Sea $\mathcal{C}_2$ el código binario con matriz generadora GP . Entonces $\mathcal{C}_2$ es un $[6, 3, 2]$ código binario equivalente por permutación a $\mathcal{C}_1$. Observe que la matriz GP se obtiene al intercambiar las columnas 2 y 6 de G . ■

Teorema 2.54. Sea $\mathcal{C}$ un código lineal. Entonces $\mathcal{C}$ es equivalente por permutación a un código lineal que tiene una matriz generadora en forma estándar.

Demostración. Supongamos que $\mathcal{C}_1$ un $[n, k]$ código sobre $\mathbb{F}_q$ con matriz generadora G . Por el *Corolario 2.6*, el rango de G es k . Así, al reducir G mediante operaciones elementales por filas, obtenemos una matriz generadora G' para $\mathcal{C}$ con k pivotes 1. Sea $i_j \in \{1, \dots, n\}$ tal que la columna i_j de G' tiene un pivote en la componente j -ésima. Sea $\sigma \in S_n$ tal que $\sigma(i_j) = j$, para todo $1 \leq j \leq k$ y sea P la matriz asociada a σ . Sea $\mathcal{C}_2$ el código lineal sobre $\mathbb{F}_q$ generado por las filas de la matriz $G'P$. Entonces $\mathcal{C}_2$ es un código equivalente por permutación a $\mathcal{C}$ que tiene una matriz generadora en forma estándar, a saber $G'P$. □

2.5.2 Códigos monomialmente equivalentes. La equivalencia monomial es otro tipo de equivalencia entre códigos, de hecho es más general que la equivalencia por permutaciones y nos será de gran utilidad cuando abordemos la Cota de Griesmer.

Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos de longitud n , sobre el mismo cuerpo $\mathbb{F}_q$. Decimos que $\mathcal{C}_1$ es *monomialmente equivalente* a $\mathcal{C}_2$ si existen $\sigma \in S_n$ y una matriz diagonal D de tamaño $n \times n$, tales que si P es la matriz de permutación asociada a σ , entonces

$$\mathcal{C}_2 = \{\mathbf{x}PD : \mathbf{x} \in \mathcal{C}_1\}.$$

Teorema 2.55. Sean $\mathcal{C}_1$ un (n, M, d) código sobre $\mathbb{F}_q$ y D una matriz diagonal de tamaño $n \times n$ tal que $D_{ii} \neq 0$, para todo $1 \leq i \leq n$. Entonces $\mathcal{C}_2 = \{\mathbf{c}D : \mathbf{c} \in \mathcal{C}_1\}$ es un (n, M, d) código sobre $\mathbb{F}_q$.

Demostración. Sea $f : \mathcal{C}_1 \rightarrow \mathcal{C}_2$ la función dada por $f(\mathbf{x}) = \mathbf{x}D$, para todo $\mathbf{x} \in \mathcal{C}_1$. Es inmediato que f es sobreyectiva. Supongamos que existen $\mathbf{x}, \mathbf{y} \in \mathcal{C}_1$ tales que $\mathbf{x}D = \mathbf{y}D$. Como $D_{ii} \neq 0$ para todo $i \in \{1, \dots, n\}$, tenemos que D es invertible. Luego, $\mathbf{x} = \mathbf{y}$. Por lo tanto, f es una biyección, lo cual implica que $|\mathcal{C}_2| = |\mathcal{C}_1| = M$.

Sean $\mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathcal{C}_1$ e $i \in \{1, \dots, n\}$ tal que $x_i = y_i$. Luego, $x_i D_{ii} = y_i D_{ii}$. Así, $i \in \{j : x_j D_{jj} = y_j D_{jj}\}$. Por otra parte, sea $i \in \{1, \dots, n\}$ tal que $x_i D_{ii} = y_i D_{ii}$. Como $D_{ii} \neq 0$ tenemos que $x_i = y_i$. Así, $i \in \{j : x_j = y_j\}$ y por ende,

$$|\{j : x_j D_{jj} = y_j D_{jj}\}| = |\{j : x_j = y_j\}|.$$

Por lo tanto,

$$d(\mathbf{x}D, \mathbf{y}D) = n - |\{j : x_j D_{jj} = y_j D_{jj}\}| = n - |\{j : x_j = y_j\}| = d(\mathbf{x}, \mathbf{y}).$$

Si $\mathbf{x}, \mathbf{y}$ son tales que $d(\mathbf{x}, \mathbf{y}) = d$, entonces $d(\mathbf{x}D, \mathbf{y}D) = d$. Por ende, $d(\mathcal{C}_2) \leq d$. Si $d(\mathcal{C}_2) < d$, tendríamos que existen $\mathbf{z}, \mathbf{w} \in \mathcal{C}_2$ tales que $d(\mathbf{w}, \mathbf{z}) = d(\mathcal{C}_2)$ y si $\mathbf{u}, \mathbf{v} \in \mathcal{C}_1$ son tales que $\mathbf{z} = \mathbf{u}D$ y $\mathbf{w} = \mathbf{v}D$ entonces obtendríamos que $0 < d(\mathbf{u}, \mathbf{v}) = d(\mathbf{w}, \mathbf{z}) < d$ pero esto contradice la minimalidad de d , por lo tanto $d(\mathcal{C}_2) = d$. □

Proposición 2.56. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos de longitud n , sobre el mismo cuerpo $\mathbb{F}_q$, tales que $\mathcal{C}_2 = \{\mathbf{x}D : \mathbf{x} \in \mathcal{C}_1\}$, con D una matriz diagonal de tamaño $n \times n$ tal que $D_{ii} \neq 0$, para todo $1 \leq i \leq n$. Si $\mathcal{C}_1$ es lineal y G es una matriz generadora para $\mathcal{C}_1$ entonces $\mathcal{C}_2$ es lineal y GD es una matriz generadora para $\mathcal{C}_2$.

Demostración. La prueba es análoga a la de la *Proposición 2.51*. □

Corolario 2.57. Sea $\mathcal{C}_1$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Si $\mathcal{C}_2 = \{\mathbf{x}D : \mathbf{x} \in \mathcal{C}_1\}$, con D una matriz diagonal de tamaño $n \times n$ tal que $D_{ii} \neq 0$, para todo $1 \leq i \leq n$. Entonces $\mathcal{C}_2$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$.

Demostración. Es consecuencia del *Teorema 2.55* y la *Proposición 2.56*. □

A una matriz diagonal D de tamaño $n \times n$, la denotaremos por $\text{diag}(D_{11}, \dots, D_{nn})$. Por brevedad en la escritura, en adelante omitiremos que $D_{ii} \neq 0$, para todo $1 \leq i \leq n$.

Teorema 2.58. Sea $\mathcal{C}_1$ un (n, M, d) código sobre $\mathbb{F}_q$. Si $\mathcal{C}_2 = \{\mathbf{x}PD : \mathbf{x} \in \mathcal{C}_1\}$, con D una matriz diagonal de tamaño $n \times n$ y P una matriz de permutación asociada a alguna $\sigma \in S_n$. Entonces $\mathcal{C}_2$ es un (n, M, d) código sobre $\mathbb{F}_q$.

Demostración. Es consecuencia de los *Teoremas 2.50* y *2.55*. □

Corolario 2.59. Sea $\mathcal{C}_1$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Si $\mathcal{C}_2 = \{\mathbf{x}PD : \mathbf{x} \in \mathcal{C}_1\}$, con D una matriz diagonal de tamaño $n \times n$ y P una matriz de permutación asociada a alguna $\sigma \in S_n$. Entonces $\mathcal{C}_2$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$.

Demostración. Es consecuencia de los *Corolarios 2.52* y *2.57*. □

Ejemplo 2.60. Sean $\sigma = (1, 2, 3) \in S_3$ y $D = \text{diag}(c, a, b)$. La matriz de permutación asociada a σ es

$$P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Sea $\mathbf{x} = 1\omega\bar{\omega} \in \mathbb{F}_4^3$. Entonces

$$\mathbf{x}PD = [1, \omega, \bar{\omega}] \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{bmatrix} = [c\bar{\omega}, a, b\omega]$$

■

2.6 CONSTRUCCIÓN DE NUEVOS CÓDIGOS A PARTIR DE OTROS YA EXISTENTES

2.6.1 Códigos perforados. Sean $\mathbf{x} = x_1 \cdots x_i \cdots x_n \in \mathbb{F}_q^n$ con $1 \leq i \leq n$ fijo. Decimos que el vector $x_1 \cdots x_{i-1}x_{i+1} \cdots x_n$ en $\mathbb{F}_q^{n-1}$ es el vector que resulta de *perforar* $\mathbf{x}$ en su i -ésima componente y lo denotamos por $\mathbf{x}^*$ o por $x_1 \cdots \widehat{x_i} \cdots x_n$.

Proposición 2.61. Sea $i \in \{1, \dots, n\}$ fijo. Si $\mathbf{x} = x_1 \cdots x_i \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_i \cdots y_n$ están en $\mathbb{F}_q^n$ entonces

$$d(\mathbf{x}^*, \mathbf{y}^*) = \begin{cases} d(\mathbf{x}, \mathbf{y}) & \text{si } x_i = y_i \\ d(\mathbf{x}, \mathbf{y}) - 1 & \text{en otro caso.} \end{cases}$$

Demostración. Si $x_i = y_i$ entonces $i \notin \{j : x_j \neq y_j\}$. Así, $\{j : x_j \neq y_j\} = \{j : j \neq i, x_j \neq y_j\}$, luego $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x}^*, \mathbf{y}^*)$. Por el contrario, si $x_i \neq y_i$ entonces

$$\{j : x_j \neq y_j\} = \{j : j \neq i, x_j \neq y_j\} \cup \{i\}.$$

Por lo tanto, $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x}^*, \mathbf{y}^*) + 1$. □

Proposición 2.62. Si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ y $\alpha \in \mathbb{F}_q$. Entonces $(\alpha\mathbf{x} + \mathbf{y})^* = \alpha\mathbf{x}^* + \mathbf{y}^*$.

Demostración. Sean $\mathbf{x} = x_1 \cdots x_i \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_i \cdots y_n$ en $\mathcal{C}$. Luego

$$\begin{aligned} \alpha\mathbf{x}^* + \mathbf{y}^* &= \alpha x_1 \cdots \alpha \widehat{x_i} \cdots \alpha x_n + y_1 \cdots \widehat{y_i} \cdots y_n \\ &= \alpha x_1 + y_1 \cdots \alpha \widehat{x_i} + y_i \cdots \alpha x_n + y_n \\ &= (\alpha\mathbf{x} + \mathbf{y})^*. \end{aligned}$$

□

Sea $\mathcal{C}$ un código sobre $\mathbb{F}_q$ de longitud n . Al subconjunto de $\mathbb{F}_q^{n-1}$

$$\mathcal{C}_i^* := \{\mathbf{x}^* : \mathbf{x} \in \mathcal{C}\},$$

que resulta al perforar cada palabra de $\mathcal{C}$ en su i -ésima componente lo llamamos el *código perforado* $\mathcal{C}$ en la i -ésima componente.

Proposición 2.63. Sean $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ con $d > 1$, $q^n > M$ e $1 \leq i \leq n$ fijo. Entonces $\mathcal{C}_i^*$ es un $(n-1, M, d')$ código sobre $\mathbb{F}_q$, donde

- i) $d' = d - 1$, si existen $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$ y $x_i \neq y_i$;
- ii) $d' = d$, en caso contrario.

Demostración. Sea $f : \mathcal{C} \rightarrow \mathcal{C}_i^*$ la función dada por $f(\mathbf{x}) = \mathbf{x}^*$, para todo $\mathbf{x} \in \mathcal{C}$. Es claro que f es sobreyectiva. Si existiesen dos palabras $\mathbf{u} = u_1 \cdots u_n$ y $\mathbf{v} = v_1 \cdots v_n$ en $\mathcal{C}$ tales que $\mathbf{u}^* = \mathbf{v}^*$ tendríamos que $u_i \neq v_i$ y $u_j = v_j$ para todo $1 \leq j \leq n$ con $j \neq i$, de aquí que $d(\mathbf{u}, \mathbf{v}) = 1$ pero esto es una contradicción pues $d(\mathcal{C}) > 1$, luego $\mathbf{u} = \mathbf{v}$ y por lo tanto, f es biyectiva. Esto implica que $|\mathcal{C}_i^*| = |\mathcal{C}| = M$.

Supongamos que existen $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$ y $x_i \neq y_i$. Luego, de la *Proposición 2.61*, $d(\mathbf{x}^*, \mathbf{y}^*) = d - 1$. Por ende, $d' \leq d - 1$. Supongamos que $d' < d - 1$. Sean $\mathbf{z}, \mathbf{w} \in \mathcal{C}_i^*$ tales que $d(\mathbf{z}, \mathbf{w}) = d'$ y sean $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ tales que $\mathbf{z} = \mathbf{a}^*$ y $\mathbf{w} = \mathbf{b}^*$. Así, $d(\mathbf{a}^*, \mathbf{b}^*) = d'$. Luego, $d(\mathbf{a}, \mathbf{b})$ es d' o $d' + 1$, ya que de lo contrario se contradice la *Proposición 2.61*. En cualquier caso obtenemos, $0 < d(\mathbf{a}, \mathbf{b}) \leq d - 1$, esto contradice la minimalidad de d . Por lo tanto, $d' = d - 1$.

Finalmente, supongamos que si un par de palabras en $\mathcal{C}$ difieren en d componentes entonces coinciden en la i -ésima. Sean $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$. Luego, $x_i = y_i$ y por la *Proposición 2.61*, $d(\mathbf{x}^*, \mathbf{y}^*) = d$, de aquí que $d' \leq d$. Supongamos que $d' < d$. Sean $\mathbf{z}, \mathbf{w} \in \mathcal{C}$ tales que $d(\mathbf{z}, \mathbf{w}) = d'$ y sean $\mathbf{a} = a_1 \cdots a_n, \mathbf{b} = b_1 \cdots b_n \in \mathcal{C}$ tales que $\mathbf{z} = \mathbf{a}^*$ y $\mathbf{w} = \mathbf{b}^*$. Así, $d(\mathbf{a}^*, \mathbf{b}^*) = d'$. Luego, $d(\mathbf{a}, \mathbf{b})$ es d' o $d' + 1$, por la *Proposición 2.61*. En cualquier caso obtenemos, $0 < d(\mathbf{a}, \mathbf{b}) \leq d$. Si, $d(\mathbf{a}, \mathbf{b}) = d$ tendríamos, por la *Proposición 2.61*, que $a_i \neq b_i$ pero esto contradice la hipótesis, de aquí que $0 < d(\mathbf{a}, \mathbf{b}) < d$ lo cual contradice la minimalidad de d . Por lo tanto, $d' = d$. □

El siguiente teorema muestra, en particular, que si $\mathcal{C}$ es lineal entonces $\mathcal{C}_i^*$ también lo es.

Teorema 2.64. Sean $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y $1 \leq i \leq n$ fijo. Si G es una matriz generadora para $\mathcal{C}$ y $\mathbf{g}_1, \dots, \mathbf{g}_k$ son las filas de G entonces $\mathcal{C}_i^* = \text{Gen}\{\mathbf{g}_1^*, \dots, \mathbf{g}_k^*\}$.

Demostración. Sea $\mathbf{c} \in \mathcal{C}_i^*$. Así, existe $\mathbf{x} \in \mathcal{C}$ tal que $\mathbf{c} = \mathbf{x}^*$. Sean $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$ tales que $\mathbf{x} = \alpha_1 \mathbf{g}_1 + \dots + \alpha_k \mathbf{g}_k$. Luego, por la *Proposición 2.62*, $\mathbf{c} = \alpha_1 \mathbf{g}_1^* + \dots + \alpha_k \mathbf{g}_k^*$. Por lo tanto, $\mathcal{C}_i^* \subseteq \text{Gen}\{\mathbf{g}_1^*, \dots, \mathbf{g}_k^*\}$, la otra inclusión es inmediata. $\square$

Teorema 2.65. Sean $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ y $1 \leq i \leq n$ fijo. Entonces

- i) Si $d > 1$, $\mathcal{C}_i^*$ es un $[n-1, k, d']$ código sobre $\mathbb{F}_q$, donde $d' = d-1$ si existe por lo menos una palabra de $\mathcal{C}$ de peso mínimo con i -ésima componente no nula y $d' = d$ en caso contrario.
- ii) Si $d = 1$ y $n > k$, $\mathcal{C}_i^*$ es un $[n-1, k, 1]$ código sobre $\mathbb{F}_q$ si cada palabra de $\mathcal{C}$ de peso 1 tiene i -ésima componente nula; en otro caso, y si además $k > 1$, $\mathcal{C}_i^*$ es un $[n-1, k-1, d']$ código sobre $\mathbb{F}_q$ con $d' \geq 1$.

Demostración.

- i) Como $\mathcal{C}$ lineal, $d(\mathcal{C}) = wt(\mathcal{C})$. Por lo tanto, el resultado es consecuencia de la *Proposición 2.63*.
- ii) Supongamos que para cada $\mathbf{y} = y_1 \dots y_n \in \mathcal{C}$ tal que $wt(\mathbf{y}) = 1$ se cumple que $y_i = 0$. Sea $\mathbf{x} = x_1 \dots x_n \in \mathcal{C}$ tal que $wt(\mathbf{x}) = 1$. Luego, $x_j = t \neq 0$, para algún $1 \leq j \leq n$ con $j \neq i$. Por lo tanto $wt(\mathbf{x}^*) = 1$ y $d' = 1$. Veamos que $\dim(\mathcal{C}_i^*) = k$. Completamos el conjunto $\{\mathbf{x}\}$ a una base $\{\mathbf{x}, \mathbf{g}_2, \dots, \mathbf{g}_k\}$ de $\mathcal{C}$. Así, una matriz generadora para $\mathcal{C}$ es

$$G = \begin{bmatrix} \mathbf{x} \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 & \dots & t & \dots & 0 \\ g_{21} & \dots & g_{2i} & \dots & g_{2j} & \dots & g_{2n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ g_{k1} & \dots & g_{ki} & \dots & g_{kj} & \dots & g_{kn} \end{bmatrix}$$

El *Teorema 2.64* proporciona un candidato a base para $\mathcal{C}_i^*$ a partir de G , a saber $\{\mathbf{x}^*, \mathbf{g}_2^*, \dots, \mathbf{g}_k^*\}$; resta verificar que dicho conjunto es linealmente independiente. Supongamos que

$$\mathbf{0} = \lambda \mathbf{x}^* + \alpha_2 \mathbf{g}_2^* + \dots + \alpha_k \mathbf{g}_k^*,$$

luego,

$$\alpha_2 g_{2m} + \dots + \alpha_k g_{km} = 0,$$

para todo $1 \leq m \leq n$, con $m \neq i$ y $m \neq j$. Además, $\lambda t + \alpha_2 g_{2j} + \dots + \alpha_k g_{kj} = 0$. Si probamos que $\alpha_2 g_{2i} + \dots + \alpha_k g_{ki} = 0$, tendríamos que $\mathbf{0} = \lambda \mathbf{x} + \alpha_2 \mathbf{g}_2 + \dots + \alpha_k \mathbf{g}_k$ y por ser $\{\mathbf{x}, \mathbf{g}_2, \dots, \mathbf{g}_k\}$ linealmente independiente podríamos concluir que $\lambda = \alpha_2 = \dots = \alpha_k = 0$. Supongamos lo contrario, sea

$$\mathbf{c} = \lambda \mathbf{x} + \alpha_2 \mathbf{g}_2 + \dots + \alpha_k \mathbf{g}_k.$$

Así, si $\mathbf{c} = c_1 \dots c_n$ tenemos que $wt(\mathbf{c}) = 1$ y $c_i \neq 0$, esto contradice la hipótesis, por lo tanto $\dim(\mathcal{C}_i^*) = k$.

Por otra parte, supongamos que $k > 1$ y que existe $\mathbf{x} = x_1 \dots x_n \in \mathcal{C}$ tal que $wt(\mathbf{x}) = 1$ y $x_i = t \neq 0$. Luego, $wt(\mathbf{x}^*) = 0$. Como $k > 1$ existe por lo menos una palabra $\mathbf{z} = z_1 \dots z_n$ en $\mathcal{C}$ que no es un múltiplo de $\mathbf{x}$, es decir, existe $1 \leq m \leq n$ con $m \neq i$ tal que $z_m \neq 0$. Luego, $wt(\mathbf{z}^*) \geq 1$. Por lo tanto, $d' \neq 0$, esto es, $d' \geq 1$. Resta verificar que $\dim(\mathcal{C}_i^*) = k-1$. Como en el caso anterior, completamos $\{\mathbf{x}\}$ a una base de $\mathcal{C}$ de tal manera que una matriz generadora para $\mathcal{C}$ es

$$G = \begin{bmatrix} \mathbf{x} \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix} = \begin{bmatrix} 0 & \dots & t & \dots & 0 \\ g_{21} & \dots & g_{2i} & \dots & g_{2n} \\ \vdots & & \vdots & & \vdots \\ g_{k1} & \dots & g_{ki} & \dots & g_{kn} \end{bmatrix}$$

Como $\mathbf{x}^* = \mathbf{0}$ tenemos que $\{\mathbf{x}^*, \mathbf{g}_2^*, \dots, \mathbf{g}_k^*\}$ es un conjunto linealmente dependiente. Veamos que $\{\mathbf{g}_2^*, \dots, \mathbf{g}_k^*\}$ es linealmente independiente. Note que este conjunto no es vacío puesto que $k > 1$. Sean $\alpha_2, \dots, \alpha_k \in \mathbb{F}_q$ tales que $\mathbf{0} = \alpha_2 \mathbf{g}_2^* + \dots + \alpha_k \mathbf{g}_k^*$, entonces

$$\alpha_2 g_{2j} + \dots + \alpha_k g_{kj} = 0,$$

para todo $1 \leq j \leq n$, con $j \neq i$. Sea $\theta = \alpha_2 g_{2i} + \dots + \alpha_k g_{ki}$ y veamos que $\theta = 0$. Supongamos lo contrario. Consideremos la siguiente combinación lineal

$$-\frac{\theta}{t} \mathbf{x} + \alpha_2 \mathbf{g}_2 + \dots + \alpha_k \mathbf{g}_k = \begin{bmatrix} 0 \\ \vdots \\ -\theta \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} \alpha_2 g_{21} + \dots + \alpha_k g_{k1} \\ \vdots \\ \alpha_2 g_{2i} + \dots + \alpha_k g_{ki} \\ \vdots \\ \alpha_2 g_{2n} + \dots + \alpha_k g_{kn} \end{bmatrix} = \mathbf{0}.$$

Así, tenemos una combinación no trivial de $\mathbf{0}$, lo que no es posible puesto que $\{\mathbf{x}, \mathbf{g}_2, \dots, \mathbf{g}_k\}$ es linealmente independiente, de aquí que $\theta = 0$. Luego, $\alpha_2 \mathbf{g}_2 + \dots + \alpha_k \mathbf{g}_k = \mathbf{0}$ y $\alpha_2 = \dots = \alpha_k = 0$ y por lo tanto $\dim(\mathcal{C}_i^*) = k - 1$.

□

Corolario 2.66. Dado un $[n, k, d]_q$ código con $d > 1$ existe un $[n - 1, k, d - 1]_q$ código.

Demostración. Sean $\mathcal{C}$ un $[n, k, d]_q$ código con $d > 1$ (esto implica que $n > 1$), $\mathbf{c} = c_1 \dots c_n \in \mathcal{C}$ una palabra de peso mínimo d e $i \in \{1, \dots, n\}$ tal que $c_i \neq 0$. Entonces por el Teorema 2.65 i) $\mathcal{C}_i^*$ es un $[n - 1, k, d - 1]$ código sobre $\mathbb{F}_q$. □

Corolario 2.67. Sea $\mathcal{C}$ un $[n, k, d]_q$ código con $d > 1$, si l es un entero tal que $0 < l < d$ entonces existe un $[n - l, k, d - l]_q$ código.

Demostración. Haremos la prueba mediante inducción sobre l . Si $l = 1$ entonces el Corolario 2.66 garantiza que existe un $[n - 1, k, d - 1]_q$ código. Supongamos que existe un $[n - l, k, d - l]_q$ código con $0 < l < d - 1$, de aquí que $d - l > 1$ y por el Corolario 2.66 tenemos que existe un $[n - (l + 1), k, d - (l + 1)]_q$ código, lo que concluye la prueba. □

Corolario 2.68. Sean $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$, $1 \leq i \leq n$ fijo, G una matriz generadora para $\mathcal{C}$ y $\mathbf{g}_1, \dots, \mathbf{g}_k$ las filas de G .

- i) Si $d > 1$, entonces una matriz generadora para $\mathcal{C}_i^*$ tiene como filas a $\mathbf{g}_1^*, \dots, \mathbf{g}_k^*$.
- ii) Lo mismo sucede si $d = 1$ y cada palabra de peso 1 tiene i -ésima componente nula.
- iii) Si $d = 1$, $k > 1$ y existe por lo menos una palabra de peso 1 con i -ésima componente no nula, entonces existe por lo menos un vector en $\{\mathbf{g}_1^*, \dots, \mathbf{g}_k^*\}$ que es combinación lineal de los otros; una matriz generadora para $\mathcal{C}_i^*$ tiene como filas a $k - 1$ vectores linealmente independientes del conjunto $\{\mathbf{g}_1^*, \dots, \mathbf{g}_k^*\}$.

Demostración. Es consecuencia de los Teoremas 2.64 y 2.65. □

Ejemplo 2.69. Sea $\mathcal{C}$ un $[5, 2, 2]$ código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Dado que $d > 1$ tenemos que una matriz generadora para $\mathcal{C}_1^*$ es

$$G_1^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Más aún, como $11000 \in \mathcal{C}$ es de peso mínimo y tiene primera componente no nula, tenemos que el peso mínimo de $\mathcal{C}_1^*$ es 1. Por lo tanto, $\mathcal{C}_1^*$ es un $[4, 2, 1]$ código binario.

Por otra parte, una matriz generadora para $\mathcal{C}_5^*$ es

$$G_5^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Como la única palabra de $\mathcal{C}$ con peso mínimo es 11000 y la quinta componente de esta palabra es cero, tenemos que el peso mínimo de $\mathcal{C}_5^*$ es 2. Por lo tanto, $\mathcal{C}_5^*$ es un $[4, 2, 2]$ código binario. ■

Ejemplo 2.70. Sea $\mathcal{D}$ un $[4, 2, 1]$ código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Como $1000 \in \mathcal{D}$ y su primera componente es no nula, tenemos que $\mathcal{D}_1^*$ es un $[3, 1]$ código binario con matriz generadora

$$G_1^* = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

De aquí que, $d(\mathcal{D}_1^*) = 3$.

Dado que 1000 es la única palabra de $\mathcal{D}$ de peso 1 y que su cuarta componente es nula, tenemos que $\mathcal{D}_4^*$ es un $[3, 2, 1]$ código binario con matriz generadora

$$G_4^* = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

■

2.6.2 Extensión de códigos. Sea $\mathbf{x} = x_1 \cdots x_n \in \mathbb{F}_2^n$. Al vector $x_1 \cdots x_n x_{n+1} \in \mathbb{F}_2^{n+1}$ con

$$x_{n+1} = \begin{cases} 1 & \text{si } wt(\mathbf{x}) \text{ es impar} \\ 0 & \text{en otro caso} \end{cases}$$

lo denotamos por $\widehat{\mathbf{x}}$. Por el Teorema 2.33 iii),

$$\mathbf{x} \cdot \mathbf{x} + x_{n+1} \equiv wt(\mathbf{x}) + x_{n+1} \pmod{2} \equiv 0 \pmod{2}.$$

Así, $x_1 + \cdots + x_n + x_{n+1} = 0$.

En general, dado $\mathbf{x} = x_1 \cdots x_n$ en $\mathbb{F}_q^n$ denotamos por $\widehat{\mathbf{x}}$ al vector $x_1 \cdots x_n x_{n+1}$ de $\mathbb{F}_q^{n+1}$ tal que

$$x_1 + \cdots + x_n + x_{n+1} = 0.$$

Proposición 2.71. Sean $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathbb{F}_q^n$. Entonces

$$d(\widehat{\mathbf{x}}, \widehat{\mathbf{y}}) = \begin{cases} d(\mathbf{x}, \mathbf{y}) & \text{si } x_1 + \cdots + x_n = y_1 + \cdots + y_n \\ d(\mathbf{x}, \mathbf{y}) + 1 & \text{en otro caso} \end{cases}$$

Demostración. Sean $\widehat{\mathbf{x}} = x_1 \cdots x_n x_{n+1}$ e $\widehat{\mathbf{y}} = y_1 \cdots y_n y_{n+1}$ en $\mathbb{F}_q^{n+1}$ con $x_1 + \cdots + x_n + x_{n+1} = 0$ y $y_1 + \cdots + y_n + y_{n+1} = 0$. Si $x_1 + \cdots + x_n = y_1 + \cdots + y_n$ entonces $x_{n+1} = y_{n+1}$. Luego,

$$\{1 \leq i \leq n+1 : x_i \neq y_i\} = \{1 \leq i \leq n : x_i \neq y_i\}.$$

Por lo tanto, $d(\widehat{\mathbf{x}}, \widehat{\mathbf{y}}) = d(\mathbf{x}, \mathbf{y})$. Si por el contrario, $x_1 + \cdots + x_n \neq y_1 + \cdots + y_n$, entonces $x_{n+1} \neq y_{n+1}$. Luego,

$$\{1 \leq i \leq n+1 : x_i \neq y_i\} = \{1 \leq i \leq n : x_i \neq y_i\} \cup \{n+1\}.$$

Por lo tanto, $d(\widehat{\mathbf{x}}, \widehat{\mathbf{y}}) = d(\mathbf{x}, \mathbf{y}) + 1$. □

Sea $\mathcal{C}$ un código sobre $\mathbb{F}_q$ de longitud n . El *código extendido* de $\mathcal{C}$ se define como

$$\widehat{\mathcal{C}} := \{\widehat{\mathbf{x}} : \mathbf{x} \in \mathcal{C}\} \subseteq \mathbb{F}_q^{n+1}.$$

Observación 2.72. La unicidad del inverso aditivo en un cuerpo garantiza que el código extendido de un código dado es único.

Teorema 2.73. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$. Entonces $\widehat{\mathcal{C}}$ es un $(n+1, M, d')$ código sobre $\mathbb{F}_q$ con $d' = d$ o $d+1$.

Demostración. Sea $f : \mathcal{C} \rightarrow \widehat{\mathcal{C}}$ la función dada por $f(\mathbf{x}) = \widehat{\mathbf{x}}$. Es claro que f es sobreyectiva. Sean $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tales que $\widehat{\mathbf{x}} = \widehat{\mathbf{y}}$. Esto implica que, $x_i = y_i$, para todo $1 \leq i \leq n$. Luego, $\mathbf{x} = \mathbf{y}$. Así, f es además inyectiva. Por lo tanto, f es una biyección, y por consiguiente, $|\widehat{\mathcal{C}}| = |\mathcal{C}| = M$.

Sean

$$A = \{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}, x_1 + \cdots + x_n = y_1 + \cdots + y_n\},$$

y

$$B = \{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} = x_1 \cdots x_n, \mathbf{y} = y_1 \cdots y_n \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}, x_1 + \cdots + x_n \neq y_1 + \cdots + y_n\}.$$

Es claro que

$$A \cup B = \{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}. \quad (2.2)$$

Analicemos los siguientes casos.

- i) Si $A = \emptyset$ entonces por (2.2), $d = \min B$. Sean $\mathbf{x}$ e $\mathbf{y}$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$. Como $d(\mathbf{x}, \mathbf{y}) \in B$ tenemos, por la *Proposición 2.71*, que

$$d(\widehat{\mathbf{x}}, \widehat{\mathbf{y}}) = d + 1.$$

De aquí que $d(\widehat{\mathcal{C}}) \leq d + 1$. Sean $\mathbf{z}, \mathbf{w} \in \widehat{\mathcal{C}}$ tales que $d(\mathbf{z}, \mathbf{w}) = d(\widehat{\mathcal{C}})$ y sean $\mathbf{u}, \mathbf{v}$ en $\mathcal{C}$, $\mathbf{u} \neq \mathbf{v}$, tales que $\mathbf{z} = \widehat{\mathbf{u}}$ y $\mathbf{w} = \widehat{\mathbf{v}}$. Como $d(\mathbf{u}, \mathbf{v}) \in B$ tenemos, por la *Proposición 2.71*

$$d(\widehat{\mathcal{C}}) = d(\mathbf{z}, \mathbf{w}) = d(\mathbf{u}, \mathbf{v}) + 1 \geq d + 1.$$

Por lo tanto, $d(\widehat{\mathcal{C}}) = d + 1$.

- ii) Si $B = \emptyset$, un razonamiento similar al anterior permite concluir que $d(\widehat{\mathcal{C}}) = d$.

Si $A \neq \emptyset$ y $B \neq \emptyset$ entonces, por (2.2), $d = \min\{\min A, \min B\}$.

- i) Si $\min B < \min A$ entonces $d = \min B$. Sean $\mathbf{x}$ e $\mathbf{y}$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$. Entonces $d(\mathbf{x}, \mathbf{y}) \in B$ y por la *Proposición 2.71*

$$d(\widehat{\mathbf{x}}, \widehat{\mathbf{y}}) = d + 1.$$

Por ende, $d(\widehat{\mathcal{C}}) \leq d + 1$. Sean $\mathbf{z}, \mathbf{w} \in \widehat{\mathcal{C}}$ palabras distintas y sean $\mathbf{u}$ y $\mathbf{v}$ en $\mathcal{C}$, $\mathbf{u} \neq \mathbf{v}$, tales que $\mathbf{z} = \widehat{\mathbf{u}}$ y $\mathbf{w} = \widehat{\mathbf{v}}$.

- A. Si $d(\mathbf{u}, \mathbf{v}) \in A$ entonces, por la *Proposición 2.71*, $d(\mathbf{z}, \mathbf{w}) = d(\mathbf{u}, \mathbf{v})$. Así, por hipótesis, $d(\mathbf{z}, \mathbf{w}) > d$. Es decir, $d(\mathbf{z}, \mathbf{w}) \geq d + 1$.
- B. Si $d(\mathbf{u}, \mathbf{v}) \in B$ entonces por la *Proposición 2.71*, $d(\mathbf{z}, \mathbf{w}) = d(\mathbf{u}, \mathbf{v}) + 1$ y por ende $d(\mathbf{z}, \mathbf{w}) \geq d + 1$.

En cualquier caso, $d(\mathbf{z}, \mathbf{w}) \geq d + 1$. Por lo tanto, $d(\widehat{\mathcal{C}}) = d + 1$.

- ii) Si $\min A \leq \min B$, un razonamiento análogo muestra que $d(\widehat{\mathcal{C}}) = d$.

□

La siguiente proposición muestra, en particular, que si $\mathcal{C}$ es lineal entonces $\widehat{\mathcal{C}}$ también lo es.

Proposición 2.74. Sea $\mathcal{C}$ un código lineal con matriz de chequeo de paridad H entonces

$$\widehat{\mathcal{H}} = \left[\begin{array}{ccc|c} 1 & \cdots & 1 & 1 \\ \hline & & & 0 \\ & & H & \vdots \\ & & & 0 \end{array} \right]$$

es una matriz de chequeo de paridad para $\widehat{\mathcal{C}}$.

Demostración. Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$ de longitud n . Sea $\mathbf{x} \in \widehat{\mathcal{C}}$, entonces existe $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tal que $\mathbf{x} = \widehat{\mathbf{y}}$. Así, $\mathbf{x} = y_1 \cdots y_n y_{n+1}$ con $y_1 + \cdots + y_n + y_{n+1} = 0$. Dado que $\mathbf{y} \in \mathcal{C}$ tenemos que $H\mathbf{y}^T = \mathbf{0}$. Por lo tanto

$$\widehat{\mathcal{H}}\mathbf{x}^T = \left[\begin{array}{ccc|c} 1 & \cdots & 1 & 1 \\ \hline & & & 0 \\ & & H & \vdots \\ & & & 0 \end{array} \right] \begin{bmatrix} y_1 \\ \vdots \\ y_n \\ y_{n+1} \end{bmatrix} = \mathbf{0}.$$

De aquí que $\widehat{\mathcal{C}} \subseteq \text{Nu}(\widehat{\mathcal{H}})$. Por otra parte, sea $\mathbf{c} \in \mathbb{F}_q^{n+1}$ tal que $\mathbf{c} \in \text{Nu}(\widehat{\mathcal{H}})$. Así, si $\mathbf{c} = c_1 \cdots c_{n+1}$ tenemos que $c_1 + \cdots + c_n + c_{n+1} = 0$ y $H(\mathbf{c}')^T = \mathbf{0}$, con $\mathbf{c}' = c_1 \cdots c_n$, luego $\mathbf{c} \in \widehat{\mathcal{C}}$. Por lo tanto, $\widehat{\mathcal{C}} = \text{Nu}(\widehat{\mathcal{H}})$. □

Corolario 2.75. Sea $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Entonces el código extendido $\widehat{\mathcal{C}}$ es un $[n + 1, k, d']$ código sobre $\mathbb{F}_q$, con $d' = d$ o $d + 1$.

Demostración. Es consecuencia del *Teorema 2.73* y la *Proposición 2.74*. □

Ejemplo 2.76. Sea $\mathcal{C}$ el tetracódigo. En los *Ejemplos 2.17* y *2.36* vimos que el tetracódigo es un $[4, 2, 3]$ código ternario con matriz generadora y de chequeo de paridad, respectivamente

$$G = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right] \quad y \quad H = \left[\begin{array}{cc|cc} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array} \right]$$

Sean A y B como en la prueba del *Teorema 2.73*. Note que $d(1120, 0112) \in A$ y $d(1011, 0112) \in B$. Por lo tanto, $d(\widehat{\mathcal{C}}) = 3$. Más aún, por el *Teorema 2.73*, $\widehat{\mathcal{C}}$ tiene 9 palabras. Así, $\dim(\widehat{\mathcal{C}}) = 2$. Como $10110, 01122 \in \widehat{\mathcal{C}}$ y ninguno es combinación lineal del otro tenemos que

$$\widehat{G} = \left[\begin{array}{ccccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 2 \end{array} \right]$$

es una matriz generadora para $\widehat{\mathcal{C}}$. Por la *Proposición 2.74*, una matriz de chequeo de paridad para $\widehat{\mathcal{C}}$ es

$$\widehat{H} = \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \end{array} \right]$$

■

Teorema 2.77. Sea $\mathcal{C}$ un código binario. Entonces $d(\mathbf{u}, \mathbf{v})$ es par, para todo $\mathbf{u}, \mathbf{v} \in \widehat{\mathcal{C}}$.

Demostración. Sean $\mathcal{C}$ un código binario de longitud n y $\mathbf{x} \in \widehat{\mathcal{C}}$. Entonces existe $\mathbf{y} = y_1 \cdots y_n \in \mathcal{C}$ tal que $\mathbf{x} = \widehat{\mathbf{y}}$. Así, $\mathbf{x} = y_1 \cdots y_n y_{n+1}$ con $y_1 + \cdots + y_n + y_{n+1} = 0$ y como $\mathcal{C}$ es binario tenemos que

$$\widehat{\mathbf{x}} \cdot \widehat{\mathbf{x}} = \sum_{i=1}^{n+1} y_i^2 = \sum_{i=1}^{n+1} y_i = 0.$$

Por el Teorema 2.33 iii) $wt(\widehat{\mathbf{x}}) \equiv \widehat{\mathbf{x}} \cdot \widehat{\mathbf{x}} \pmod{2}$, luego $wt(\widehat{\mathbf{x}})$ es par. Por lo tanto, para todo $\mathbf{u}, \mathbf{v} \in \widehat{\mathcal{C}}$

$$d(\mathbf{u}, \mathbf{v}) = wt(\mathbf{u}) + wt(\mathbf{v}) - 2wt(\mathbf{u} \cap \mathbf{v}),$$

es par. □

Ejemplo 2.78. Sea $\mathcal{C}$ un $[4, 2, 1]$ código binario con matriz generadora

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Como $10001 \in \widehat{\mathcal{C}}$ tenemos que $d(\widehat{\mathcal{C}}) \leq 2$. Por el Teorema 2.77, $d(\widehat{\mathcal{C}})$ es par. Por lo tanto, $d(\widehat{\mathcal{C}}) = 2$. ■

2.7 CODIFICACIÓN Y DECODIFICACIÓN

Teniendo en cuenta la Figura 1 analizaremos cómo enviar un mensaje a través de un canal de comunicación, qué sucede con el mensaje cuando el canal presenta ruido y cómo determina el decodificador (mediante la decodificación de máxima verosimilitud) qué mensaje fue enviado.

2.7.1 Codificación. La Figura 1 refleja que la *codificación* es una función que a cada mensaje proveniente de la fuente de mensajes le asigna una palabra código (de algún código fijo). Si el código no es lineal lo único que le pediremos a la codificación es que sea una función biyectiva entre mensajes y palabras código. En lo que sigue abordaremos el caso lineal.

Observación 2.79. Si $\mathcal{C}$ es un código que se usa para codificar ciertos mensajes entonces hay una correspondencia biunívoca entre los mensajes y palabras código de $\mathcal{C}$. Si $\mathcal{C}$ es no lineal se sigue por definición; si $\mathcal{C}$ es lineal se tiene como consecuencia del Corolario 2.82 y la Proposición 2.86.

Sea $\mathcal{C}$ un $[n, k]$ código sobre un cuerpo finito $\mathbb{F}_q$. Este código tiene q^k palabras código que estarán en correspondencia 1 a 1 con q^k mensajes. Como $\mathcal{C} \cong \mathbb{F}_q^k$ cada mensaje estará en correspondencia 1 a 1 con un vector $\mathbf{x} \in \mathbb{F}_q^k$. Por ende, trataremos los mensajes como vectores de $\mathbb{F}_q^k$.

La codificación del mensaje $\mathbf{x}$ puede hacerse ya sea usando una matriz generadora o una de chequeo de paridad para el código $\mathcal{C}$. Sin embargo, no cualquier matriz generadora o de chequeo de paridad para $\mathcal{C}$ nos será útil.

En primer lugar, ilustraremos el proceso que se sigue al usar una matriz generadora para $\mathcal{C}$, digamos G . En este caso, $\mathbf{x}$ se codifica como

$$\mathbf{c} = \mathbf{x}G.$$

Proposición 2.80. Sean $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y G una matriz generadora para $\mathcal{C}$. Si $\mathbf{x} = x_1 \cdots x_k$ está en $\mathbb{F}_q^k$ y $\mathbf{c} = \mathbf{x}G$ entonces $\mathbf{c} \in \mathcal{C}$.

Demostración. Sean $\mathbf{g}_1, \dots, \mathbf{g}_k$ las filas de G y $\mathbf{g}_i = g_{i1} \cdots g_{in}$ para todo $1 \leq i \leq k$. Entonces

$$\mathbf{c} = \mathbf{x}G = x_1 \cdots x_k \begin{bmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{bmatrix} = \begin{bmatrix} x_1 g_{11} + \cdots + x_k g_{k1} \\ \vdots \\ x_1 g_{1n} + \cdots + x_k g_{kn} \end{bmatrix} = x_1 \mathbf{g}_1 + \cdots + x_k \mathbf{g}_k.$$

□

Sean G una matriz generadora en forma estándar para un $[n, k]_q$ código $\mathcal{C}$ y $\mathbf{x} \in \mathbb{F}_q^k$, se puede verificar que las primeras k componentes de $\mathbf{c} = \mathbf{x}G$ son exactamente las k componentes de $\mathbf{x}$. Por lo que diremos que las primeras k componentes de $\mathbf{c}$ son las *componentes de información* de $\mathbf{x}$ y que las restantes $n - k$ componentes son las *componentes de chequeo de paridad*. Estos últimos son la *redundancia* que se le añade a $\mathbf{x}$ con el fin de ayudar a recuperar el mensaje si ocurren errores durante la transmisión. Si G no está en forma estándar pero tiene $i_1, i_2, \dots, i_k$ columnas tales que la matriz de tamaño $k \times k$ formada por dichas columnas es I_k , entonces la coordenada x_j de $\mathbf{x}$ se encuentra en la coordenada c_{i_j} de $\mathbf{c}$. Cuando esto sucede decimos que el codificador es *sistemático*. Claramente, si la matriz está en forma estándar el codificador es sistemático.

Cuando se define la codificación de un mensaje vía una matriz generadora se hace de forma general, es decir, se puede codificar con cualquier matriz generadora, incluso una que haga que el codificador no sea sistemático; sin embargo, la palabra código que se asigna a un mensaje mediante dicha matriz no contiene símbolos de información ni de redundancia, por lo cual no es viable trabajar con ella. Pero, ¿siempre es posible elegir una matriz generadora que haga que el codificador sea sistemático? La siguiente proposición muestra que sí.

Proposición 2.81. Sea $\mathcal{C}$ un $[n, k]$ código sobre un cuerpo finito $\mathbb{F}_q$ entonces $\mathcal{C}$ tiene una matriz generadora que hace que el codificador sea sistemático.

Demostración. Por el Corolario 2.6 el rango de G es k , así G tiene k columnas que forman un conjunto linealmente independiente. Por lo que mediante reducción por filas se puede obtener una matriz equivalente por filas a G que tenga k columnas con las que se pueda formar la matriz I_k . □

Corolario 2.82. La codificación asigna diferentes palabras código a diferentes mensajes.

Demostración. Supongamos que $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_q^k$ son distintos. Sea G una matriz generadora tal que el codificador es sistemático y supongamos que

$$\mathbf{c} = \mathbf{x}_1 G = \mathbf{x}_2 G. \quad (2.3)$$

Como $\mathbf{x}_1 \neq \mathbf{x}_2$, existe por lo menos una coordenada, digamos i , en la que ellos difieren. Sea x_{ti} la componente i -ésima de $\mathbf{x}_t$ para $t \in \{1, 2\}$, entonces $x_{1i} \neq x_{2i}$. Por (2.3) y por ser el codificador sistemático, existe una componente de $\mathbf{c}$, digamos j , tal que $c_j = x_{1i} = x_{2i}$, lo cual es una contradicción. □

Observación 2.83. Si estamos interesados en que el conjunto información se encuentre en las primeras k componentes pero el código $\mathcal{C}$ con el que estamos codificando no tiene una matriz generadora en forma estándar, entonces por el Teorema 2.54 podemos trabajar con un código lineal equivalente por permutaciones a $\mathcal{C}$ que tenga una matriz generadora en forma estándar.

Ejemplo 2.84. Consideremos el tetracódigo $\mathcal{C}$. Por el Ejemplo 2.17 una matriz generadora para $\mathcal{C}$ es

$$G = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right]$$

Se puede verificar que otra matriz generadora para $\mathcal{C}$ es

$$G_1 = \begin{bmatrix} 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 0 \end{bmatrix}$$

Ambas matrices hacen que el codificador sea sistemático. Al codificar mediante ambas matrices el vector $\mathbf{x} = 22 \in \mathbb{F}_3^2$ se obtiene, respectivamente, $\mathbf{c}_1 = 2210$ y $\mathbf{c}_2 = 2022$. ■

Observación 2.85. La codificación varía si se toman diferentes matrices generadoras para un mismo código.

Proposición 2.86. Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$ y sea G una matriz generadora para $\mathcal{C}$. Para cada $\mathbf{c} \in \mathcal{C}$ existe un vector $\mathbf{x} \in \mathbb{F}_q^k$ tal que

$$\mathbf{c} = \mathbf{x}G.$$

Demostración. Por el Corolario 2.6, las filas de G forman un conjunto linealmente independiente, lo que implica que G tiene inversa a derecha. Así, existe una matriz K de tamaño $n \times k$ con entradas en $\mathbb{F}_q$ tal que $GK = I_k$, luego $\mathbf{c}K = \mathbf{x}GK = \mathbf{x}I_k = \mathbf{x}$. □

Sean $\mathcal{C}$ un $[n, k]_q$ código y G una matriz generadora para $\mathcal{C}$ en forma estándar. Veamos cómo es el proceso para codificar un vector $\mathbf{x} = x_1 \cdots x_k \in \mathbb{F}_q^k$ usando la matriz de chequeo de paridad H para $\mathcal{C}$ que se obtiene mediante el Teorema 2.9. Por el Teorema 2.9, $H = [-A^T | I_{n-k}]$ siendo A una matriz de tamaño $k \times (n - k)$ con entradas $a_{ij} \in \mathbb{F}_q$. Sea $\mathbf{c} = c_1 \cdots c_n \in \mathbb{F}_q^n$ tal que $\mathbf{c} = \mathbf{x}G$. Nuestro objetivo es determinar las componentes de $\mathbf{c}$ sin calcular el producto $\mathbf{x}G$. Como G está en forma estándar tenemos que $c_i = x_i$ para todo $1 \leq i \leq k$. Así, nuestro objetivo se reduce a determinar las restantes $n - k$ componentes de $\mathbf{c}$, usando la matriz H . Por la Proposición 2.80, $\mathbf{c} \in \mathcal{C}$, luego

$$\mathbf{0} = H\mathbf{c}^T = \left[\begin{array}{ccc|cccc} -a_{11} & \cdots & -a_{k1} & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ -a_{1\ n-k} & \cdots & -a_{k\ n-k} & 0 & 0 & \cdots & 1 \end{array} \right] \begin{bmatrix} c_1 \\ \vdots \\ c_k \\ \vdots \\ c_n \end{bmatrix}$$

De donde obtenemos

$$\begin{cases} 0 = -\sum_{i=1}^k a_{i1}c_i + c_{k+1} \\ 0 = -\sum_{i=1}^k a_{i2}c_i + c_{k+2} \\ \vdots \\ 0 = -\sum_{i=1}^k a_{i(n-k)}c_i + c_n. \end{cases}$$

Lo cual permite determinar los $n - k$ símbolos de redundancia de $\mathbf{c}$, puesto que para todo $i = 1, \dots, k$ y $j = 1, \dots, n - k$, los elementos a_{ij} y c_i son conocidos. Más aún, la componente c_{k+j} de $\mathbf{c}$ es

$$c_{k+j} = \sum_{i=1}^k a_{ij}c_i.$$

Ejemplo 2.87. Consideremos el código $\mathcal{C}$, la matriz generadora G y el vector $\mathbf{x} = 22$ del Ejemplo 2.84. Sea $\mathbf{c} = \mathbf{x}G \in \mathbb{F}_3^4$, como G está en forma estándar tenemos que $\mathbf{c} = 22c_3c_4$. Ahora, por el Teorema 2.9 se sigue que

$$\mathbf{0} = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \\ c_3 \\ c_4 \end{bmatrix}$$

De aquí que $1 + 1 + c_3 = 0$ y $1 + 2 + c_4 = 0$. Por lo tanto, $c_3 = 1$ y $c_4 = 0$, es decir, $\mathbf{c} = 2210$. Observe que $\mathbf{c}$ es igual al vector $\mathbf{c}_1$ del *Ejemplo 2.84*. ■

2.7.2 Decodificación de máxima verosimilitud. Supongamos que el mensaje $\mathbf{x}$ se codifica como $\mathbf{c}$ y se envía a través de un canal de comunicación. El canal puede producir un ruido que altera $\mathbf{c}$, como muestra la *Figura 1*, por lo que conocer con exactitud la palabra código enviada no siempre es sencillo. La *decodificación* es un proceso que consiste precisamente en determinar qué palabra código $\mathbf{c}$ (y por ende qué mensaje $\mathbf{x}$) fue enviada cuando se recibe un vector $\mathbf{y}$.

Ahora bien, ¿cómo se refleja matemáticamente el ruido que produce el canal y que altera $\mathbf{c}$? Decimos que ocurren h errores en la transmisión de una palabra código $\mathbf{c}$ si se recibe un vector $\mathbf{y}$ tal que $d(\mathbf{y}, \mathbf{c}) = h$. Sea $\mathbf{e} = \mathbf{y} - \mathbf{c}$ entonces por el *Teorema 2.31*

$$wt(\mathbf{e}) = wt(\mathbf{y} - \mathbf{c}) = d(\mathbf{y}, \mathbf{c}).$$

Por lo tanto, el ruido en un canal de comunicación añade un *vector de error* $\mathbf{e}$ a la palabra código $\mathbf{c}$ haciendo que el decodificador reciba un vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$, más aún, el vector $\mathbf{e}$ es tal que su peso refleja la cantidad de errores que ocurren en la transmisión de $\mathbf{c}$.

Sean $\mathcal{C} \subseteq \mathbb{F}_q^n$ y t un entero positivo. Decimos que $\mathcal{C}$ es un código que *detecta a lo sumo t errores* si cada vez que ocurren entre 1 y t errores al enviar una palabra código de $\mathcal{C}$, el vector que se recibe no es una palabra código de $\mathcal{C}$, y decimos que $\mathcal{C}$ *detecta exactamente t errores* si es un código que detecta a lo sumo t errores pero no detecta a lo sumo $t + 1$, esto último significa que existen por lo menos dos palabras de $\mathcal{C}$ que difieren en $t + 1$ componentes.²

Teorema 2.88. Un código $\mathcal{C}$ detecta exactamente t errores si y solo si $d(\mathcal{C}) = t + 1$.

Demostración. Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$. En primer lugar, supongamos que $d(\mathcal{C}) = t + 1$, si $\mathbf{c}$ es una palabra código de $\mathcal{C}$ enviada a través de un canal con ruido, $\mathbf{x} \in \mathbb{F}_q^n$ es el vector recibido y $0 < d(\mathbf{c}, \mathbf{x}) \leq t$ entonces $0 < d(\mathbf{c}, \mathbf{x}) < d(\mathcal{C})$ y por la minimalidad de $\mathcal{C}$ se sigue que $\mathbf{x} \notin \mathcal{C}$, de aquí que $\mathcal{C}$ detecta a lo sumo t errores; por otra parte, la definición de distancia mínima garantiza que existen por lo menos dos palabras en $\mathcal{C}$ que difieren en $t + 1$ componentes. Por lo tanto, $\mathcal{C}$ detecta exactamente t errores.

Recíprocamente, si $\mathcal{C}$ detecta exactamente t errores entonces existen dos palabras de $\mathcal{C}$ que difieren en $t + 1$ componentes, así $d(\mathcal{C}) \leq t + 1$; por otra parte, sean $\mathbf{x}$ e $\mathbf{y}$ en $\mathcal{C}$ tales que $\mathbf{x} \neq \mathbf{y}$, si $1 \leq d(\mathbf{x}, \mathbf{y}) \leq t$ tendríamos que si se cometen $d(\mathbf{x}, \mathbf{y})$ errores al enviar la palabra $\mathbf{x}$, el vector recibido podría ser $\mathbf{y}$ pero esto contradice el hecho de que $\mathcal{C}$ detecta a lo sumo t errores, así $d(\mathbf{x}, \mathbf{y}) \geq t + 1$ y por ende $t + 1$ es una cota inferior del conjunto $\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}$, luego $d(\mathcal{C}) \geq t + 1$, lo que concluye la prueba. □

Observación 2.89. Sea $\mathcal{C}$ un código que detecta exactamente t errores. Si se envía una palabra de $\mathcal{C}$ a través de un canal con ruido y ocurren $t + 1$ errores durante la transmisión entonces el vector recibido puede o no, ser una palabra código de $\mathcal{C}$.

Ejemplo 2.90. Sean $\mathcal{C}_1$, $\mathcal{C}_2$ y $\mathcal{C}_3$ los códigos del *Ejemplo 2.28*. Por el *Teorema 2.88* $\mathcal{C}_1$ no detecta errores mientras que $\mathcal{C}_2$ y $\mathcal{C}_3$ detectan exactamente uno y dos errores, respectivamente. Ahora, supongamos que se envía la palabra $01101 \in \mathcal{C}_3$ y se cometen 3 errores durante la transmisión de tal forma que el vector que se recibe es $\mathbf{y} = 10001$, en este caso tenemos que el vector recibido no es una palabra código de $\mathcal{C}_3$, sin embargo, si el vector que se recibe es $\mathbf{y} = 11011$ tenemos que sí. ■

²Las definiciones relativas a detección y corrección de errores fueron tomadas de [7].

A continuación, diremos en qué consiste la decodificación de máxima verosimilitud. Sean $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código usado en la codificación de ciertos mensajes, $\mathbf{y} \in \mathbb{F}_q^n$ un vector recibido y $\mathbf{c} \in \mathcal{C}$ tal que

$$d(\mathbf{y}, \mathbf{c}) = \min \{d(\mathbf{y}, \mathbf{x}) : \mathbf{x} \in \mathcal{C}\}. \quad (2.4)$$

Si $\mathbf{c}$ es la única palabra código que satisface (2.4), la *decodificación de máxima verosimilitud* establece que $\mathbf{c}$ fue la palabra enviada; si existen varias palabras de $\mathcal{C}$ que satisfacen (2.4) entonces la decodificación de máxima verosimilitud escoge arbitrariamente una (y solo una) y decodifica a $\mathbf{y}$ como dicha palabra.

Sean $\mathcal{C} \subseteq \mathbb{F}_q^n$ y t un entero positivo. Decimos que $\mathcal{C}$ es un código que *corrige a lo sumo t errores* (mediante la decodificación de máxima verosimilitud) si cada vez ocurren entre 1 y t errores al enviar una palabra código $\mathbf{c} \in \mathcal{C}$, el vector recibido $\mathbf{y}$ satisface que $d(\mathbf{c}', \mathbf{y}) > d(\mathbf{y}, \mathbf{c})$ para todo $\mathbf{c}' \in \mathcal{C}$ con $\mathbf{c}' \neq \mathbf{c}$; y decimos que $\mathcal{C}$ *corrige exactamente t errores* si es un código que corrige a lo sumo t errores y si existen $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ e $\mathbf{x} \in \mathbb{F}_q^n$ con $\mathbf{c}_1 \neq \mathbf{c}_2$ tales que $d(\mathbf{x}, \mathbf{c}_1) = t + 1$ y $d(\mathbf{x}, \mathbf{c}_2) \leq d(\mathbf{x}, \mathbf{c}_1)$.

Observación 2.91. Sea $\mathcal{C}$ un código que corrige a lo sumo t errores. Si se envía una palabra $\mathbf{c}$ de $\mathcal{C}$ a través de un canal con ruido y ocurren entre 1 y t errores durante la transmisión, es decir, si se recibe $\mathbf{y} \in \mathbb{F}_q^n$ tal que $1 \leq d(\mathbf{y}, \mathbf{c}) \leq t$ entonces la decodificación de máxima verosimilitud determina que la palabra enviada fue $\mathbf{c}$, es decir decodifica $\mathbf{y}$ de manera única y correcta.

A continuación, vamos a introducir el concepto de bola cerrada, el cual nos permitirá establecer una relación entre la capacidad para corregir errores de un código y su distancia mínima.

La *bola cerrada* centrada en $\mathbf{u} \in \mathbb{F}_q^n$ de radio r , con r un entero no negativo, se define como el conjunto

$$\overline{B}_r(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_q^n : d(\mathbf{u}, \mathbf{v}) \leq r\},$$

formado por todos los vectores en $\mathbb{F}_q^n$ cuya distancia a $\mathbf{u}$ es menor o igual que r .

Proposición 2.92. El número de vectores en una bola cerrada centrada en un elemento de $\mathbb{F}_q^n$ de radio r , con $0 \leq r \leq n$, es

$$\sum_{i=0}^r \binom{n}{i} (q-1)^i.$$

Demostración. Sea $\mathbf{u} \in \mathbb{F}_q^n$. Analicemos cuántos vectores $\mathbf{v}$ distan de $\mathbf{u}$ exactamente m unidades, donde $0 \leq m \leq n$. Las m posiciones en las cuales $\mathbf{u}$ y $\mathbf{v}$ difieren pueden ser elegidas de $\binom{n}{m}$ maneras distintas y en cada una de ellas, m posiciones de $\mathbf{v}$ pueden ser tomadas de $q-1$ maneras para diferir de la correspondiente entrada de $\mathbf{u}$. Así, el número de vectores que distan exactamente m unidades de $\mathbf{u}$ es $\binom{n}{m}(q-1)^m$. Por lo tanto, el número total de vectores en $\overline{B}_r(\mathbf{u})$ es

$$\sum_{i=0}^r \binom{n}{i} (q-1)^i.$$

□

Denotaremos por $V_q(n, a)$ al número de vectores en una bola cerrada de radio a centrada en algún vector de $\mathbb{F}_q^n$, en virtud de la proposición anterior

$$V_q(n, a) = \sum_{i=0}^a \binom{n}{i} (q-1)^i. \quad (2.5)$$

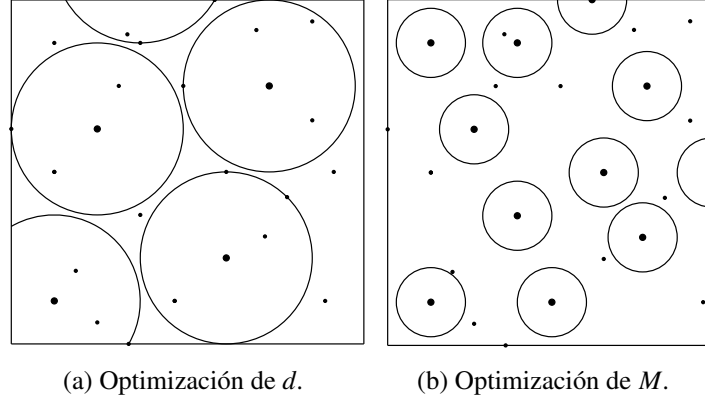


Figura 2.2: Optimización de parámetros.

Observación 2.93. En adelante $\lfloor \cdot \rfloor$ denotará la función parte entera.

Teorema 2.94. Si $d > 0$ es la distancia mínima de un código $\mathcal{C}$ y $t = \lfloor (d-1)/2 \rfloor$ entonces las bolas cerradas de radio t centradas en distintas palabras código son disjuntas dos a dos.

Demostración. Sean $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ con $\mathbf{c}_1 \neq \mathbf{c}_2$ y $\mathbf{z} \in \overline{B}_t(\mathbf{c}_1) \cap \overline{B}_t(\mathbf{c}_2)$. Luego, $d(\mathbf{z}, \mathbf{c}_1) \leq t$, $d(\mathbf{z}, \mathbf{c}_2) \leq t$ y por desigualdad triangular

$$d(\mathbf{c}_1, \mathbf{c}_2) \leq d(\mathbf{c}_1, \mathbf{z}) + d(\mathbf{z}, \mathbf{c}_2) \leq 2t = 2 \left\lfloor \frac{d-1}{2} \right\rfloor \leq \frac{2(d-1)}{2} < d,$$

de aquí que $d(\mathbf{c}_1, \mathbf{c}_2) = 0$, así $\mathbf{c}_1 = \mathbf{c}_2$ lo cual es una contradicción. $\square$

Corolario 2.95. Sean $\mathcal{C}$ un código con distancia mínima $d > 0$ y $t = \lfloor (d-1)/2 \rfloor$. Entonces $\mathcal{C}$ corrige exactamente t errores.

Demostración. Supongamos que al enviar una palabra código $\mathbf{c}$ de $\mathcal{C}$ a través de una canal con ruido se cometen entre 1 y t errores de tal manera que se recibe $\mathbf{y} \in \mathbb{F}_q^n$, así $1 \leq d(\mathbf{y}, \mathbf{c}) \leq t$, luego $\mathbf{y} \in \overline{B}_t(\mathbf{c})$ y por el Teorema 2.94 tenemos que $d(\mathbf{y}, \mathbf{c}') > t$ para todo $\mathbf{c}' \in \mathcal{C}$ con $\mathbf{c}' \neq \mathbf{c}$, por transitividad se sigue que $\mathcal{C}$ corrige a lo sumo t errores.

Por otra parte, sean $\mathbf{c} = c_1 \cdots c_n$ y $\mathbf{c}' = c'_1 \cdots c'_n$ en $\mathcal{C}$ tales que $d(\mathbf{c}, \mathbf{c}') = d$ e $i_1, \dots, i_d$ tales que $c_{i_j} \neq c'_{i_j}$ para todo $1 \leq j \leq d$ y si $j_1 < j_2$ entonces $i_{j_1} < i_{j_2}$. Se puede verificar fácilmente que $t+1 < d$. Sea $\mathbf{y} = y_1 \cdots y_n$ el vector en $\mathbb{F}_q^n$ dado por

$$y_s = \begin{cases} c_s & \text{si } c_s = c'_s \\ c'_s & \text{si } c_s \neq c'_s, c_s = c_{i_j} \text{ y } j \leq t+1 \\ c_s & \text{en caso contrario} \end{cases}$$

para todo $1 \leq s \leq n$. De esta manera $d(\mathbf{y}, \mathbf{c}) = t+1$ y $d(\mathbf{y}, \mathbf{c}') = d - (t+1)$. Dado que $d \leq 2(t+1)$ se sigue que $d(\mathbf{y}, \mathbf{c}') = d - (t+1) \leq t+1 = d(\mathbf{y}, \mathbf{c})$. Por lo tanto, $\mathcal{C}$ corrige exactamente t errores. $\square$

Ejemplo 2.96. Por el Corolario 2.95, el código $\mathcal{C}_3$ del Ejemplo 2.28 corrige exactamente un error. $\blacksquare$

Observación 2.97. Sean n y M enteros positivos, $\mathbb{F}_q$ un cuerpo finito y fijemos todos los códigos sobre $\mathbb{F}_q$ de longitud n que tengan M palabras. De todos estos posibles subconjuntos de $\mathbb{F}_q^n$ con cardinal M , el

que mayor distancia mínima d tenga nos permitirá, por el *Corolario 2.95*, corregir más errores que los otros códigos.

Por otra parte, supongamos que uno de los parámetros fijos no es M sino d y que fijamos todos los códigos sobre $\mathbb{F}_q$ de longitud n que tienen distancia mínima d . De esta manera t es un valor fijo y por el *Corolario 2.95* cualquiera de estos códigos va a corregir exactamente t errores. Ahora bien, entre más palabras tenga un código más bolas cerradas centradas en palabras código de radio t hay y por ende más vectores recibidos pueden ser decodificados correctamente. Por lo tanto, de todos los posibles subconjuntos de $\mathbb{F}_q^n$ con distancia mínima d , el que mayor cantidad de palabras tenga nos permitirá decodificar correctamente una mayor cantidad de vectores.

La *Figura 2.2* ejemplifica la observación anterior. En 2.2a y 2.2b se tienen los mismos puntos, los cuales representan vectores de un espacio vectorial $\mathbb{F}_q^n$. En 2.2a se fija la cantidad de palabras códigos y en 2.2a se fija la distancia mínima.

3

COTAS EN EL TAMAÑO DE LOS CÓDIGOS

En este capítulo vamos a establecer cuál es el principal problema de la teoría de códigos y vamos a estudiar cotas, tanto superiores como inferiores, para los parámetros de un código. Nuestra referencia será el segundo capítulo de [2].

3.1 EL PRINCIPAL PROBLEMA EN LA TEORÍA DE CÓDIGOS

Al transmitir mensajes hay tres aspectos que se pretenden optimizar. En primer lugar, buscamos *rapidez* en la transmisión; en segundo lugar, nos interesa enviar una amplia *variedad* de mensajes; y, finalmente, si hay lugar a errores durante el proceso, deseamos *detectar* y *corregir* la mayor cantidad posible de estos.

De la *Observación 2.79*, se sigue que la rapidez en la transmisión, es decir, la rapidez con que se transmite un mensaje, equivale a la celeridad con que se envía la palabra código que se use para codificarlo; la cual depende de su longitud. Por ejemplo, un vector de longitud 120 se enviará más rápido que uno de longitud 700000000. En este orden de ideas, podría pensarse que lo ideal es usar en la codificación, un código de longitud 1 sobre algún cuerpo finito. El problema con este código, es que de ocurrir algún error ocasionado por el ruido durante la transmisión, el vector recibido sería una palabra código, por lo que el receptor no tendría manera de reconocer que se ha producido un error. En otras palabras, este código permite enviar mensajes lo más rápido posible pero no detecta y mucho menos corrige errores; por ende, no proporciona confiabilidad. En general, ninguno de nuestros tres aspectos de interés se optimiza de manera independiente, es decir, sin tener en cuenta los otros dos.

Así como la rapidez en la transmisión se relaciona directamente con uno de los parámetros del código $\mathcal{C}$ que se use en la codificación, a saber la longitud; también se puede afirmar, de nuevo por la *Observación 2.79*, que la variedad de mensajes que se transmiten depende de la cantidad de palabras código de $\mathcal{C}$. Por otra parte, el *Corolario 2.95* relaciona la capacidad de corregir errores que hayan ocurrido durante la transmisión, mediante la decodificación de máxima verosimilitud, con la distancia mínima de $\mathcal{C}$.

Diremos que un (n, M, d) código sobre algún cuerpo finito $\mathbb{F}_q$ es un *buen código* si tiene una longitud n pequeña, una cantidad de palabras M grande y una distancia mínima d grande; entendiendo por supuesto que los conceptos de pequeñez y grandeza son relativos. Así las cosas, estamos interesados en encontrar buenos códigos; ya que estos nos permiten codificar una amplia gama de mensajes, además nos garantizan rapidez y confiabilidad al enviarlos mediante un canal con posible ruido.

El *principal problema en la teoría de códigos* consiste en fijar tanto un cuerpo finito como dos de los parámetros que tiene un código sobre este cuerpo y optimizar el tercero. Por ejemplo, la *Observación*

2.97 muestra qué entendemos por optimizar la distancia mínima cuando se han fijado $\mathbb{F}_q, n$ y M . El problema usual y el que consideraremos consiste en optimizar la cantidad de palabras una vez fijados $\mathbb{F}_q, n$ y d ; la *Observación 2.97* muestra que optimizar este parámetro equivale a encontrar el mayor entero positivo M tal que (n, M, d) sea un código sobre $\mathbb{F}_q$.

3.2 $A_q(n, d)$ y $B_q(n, d)$

Sea

$$A_q(n, d) := \max \{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) = d \},$$

el mayor entero positivo M para el cual existe un código en $\mathbb{F}_q^n$ con M palabras y distancia mínima d . Análogamente, definimos

$$B_q(n, d) := \max \{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código lineal con } d(\mathcal{C}) = d \}.$$

Dados q, n y d ¿siempre es posible encontrar un código lineal con dichos parámetros? ¿siempre tiene sentido hablar tanto de $A_q(n, d)$ como de $B_q(n, d)$? La siguiente proposición da respuesta a estas preguntas. Además establece la relación entre $A_q(n, d)$ y $B_q(n, d)$, y da el valor de $A_q(n, d)$ cuando d es 1 o n .

Proposición 3.1.

- i) $B_q(n, 0) = 1$ y $B_q(n, d) \geq q$ si $d > 0$.
- ii) $B_q(n, d) \leq A_q(n, d)$ y $B_q(n, d)$ es una potencia entera no negativa de q .
- iii) $A_q(n, 1) = q^n$ y $A_q(n, n) = q$.

Demostración.

- i) El único código de longitud n sobre $\mathbb{F}_q$ con distancia mínima 0 es el código lineal trivial de $\mathbb{F}_q^n$. Por lo tanto, $B_q(n, 0) = 1$. Por otra parte, sean $\mathbf{c} \in \mathbb{F}_q^n$ un vector de peso $d > 0$ y $\mathcal{C} = \{\alpha \mathbf{c} : \alpha \in \mathbb{F}_q\}$. $\mathcal{C}$ es un $[n, 1, d]$ código sobre $\mathbb{F}_q$ y por ende, $B_q(n, d) \geq q$.
- ii) Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código lineal con distancia mínima d y $M = B_q(n, d)$ palabras. Entonces $A_q(n, d) \geq M$ y $M = q^k$, donde $k = \dim(\mathcal{C})$.
- iii) Dado que $d(\mathbb{F}_q^n) = 1$ tenemos que $A_q(n, 1) = q^n$. Supongamos $d = n$. Sabemos que el código de repetición q -ario de longitud n es un (n, q, n) código sobre $\mathbb{F}_q$ luego $A_q(n, n) \geq q$. Sea $\mathcal{C}$ un (n, M, n) código sobre $\mathbb{F}_q$, como $d = n$ tenemos que cualesquiera dos palabras en $\mathcal{C}$ deben diferir en todas sus componentes. Así, si fijamos una palabra $\mathbf{c} = c_1 \cdots c_n \in \mathcal{C}$ y alguna de sus componentes, la primera por ejemplo, tenemos que $c'_1 \neq c_1$, para todo $\mathbf{c}' = c'_1 \cdots c'_n \in \mathcal{C}$ con $\mathbf{c}' \neq \mathbf{c}$.

Ahora bien, hay $q-1$ elementos de $\mathbb{F}_q$ distintos de c_1 luego, hay a lo más $q-1$ palabras en $\mathcal{C}$ distintas a $\mathbf{c}$ y por ende $M \leq q$. Así, q es una cota superior de $\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) = n \}$, lo cual implica que $A_q(n, n) \leq q$ y por tanto, $A_q(n, n) = q$.

□

En algunos textos, $A_q(n, d)$ se define como el mayor entero positivo M para el cual existe un código en $\mathbb{F}_q^n$ con M palabras y distancia mínima al menos $d > 0$. De forma análoga en el caso lineal. La *Proposición 3.4* muestra que ambas definiciones son equivalentes.

Lema 3.2. Si $0 < d < d'$ entonces $A_q(n, d') \leq A_q(n, d)$.¹

Demostración. Sean $\mathcal{C}'$ un (n, M, d') código sobre $\mathbb{F}_q$ con $M = A_q(n, d')$ y $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}'$ tales que $d(\mathbf{x}, \mathbf{y}) = d'$. Sean $i_1, \dots, i_{d'}$ tales que $x_{i_j} \neq y_{i_j}$, para todo $1 \leq j \leq d'$. Consideremos $\sigma \in S_n$ tal que $\sigma(i_j) = j$ para todo $1 \leq j \leq d'$ y el conjunto

$$\mathcal{C}_p = \{\mathbf{c}\sigma : \mathbf{c} \in \mathcal{C}'\}.$$

Por el Teorema 2.50, $\mathcal{C}_p$ es un (n, M, d') código sobre $\mathbb{F}_q$. Además

$$\mathbf{x}\sigma = x_{i_1} \cdots x_{i_{d'}} x_{\sigma^{-1}(d'+1)} \cdots x_{\sigma^{-1}(n)} \quad \text{y} \quad \mathbf{y}\sigma = y_{i_1} \cdots y_{i_{d'}} y_{\sigma^{-1}(d'+1)} \cdots y_{\sigma^{-1}(n)}.$$

Así, $d(\mathbf{x}\sigma, \mathbf{y}\sigma) = d'$ y $\mathbf{x}\sigma = x_{i_1} \cdots x_{i_{d'}} y_{\sigma^{-1}(d'+1)} \cdots y_{\sigma^{-1}(n)}$. Observe que $d(\mathbf{x}', \mathbf{y}\sigma) = d$, donde $\mathbf{x}' = x_{i_1} \cdots x_{i_d} y_{i_{d+1}} \cdots y_{i_{d'}} y_{\sigma^{-1}(d'+1)} \cdots y_{\sigma^{-1}(n)} \in \mathbb{F}_q^n$. De aquí que, $\mathbf{x}' \notin \mathcal{C}_p$ y

$$\mathcal{C} = (\mathcal{C}_p \setminus \{\mathbf{x}\sigma\}) \cup \{\mathbf{x}'\},$$

es un código sobre $\mathbb{F}_q$ con longitud n y M palabras. Veamos que $d(\mathcal{C}) = d$. Como $\mathbf{y}\sigma, \mathbf{x}' \in \mathcal{C}$ y $d(\mathbf{x}', \mathbf{y}\sigma) = d$ tenemos que $d(\mathcal{C}) \leq d$. Supongamos que $d(\mathcal{C}) < d$ y sean $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, tales que $d(\mathbf{u}, \mathbf{v}) = d(\mathcal{C})$. Consideremos los siguientes casos:

- i) Si $\mathbf{u}, \mathbf{v} \in \mathcal{C}_p \setminus \{\mathbf{x}\sigma\}$, entonces $0 < d(\mathbf{u}, \mathbf{v}) < d < d'$, lo cual contradice que $d' = d(\mathcal{C}_p)$.
- ii) Sin pérdida de generalidad, supongamos que $\mathbf{u} \in \mathcal{C}_p \setminus \{\mathbf{x}\sigma\}$ y que $\mathbf{v} = \mathbf{x}'$. Por la desigualdad triangular tenemos que

$$d(\mathbf{u}, \mathbf{x}\sigma) \leq d(\mathbf{u}, \mathbf{x}') + d(\mathbf{x}\sigma, \mathbf{x}') = d(\mathbf{u}, \mathbf{v}) + (d' - d) < d + (d' - d) = d'.$$

Por otra parte, como $\mathbf{u}, \mathbf{x}\sigma \in \mathcal{C}_p$ y son distintos, tenemos que $d(\mathbf{u}, \mathbf{x}\sigma) \geq d'$, lo cual es una contradicción.

Así, $d(\mathcal{C}) = d$ y por lo tanto, $A_q(n, d) \geq M$. □

Lema 3.3. Si $0 < d < d'$ entonces $B_q(n, d') \leq B_q(n, d)$.

Demostración. Sean $\mathcal{C}'$ un $[n, k, d']$ código sobre $\mathbb{F}_q$ con $k = B_q(n, d')$ y $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}'$ tal que $wt(\mathbf{x}) = d'$. Sean $i_1, \dots, i_{d'}$ tales que $x_{i_j} \neq 0$, para todo $1 \leq j \leq d'$. Consideremos $\sigma \in S_n$ tal que $\sigma(i_j) = j$ para todo $1 \leq j \leq d'$ y el conjunto

$$\mathcal{C}_p = \{\mathbf{c}\sigma : \mathbf{c} \in \mathcal{C}'\}.$$

Por el Corolario 2.52, $\mathcal{C}_p$ es un $[n, k, d']$ código sobre $\mathbb{F}_q$. Además

$$\mathbf{x}\sigma = x_{i_1} \cdots x_{i_{d'}} x_{\sigma^{-1}(d'+1)} \cdots x_{\sigma^{-1}(n)}.$$

Así, $wt(\mathbf{x}\sigma) = d'$, $\mathbf{x}\sigma = x_{i_1} \cdots x_{i_{d'}} 0 \cdots 0$ y $wt(\mathbf{x}') = d$, con $\mathbf{x}' = x_{i_1} \cdots x_{i_d} 0 \cdots 0 \in \mathbb{F}_q^n$. De aquí que, $\mathbf{x}' \notin \mathcal{C}_p$. Completamos el conjunto $\{\mathbf{x}\sigma\}$ a una base $\{\mathbf{x}\sigma, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ de $\mathcal{C}_p$. Sea

$$\mathcal{C} = \text{Gen}\{\mathbf{x}', \mathbf{v}_2, \dots, \mathbf{v}_k\}.$$

Como $\{\mathbf{v}_2, \dots, \mathbf{v}_k\}$ es linealmente independiente y $\mathbf{x}' \notin \mathcal{C}_p$, tenemos que $\dim(\mathcal{C}) = k$. Así, $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_q$ de longitud n y dimensión k . Veamos que $d(\mathcal{C}) = d$. Como $\mathbf{x}' \in \mathcal{C}$, $d(\mathcal{C}) \leq d$. Supongamos que $d(\mathcal{C}) < d$. Sea $\mathbf{y} \in \mathcal{C}$ tal que $wt(\mathbf{y}) = d(\mathcal{C})$. Sean $\lambda, \alpha_2, \dots, \alpha_k \in \mathbb{F}_q$ tales que

¹La idea para esta prueba fue tomada de [5].

$\mathbf{y} = \lambda \mathbf{x}' + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_k \mathbf{v}_k$. Si $\lambda = 0$ entonces $\mathbf{y} \in \mathcal{C}_p$ y por ende, $d' \leq wt(\mathbf{y}) < d$, lo cual es una contradicción. Por lo tanto, $\lambda \neq 0$. Sea $\mathbf{c} = \alpha_2 \mathbf{v}_2 + \cdots + \alpha_k \mathbf{v}_k$. Luego, $\mathbf{c} \in \mathcal{C}_p$, $\mathbf{c} \neq \mathbf{x}\sigma$ y

$$wt(\mathbf{y}) = wt(\mathbf{c} + \lambda \mathbf{x}') = d(\mathbf{c}, -\lambda \mathbf{x}').$$

Por la desigualdad triangular y por ser $\lambda \neq 0$ tenemos que

$$d(\mathbf{c}, \mathbf{x}\sigma) \leq d(\mathbf{c}, -\lambda \mathbf{x}') + d(-\lambda \mathbf{x}', \mathbf{x}\sigma) = wt(\mathbf{y}) + (d' - d) < d + (d' - d) = d'.$$

Por otra parte, como $\mathbf{c}, \mathbf{x}\sigma \in \mathcal{C}_p$ y son distintos, tenemos que $d(\mathbf{c}, \mathbf{x}\sigma) \geq d'$, lo cual es una contradicción. Luego, $d(\mathcal{C}) = d$ y por lo tanto $B_q(n, d) \geq q^k$. $\square$

Proposición 3.4. Si $d > 0$ entonces

$$A_q(n, d) = \max \left\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) \geq d \right\},$$

y

$$B_q(n, d) = \max \left\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código lineal con } d(\mathcal{C}) \geq d \right\}.$$

Demostración. Note que

$$\left\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) \geq d \right\} = \bigcup_{d' \geq d} \left\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) = d' \right\}.$$

Luego,

$$\max \left\{ |\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) \geq d \right\} = \max \left\{ A_q(n, d), \dots, A_q(n, n) \right\}.$$

Por el Lema 3.2, $\max \left\{ A_q(n, d), \dots, A_q(n, n) \right\} = A_q(n, d)$, lo que concluye la primera parte de la prueba. Para $B_q(n, d)$ se sigue el mismo razonamiento usando el Lema 3.3. $\square$

Finalizamos esta sección presentando algunos resultados conocidos para $A_q(n, d)$ y $B_q(n, d)$.

Proposición 3.5. Sea $d > 1$. Entonces

- i) $A_q(n, d) \leq A_q(n-1, d-1)$ y $B_q(n, d) \leq B_q(n-1, d-1)$.
- ii) Si d es par, $A_2(n, d) = A_2(n-1, d-1)$ y $B_2(n, d) = B_2(n-1, d-1)$.
- iii) Si d es par y $M = A_2(n, d)$, existe un (n, M, d) código binario par tal que la distancia entre cualesquiera dos palabras es par.

Demostración.

- i) Sean $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ con $M = A_q(n, d)$, $\mathbf{x} = x_1 \cdots x_n$ e $\mathbf{y} = y_1 \cdots y_n$ en $\mathcal{C}$ tales que $d(\mathbf{x}, \mathbf{y}) = d$ e $i \in \{1, \dots, n\}$ tal que $x_i \neq y_i$. Por la Proposición 2.63 i) $(\mathcal{C})_i^*$ es un $(n-1, M, d-1)$ código sobre $\mathbb{F}_q$. Por lo tanto, $A_q(n-1, d-1) \geq M$.

Sean $\mathcal{C}'$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ con $B_q(n, d) = q^k$, $\mathbf{c} = c_1 \cdots c_n \in \mathcal{C}'$ tal que $wt(\mathbf{c}) = d$ e $i \in \{1, \dots, n\}$ tal que $c_i \neq 0$. Por el Teorema 2.65 i), $\mathcal{C}'_i^*$ es un $[n-1, k, d-1]$ código sobre $\mathbb{F}_q$. Por lo tanto, $B_q(n-1, d-1) \geq q^k$.

- ii) Por i) resta verificar que $A_2(n, d) \geq A_2(n-1, d-1)$ y que $B_2(n, d) \geq B_2(n-1, d-1)$. Sea $\mathcal{C}$ un $(n-1, M, d-1)$ código binario con $M = A_2(n-1, d-1)$. Luego, por el Teorema 2.73, $\widehat{\mathcal{C}}$ es un (n, M, d') código binario con $d' = d-1$ o d . Como $\mathcal{C}$ es binario, el Teorema 2.77 garantiza que d' es par puesto que d es par por hipótesis, concluimos que $\widehat{\mathcal{C}}$ es un (n, M, d) código binario. Por lo tanto, $A_2(n, d) \geq M$. En el caso lineal se sigue un razonamiento análogo, teniendo en cuenta el Corolario 2.75.

iii) Es consecuencia de i) y ii)

□

Corolario 3.6. $A_2(n, 2) = B_2(n, 2) = 2^{n-1}$.

Demostración. Es consecuencia de las *Proposiciones* 3.1 y 3.5.

□

Teorema 3.7. Para $n \geq 2$ y $d < n$ se cumple que

$$A_q(n, d) \leq qA_q(n-1, d) \quad \text{y} \quad B_q(n, d) \leq qB_q(n-1, d).$$

Demostración. Si $d = 0$, entonces por la *Proposición* 3.1 se tiene el resultado. Supongamos que $d > 0$ y analicemos primero el caso lineal. Sean $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ tal que $q^k = B_q(n, d)$ y $\mathbf{x} \in \mathcal{C}$ una palabra de peso mínimo d , como $d < n$ se sigue que $\mathbf{x}$ tiene por lo menos una componente nula. Sea $1 \leq i \leq n$ una posición en que $\mathbf{x}$ tiene una componente nula. Por facilidad en los cálculos que haremos más adelante, trabajaremos con un código equivalente por permutación a $\mathcal{C}$. Sean $\sigma = (1, i) \in S_n$ y

$$\mathcal{C}_p = \{\mathbf{u}\sigma : \mathbf{u} \in \mathcal{C}\}.$$

Por el *Corolario* 2.52, $\mathcal{C}_p$ es un $[n, k, d]_q$ código que tiene una palabra de peso mínimo d , digamos $\mathbf{y}$, de la forma $\mathbf{y} = 0y_2 \cdots y_n$. Consideremos el siguiente subconjunto de $\mathcal{C}_p$:

$$\mathcal{C}_p(0) := \{\mathbf{c} \in \mathcal{C}_p : \mathbf{c} = 0c_2 \cdots c_n\}.$$

Si $\mathcal{C}_p(0) = \mathcal{C}_p$, entonces $\mathcal{C}_p(0)$ es lineal con los mismos parámetros de $\mathcal{C}_p$. Como la primera componente de todas las palabras de $\mathcal{C}_p(0)$ es igual a 0 se sigue, por el *Teorema* 2.65 i) que $(\mathcal{C}_p(0))_1^*$ es un $[n-1, k, d]_q$ código, luego $B_q(n-1, d) \geq q^k$, de aquí que

$$B_q(n, d) = q^k < qq^k \leq qB_q(n-1, d).$$

Supongamos ahora que $\mathcal{C}_p(0)$ está contenido estrictamente en $\mathcal{C}_p$, esto implica que $k \neq 1$. En efecto, si $k = 1$, entonces

$$\mathcal{C}_p = \{\alpha\mathbf{y} : \alpha \in \mathbb{F}_q\} = \{0(\alpha y_2) \cdots \alpha y_n : \alpha \in \mathbb{F}_q\}.$$

De aquí que $\mathcal{C}_p \subseteq \mathcal{C}_p(0)$ y por ende $\mathcal{C}_p(0) = \mathcal{C}_p$, lo cual contradice que $\mathcal{C}_p(0) \neq \mathcal{C}_p$. Más aún, como $d > 0$ y $k \neq 1$ entonces por la *Proposición* 3.1 $k > 1$.

Veamos que $\mathcal{C}_p(0)$ es lineal. Como $\mathbf{y} \in \mathcal{C}_p(0)$ tenemos que $\mathcal{C}_p(0) \neq \emptyset$. Sean $\mathbf{u}, \mathbf{v} \in \mathcal{C}_p(0)$ y $\alpha \in \mathbb{F}_q$ luego, $\mathbf{u} = 0u_2 \cdots u_n$, $\mathbf{v} = 0v_2 \cdots v_n \in \mathcal{C}_p$, así y por ser $\mathcal{C}_p$ lineal tenemos que

$$\alpha\mathbf{u} + \mathbf{v} = 0(\alpha u_2 + v_2) \cdots \alpha u_n + v_n \in \mathcal{C}_p.$$

Analicemos los parámetros de $\mathcal{C}_p(0)$. Es claro que su longitud es n , como $\mathbf{y} \in \mathcal{C}_p(0)$ se sigue que $d(\mathcal{C}_p(0)) \leq d$. Si $d(\mathcal{C}_p(0)) < d$ tendríamos que existe en $\mathcal{C}_p$ una palabra no nula de peso menor a d pero esto no puede ser y por lo tanto $d(\mathcal{C}_p(0)) = d$. Para determinar la dimensión de $\mathcal{C}_p(0)$ construiremos una matriz generadora para $\mathcal{C}_p(0)$ a partir de una matriz generadora para $\mathcal{C}_p$. Si

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

es una matriz generadora para $\mathcal{C}_p$ entonces aplicar reducción Gaussiana a G , obtenemos una matriz generadora G' para $\mathcal{C}_p$ de la forma

$$G' = \begin{bmatrix} 1 & g'_{12} & \cdots & g'_{1n} \\ 0 & g'_{22} & \cdots & g'_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & g'_{k2} & \cdots & g'_{kn} \end{bmatrix}$$

Es importante resaltar que la componente $(1, 1)$ de G' es no nula ya que $\mathcal{C}_p(0) \neq \mathcal{C}_p$. Más aún, como $k > 1$, tanto G como G' tienen más de una fila.

Como G' es una matriz generadora para $\mathcal{C}_p$ toda palabra en $\mathcal{C}_p$ se puede expresar como combinación lineal de sus filas. En particular, dado $\mathbf{c} = 0c_2 \cdots c_n \in \mathcal{C}_p(0)$ existen $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{F}_q$ tales que

$$\begin{bmatrix} 0 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \alpha_1 \begin{bmatrix} 1 \\ g'_{12} \\ \vdots \\ g'_{1n} \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ g'_{22} \\ \vdots \\ g'_{2n} \end{bmatrix} + \cdots + \alpha_k \begin{bmatrix} 0 \\ g'_{k2} \\ \vdots \\ g'_{kn} \end{bmatrix}.$$

De aquí que $\alpha_1 = 0$, así que toda palabra de $\mathcal{C}_p(0)$ se puede escribir como combinación lineal de las últimas $k - 1$ filas de G' . El conjunto formado por dichas filas es linealmente independiente y por lo tanto

$$\begin{bmatrix} 0 & g'_{22} & \cdots & g'_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & g'_{k2} & \cdots & g'_{kn} \end{bmatrix}$$

es una matriz generadora para $\mathcal{C}_p(0)$, lo cual indica que la dimensión de $\mathcal{C}_p(0)$ es $k - 1$.

En resumen, si $\mathcal{C}_p(0) \neq \mathcal{C}_p$ entonces $\mathcal{C}_p(0)$ es un $[n, k - 1, d]$ código sobre lineal $\mathbb{F}_q$ con $k > 1$. A partir de $\mathcal{C}_p(0)$ construiremos un código sobre $\mathbb{F}_q$ con los mismos parámetros, exceptuando la longitud, la cual será $n - 1$. Dado que la primera componente de cada palabra de $\mathcal{C}_p(0)$ es igual a 0 se sigue, por el Teorema 2.65 i) que $(\mathcal{C}_p(0))^*_1$ es un $[n - 1, k - 1, d]_q$ código, así, $B_q(n - 1, d) \geq q^{k-1}$ y

$$B_q(n, d) = q^k = qq^{k-1} \leq qB_q(n - 1, d).$$

Resta verificar el caso no lineal. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ tal que $M = A_q(n, d)$. Para cada $\alpha \in \mathbb{F}_q$ sea

$$\mathcal{C}(\alpha) = \{\mathbf{c} \in \mathcal{C} : \mathbf{c} = \alpha c_2 \cdots c_n\}.$$

De esta forma

$$\mathcal{C} = \bigsqcup_{\alpha \in \mathbb{F}_q} \mathcal{C}(\alpha).$$

Luego,

$$M = |\mathcal{C}| = \sum_{\alpha \in \mathbb{F}_q} |\mathcal{C}(\alpha)|. \quad (3.1)$$

Si para todo $\alpha \in \mathbb{F}_q$ se cumpliera que $|\mathcal{C}(\alpha)| < M/q$, entonces tendríamos que

$$\sum_{\alpha \in \mathbb{F}_q} |\mathcal{C}(\alpha)| < q(M/q) = M,$$

lo que contradice (3.1). Por lo tanto, existe $\beta \in \mathbb{F}_q$ tal que $|\mathcal{C}(\beta)| = N \geq M/q$.

Por otra parte, si $d(\mathcal{C}(\beta)) < d$ tendríamos que existen $\mathbf{x}, \mathbf{y} \in \mathcal{C}(\beta)$, $\mathbf{x} \neq \mathbf{y}$, tales que $d(\mathcal{C}(\beta)) = d(\mathbf{x}, \mathbf{y})$. Como $\mathcal{C}(\beta) \subseteq \mathcal{C}$ se seguiría que $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ y $0 < d(\mathbf{x}, \mathbf{y}) < d$ pero esto no puede ser y por ende $d(\mathcal{C}(\beta)) \geq d$.

Dado que la primera componente de todas las palabras de $\mathcal{C}(\beta)$ es β se sigue, por la *Proposición 2.63*, que $(\mathcal{C}(\beta))_1^*$ es un $(n-1, N, d')$ código sobre $\mathbb{F}_q$, con $N \geq M/q$ y $d' \geq d > 0$. Por la *Proposición 3.4*, $A_q(n-1, d) \geq N$, de aquí concluimos que $A_q(n-1, d) \geq A_q(n, d)/q$. $\square$

En general, si q, n y d son muy grandes es difícil conocer el valor de $A_q(n, d)$ y $B_q(n, d)$, por ello el principal problema de la teoría de códigos se convierte en encontrar cotas tanto superiores como inferiores para $A_q(n, d)$ y $B_q(n, d)$. Las cotas superiores nos dicen cuán grande puede llegar a ser o qué tantas palabras código puede llegar a tener un código sobre $\mathbb{F}_q$ con longitud n y distancia mínima d , por su parte las cotas inferiores están vinculadas a la construcción de códigos, es decir, se enfocan en encontrar algún código sobre $\mathbb{F}_q$ de longitud n y distancia mínima d y por ende nos dicen cuál es el valor mínimo que pueden tener $A_q(n, d)$ y $B_q(n, d)$.

3.3 COTA DE HAMMING

La cota superior más conocida es la *Cota de Hamming*.

Teorema 3.8. (Cota de Hamming) Un (n, M, d) código sobre $\mathbb{F}_q$ satisface

$$M \sum_{i=0}^t \binom{n}{i} (q-1)^i \leq q^n,$$

con $t = \lfloor (d-1)/2 \rfloor$ y $d > 0$. Más aún, $A_q(n, d) \leq \left\lfloor q^n / \left(\sum_{i=0}^t \binom{n}{i} (q-1)^i \right) \right\rfloor$.

Demostración. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$. Por *Teorema 2.94*, las M bolas cerradas de radio t centradas en las distintas palabras código de $\mathcal{C}$ son disjuntas dos a dos. Luego,

$$\left| \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c}) \right| = \sum_{\mathbf{c} \in \mathcal{C}} |B_t(\mathbf{c})|.$$

Por (2.5), tenemos que

$$\sum_{\mathbf{c} \in \mathcal{C}} |B_t(\mathbf{c})| = \sum_{\mathbf{c} \in \mathcal{C}} V_q(n, t) = M \sum_{i=0}^t \binom{n}{i} (q-1)^i.$$

Así,

$$\left| \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c}) \right| = M \sum_{i=0}^t \binom{n}{i} (q-1)^i.$$

Ahora bien, es claro que $\bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c}) \subseteq \mathbb{F}_q^n$. Por lo tanto,

$$M \sum_{i=0}^t \binom{n}{i} (q-1)^i \leq q^n.$$

Como $\mathcal{C}$ es un código arbitrario tenemos que $q^n / \left(\sum_{i=0}^t \binom{n}{i} (q-1)^i \right)$ es una cota superior del conjunto $\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) = d\}$, de aquí que $A_q(n, d) \leq \left\lfloor q^n / \left(\sum_{i=0}^t \binom{n}{i} (q-1)^i \right) \right\rfloor$. $\square$

Que existan números q, n, M y d que satisfagan la desigualdad de la Cota de Hamming no garantiza que exista un (n, M, d) código sobre $\mathbb{F}_q$. En efecto, se puede verificar que los valores $q = 2$, $M = 16$, $n = 7$ y $d = 4$ satisfacen la desigualdad de la Cota de Hamming. Sin embargo, el siguiente ejemplo muestra que no existe un $(7, 16, 4)$ código binario.

Ejemplo 3.9. Sean $n = 7$, $d = 4$ y $q = 2$. Por la Cota de Hamming $A_2(7, 4) \leq 16$ y por el Teorema 3.5, $A_2(7, 4) = A_2(6, 3)$. De la Cota de Hamming, $A_2(6, 3) \leq 9$. Por lo tanto, 9 es una cota superior para $A_2(7, 4)$.

Esto implica, por Teorema 3.1, que $B_2(7, 4) \leq 9$. Como $B_2(7, 4)$ es una potencia positiva de 2 tenemos que $B_2(7, 4) \leq 8$. En el Ejemplo 2.44, vimos que el dual del $[7, 4]$ código Hamming es un $[7, 3, 4]$ código binario y por lo tanto, $B_2(7, 4) = 8$ y $A_2(7, 4)$ es 8 o 9. ■

Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ con $d > 0$. Si cada vector en $\mathbb{F}_q^n$ pertenece a alguna de las M bolas cerradas de radio $t = \lfloor (d-1)/2 \rfloor$ centradas en las distintas palabras código de $\mathcal{C}$, es decir, si $\mathbb{F}_q^n \subseteq \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c})$, entonces de la prueba del Teorema de la Cota de Hamming tenemos que

$$M \sum_{i=0}^t \binom{n}{i} (q-1)^i = q^n.$$

En este sentido decimos que $\mathcal{C}$ alcanza la Cota de Hamming y se conoce con exactitud el valor de $A_q(n, d)$. Más aún, al tener que $\mathbb{F}_q^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c})$ decimos, en primer lugar que cubrimos el espacio $\mathbb{F}_q^n$ mediante bolas cerradas de radio t disjuntas dos a dos puesto que t es el radio de empaquetamiento de $\mathcal{C}$; y en segundo lugar, que el código $\mathcal{C}$ es *perfecto*.

Ejemplo 3.10. Sean $\mathcal{C}$ un código de repetición binario y longitud impar $n = 2h + 1$, $\mathbf{x} \in \mathbb{F}_2^n$ y $m = wt(\mathbf{x})$. Veamos que $\mathcal{C}$ es perfecto. Si $m \leq \lfloor n/2 \rfloor = \lfloor h + (1/2) \rfloor = h$ entonces $m = d(\mathbf{x}, \mathbf{0}) \leq h$, de aquí que $\mathbf{x} \in B_h(\mathbf{0})$; en caso contrario, es decir si $m > h$ entonces $m + h > 2h$, como $2h = n - 1$ se sigue que $m + h \geq n$ así $h \geq n - m$, por el Teorema 2.33 i) $\mathbf{x} \in B_h(\mathbf{1})$, en efecto

$$d(\mathbf{x}, \mathbf{1}) = wt(\mathbf{x} + \mathbf{1}) = wt(\mathbf{x}) + wt(\mathbf{1}) - 2wt(\mathbf{x} \cap \mathbf{1}) = m + n - 2m = n - m \leq h.$$

Como $\mathcal{C}$ es un código de repetición, $d(\mathcal{C}) = n$, luego $t = \lfloor (d(\mathcal{C}) - 1)/2 \rfloor = h$. Así las cosas,

$$\mathbb{F}_2^n \subseteq \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c}) = B_t(\mathbf{0}) \cup B_t(\mathbf{1}).$$

La otra inclusión es inmediata. Por lo tanto, $\mathcal{C}$ es perfecto. ■

Siempre podemos cubrir el espacio vectorial $\mathbb{F}_q^n$ con bolas cerradas centradas en las distintas palabras de cualquier código $\mathcal{C} \subseteq \mathbb{F}_q^n$. Al entero más pequeño s para el cual $\mathbb{F}_q^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_s(\mathbf{c})$ lo llamaremos el *radio de cubrimiento* de $\mathcal{C}$ y le denotaremos por $\rho(\mathcal{C})$. El siguiente teorema muestra que $\rho(\mathcal{C})$ existe y da una pauta para calcularlo.

Teorema 3.11. Sea $\mathcal{C}$ un código de longitud n sobre $\mathbb{F}_q$. Entonces $\rho(\mathcal{C})$ existe. Más aún,

$$\rho(\mathcal{C}) = \max_{\mathbf{x} \in \mathbb{F}_q^n} \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c}).$$

Demostración. Sea

$$r = \max_{\mathbf{x} \in \mathbb{F}_q^n} \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c}).$$

Es claro que r es un entero no negativo. Ahora, veamos que $\mathbb{F}_q^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_r(\mathbf{c})$. Sean $\mathbf{y} \in \mathbb{F}_q^n$ arbitrario y $\mathbf{c}_1 \in \mathcal{C}$ tal que $d(\mathbf{y}, \mathbf{c}_1) = \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{y}, \mathbf{c})$. Luego, $d(\mathbf{y}, \mathbf{c}_1) \leq r$, por consiguiente, $\mathbf{y} \in B_r(\mathbf{c}_1)$. Así, $\mathbb{F}_q^n \subseteq \bigcup_{\mathbf{c} \in \mathcal{C}} B_r(\mathbf{c})$. La otra inclusión es inmediata, por lo tanto $\rho(\mathcal{C})$ existe y $\rho(\mathcal{C}) \leq r$.

Como $\mathbb{F}_q^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_{\rho(\mathcal{C})}(\mathbf{c})$, dado $\mathbf{y} \in \mathbb{F}_q^n$ existe $\mathbf{c}_2 \in \mathcal{C}$ tal que $\mathbf{y} \in B_{\rho(\mathcal{C})}(\mathbf{c}_2)$, así $d(\mathbf{y}, \mathbf{c}_2) \leq \rho(\mathcal{C})$. Por otra parte, $\min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{y}, \mathbf{c}) \leq d(\mathbf{y}, \mathbf{c}_2)$, por transitividad $\min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{y}, \mathbf{c}) \leq \rho(\mathcal{C})$. Esto implica que $\rho(\mathcal{C})$ es una cota superior del conjunto $\{\min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c}) : \mathbf{x} \in \mathbb{F}_q^n\}$ y por lo tanto, $r \leq \rho(\mathcal{C})$. □

Teorema 3.12. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ con $M = A_q(n, d)$ y $d > 0$. Entonces $\mathcal{C}$ tiene radio de cubrimiento a lo más $d - 1$.

Demostración. Si $d = 1$ es claro que $\rho(\mathcal{C}) = 0$. Supongamos que $\rho(\mathcal{C}) \geq d > 1$. Por el Teorema 3.11, existe $\mathbf{x} \in \mathbb{F}_q^n$ tal que $\rho(\mathcal{C}) = \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c})$. Luego, $d \leq \rho(\mathcal{C}) \leq d(\mathbf{x}, \mathbf{c})$, para todo $\mathbf{c} \in \mathcal{C}$ y por lo tanto, $\mathcal{C}' = \mathcal{C} \cup \{\mathbf{x}\}$ es un código con distancia mínima d y $A_q(n, d) + 1$ palabras, lo que es una contradicción. $\square$

Este resultado también es válido en el caso lineal.

Teorema 3.13. Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código lineal con distancia mínima $d > 0$ y $B_q(n, d)$ palabras. Entonces, $\mathcal{C}$ tiene radio de cubrimiento a lo más $d - 1$.

Demostración. Es inmediato que $\rho(\mathcal{C}) = 0$ si $d = 1$, es decir, si $\mathcal{C} = \mathbb{F}_q^n$. Supongamos que $\rho(\mathcal{C}) \geq d > 1$. Por el Teorema 3.11, existe $\mathbf{x} \in \mathbb{F}_q^n$ tal que $\rho(\mathcal{C}) = \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c})$, luego $d \leq \rho(\mathcal{C}) \leq d(\mathbf{x}, \mathbf{c})$ para todo $\mathbf{c} \in \mathcal{C}$, de aquí que $\mathbf{x} \notin \mathcal{C}$. Sean $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ una base de $\mathcal{C}$ y

$$\mathcal{C}' = \text{Gen}\{\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{x}\}.$$

Puesto que $\mathbf{x} \notin \mathcal{C}$ se sigue que $\{\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{x}\}$ es un conjunto linealmente independiente. Veamos que $d(\mathcal{C}') = d$. Sea $\mathbf{y} \in \mathcal{C}'$, luego existen $\alpha_1, \dots, \alpha_k, \lambda \in \mathbb{F}_q$ tales que $\mathbf{y} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k + \lambda \mathbf{x}$.

1. Si $\lambda \neq 0$ entonces $d(\mathbf{x}, -\lambda \mathbf{x}) = 0$. Si $\mathbf{c} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k \in \mathcal{C}$ entonces $wt(\mathbf{y}) = d(\mathbf{c}, -\lambda \mathbf{x})$, por lo tanto

$$d \leq d(\mathbf{c}, \mathbf{x}) \leq d(\mathbf{c}, -\lambda \mathbf{x}) + d(-\lambda \mathbf{x}, \mathbf{x}) = wt(\mathbf{y}).$$

2. Si $\lambda = 0$ entonces $\mathbf{y} \in \mathcal{C}$ y por lo tanto $wt(\mathbf{y}) \geq d$.

Toda palabra de $\mathcal{C}$ de peso mínimo d es una palabra de $\mathcal{C}'$, por ende $d(\mathcal{C}') = d$. Así, $\mathcal{C}' \subseteq \mathbb{F}_q^n$ es un código lineal con dimensión d y $qB_q(n, d)$ palabras, esto es una contradicción. $\square$

La noción de radio de cubrimiento será fundamental cuando abordemos la Cota de Gilbert.

3.4 COTA DE PLOTKIN

Esta cota superior en algunos casos mejora la Cota de Hamming.

Lema 3.14. Sean a y b enteros tales que $M = a + b$ con M un entero positivo impar. Entonces $ab \leq (M^2 - 1)/4$.

Demostración. Tenemos que $ab = a(M - a)$. Sea $f(x) = x(M - x)$, para cada $x \in \mathbb{R}$. f es una parábola alcanza su valor máximo $M^2/4$ en $x = M/2$. Como M es impar, $M^2/4$ no es un entero. Dado que f es una parábola que abre hacia abajo, su valor máximo entero es $\lfloor M^2/4 \rfloor$. Si $M = 2k + 1$ con k un entero no negativo, entonces

$$\left\lfloor \frac{M^2}{4} \right\rfloor = \left\lfloor \frac{4k^2 + 4k + 1}{4} \right\rfloor = \left\lfloor k^2 + k + \frac{1}{4} \right\rfloor = k(k + 1).$$

Como $\lfloor M/2 \rfloor = \lfloor (2k + 1)/2 \rfloor = k$ y $f(k) = f(k + 1) = k(k + 1)$ tenemos que $f(t) \leq k(k + 1)$ para todo entero t y por lo tanto

$$ab = f(a) \leq k(k + 1) = \left(\frac{2k + 1 - 1}{2} \right) \left(\frac{2k + 2}{2} \right) = \left(\frac{M - 1}{2} \right) \left(\frac{M + 1}{2} \right).$$

$\square$

Teorema 3.15. (Cota de Plotkin) Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ tal que $rn < d$, donde $r = 1 - q^{-1}$. Entonces

$$M \leq \left\lfloor \frac{d}{d - rn} \right\rfloor.$$

En particular,

$$A_q(n, d) \leq \left\lfloor \frac{d}{d - rn} \right\rfloor,$$

siempre que $rn < d$. En el caso binario,

$$A_2(n, d) \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor,$$

siempre que $n < 2d$.

Demostración. Sea

$$S = \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\mathbf{y} \in \mathcal{C}} d(\mathbf{x}, \mathbf{y}).$$

Como $d(\mathbf{x}, \mathbf{y}) = 0$ si y solo si $\mathbf{x} = \mathbf{y}$, podemos ver a S de la siguiente manera

$$S = \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\substack{\mathbf{y} \in \mathcal{C} \\ \mathbf{y} \neq \mathbf{x}}} d(\mathbf{x}, \mathbf{y}).$$

Si $\mathbf{x} \neq \mathbf{y}$ entonces $d(\mathbf{x}, \mathbf{y}) \geq d$. Luego,

$$\sum_{\mathbf{x} \in \mathcal{C}} \sum_{\substack{\mathbf{y} \in \mathcal{C} \\ \mathbf{y} \neq \mathbf{x}}} d(\mathbf{x}, \mathbf{y}) \geq \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\substack{\mathbf{y} \in \mathcal{C} \\ \mathbf{y} \neq \mathbf{x}}} d.$$

Dado que existen M elecciones de $\mathbf{x}$ y para cada una de ellas existen $M - 1$ elecciones de $\mathbf{y}$ tales que $\mathbf{x} \neq \mathbf{y}$ tenemos que

$$\sum_{\mathbf{x} \in \mathcal{C}} \sum_{\substack{\mathbf{y} \in \mathcal{C} \\ \mathbf{y} \neq \mathbf{x}}} d = M(M - 1)d.$$

Por lo tanto,

$$S \geq M(M - 1)d. \quad (3.2)$$

Sea μ la matriz $M \times n$ cuyas filas son las palabras de $\mathcal{C}$. Para $1 \leq i \leq n$, definimos $\eta_{i,\alpha}$ como el número de veces en que $\alpha \in \mathbb{F}_q$ aparece en la columna i de μ .

Para calcular S

1. Se fija una palabra $\mathbf{x}$ de las M palabras de $\mathcal{C}$ ($\mathbf{x}$ corresponde a una fila j de las M filas de μ), se calcula la distancia de $\mathbf{x}$ a las $M - 1$ palabras de $\mathcal{C}$ distintas a $\mathbf{x}$ (las $M - 1$ filas distintas a la fila j) y se suman estos $M - 1$ resultados.
2. Se repite el proceso con cada palabra de $\mathcal{C}$ (cada fila de μ).
3. Finalmente, se suman los M resultados obtenidos.

En este sentido, decimos que estamos haciendo un “cálculo por las filas de μ ”. Pues bien, la noción de $\eta_{i,\alpha}$ nos permite ver a S como un “cálculo por las columnas de μ ”. En efecto, en lugar de fijar una fila j de μ , fijamos una columna i de las n columnas de μ y calculamos $\eta_{i,\alpha}$ para $\alpha \in \mathbb{F}_q$, fijo. Como

$$M = \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha},$$

tenemos que en la columna i de μ , $M - \eta_{i,\alpha}$ veces no aparece α . Por ende, una componente de la columna i en la que aparece α difiere de $M - \eta_{i,\alpha}$ componentes de la columna i . Así, como hay $\eta_{i,\alpha}$ componentes de la columna i cuya entrada es α , tenemos que $\eta_{i,\alpha}(M - \eta_{i,\alpha})$ parejas de palabras de $\mathcal{C}$ difieren en la componente i -ésima (una tiene a α en su i -ésima componente mientras que la otra no).

Al realizar este proceso con cada elemento de $\mathbb{F}_q$, obtenemos que el número de parejas de palabras de $\mathcal{C}$ que difieren en la i -ésima componente es $\sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}(M - \eta_{i,\alpha})$.

Repitiendo este proceso con cada columna de μ , llegamos a

$$S = \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\substack{\mathbf{y} \in \mathcal{C} \\ \mathbf{y} \neq \mathbf{x}}} d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}(M - \eta_{i,\alpha}). \quad (3.3)$$

Por ende,

$$\begin{aligned} S &= \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} M - \eta_{i,\alpha}^2 = M \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2 \\ &= M \sum_{i=1}^n M - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2 \\ &= nM^2 - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2. \end{aligned}$$

Por otra parte, para cada $1 \leq i \leq n$ sean $\mathbf{u} = (1, \dots, 1) \in \mathbb{R}^q$ y $\mathbf{v} \in \mathbb{R}^q$ el vector cuyas componentes son los q valores que resultan al calcular $\eta_{i,\alpha}$ para cada $\alpha \in \mathbb{F}_q$, entonces por la desigualdad de Cauchy-Schwartz

$$\left(\sum_{\alpha \in \mathbb{F}_q} (\eta_{i,\alpha})(1) \right)^2 \leq \sum_{\alpha \in \mathbb{F}_q} 1^2 \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2.$$

Esto implica que,

$$\sum_{i=1}^n (1/q) \left(\sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} \right)^2 \leq \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2.$$

Así las cosas,

$$\begin{aligned} S &= nM^2 - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2 \leq nM^2 - \sum_{i=1}^n (1/q) \left(\sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} \right)^2 \\ &= nM^2 - \sum_{i=1}^n (1/q) M^2 \\ &= nM^2 - \frac{nM^2}{q} \\ &= nM^2 \left(1 - \frac{1}{q} \right) \\ &= nM^2 r. \end{aligned}$$

De este resultado y la desigualdad (3.2) se sigue que $M(M-1)d \leq nrM^2$. Como por hipótesis $rn < d$ entonces

$$M \leq \frac{d}{d - nr}, \quad (3.4)$$

Ahora, puesto que M es un entero tenemos

$$M \leq \left\lfloor \frac{d}{d - nr} \right\rfloor.$$

Dado que $\mathcal{C}$ es un (n, M, d) código sobre $\mathbb{F}_q$, arbitrario, concluimos que $\lfloor d/(d - nr) \rfloor$ es una cota superior del conjunto $\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_q^n \text{ es un código con } d(\mathcal{C}) = d\}$ y que

$$A_q(n, d) \leq \left\lfloor \frac{d}{d - nr} \right\rfloor.$$

Resta analizar el caso binario, por (3.4)

$$M \leq \frac{d}{d - \frac{n}{2}} = \frac{2d}{2d - n}.$$

Si M es par, digamos $M = 2k$, con k un entero no negativo entonces $k \leq d/(2d - n)$, luego

$$k \leq \left\lfloor \frac{d}{2d - n} \right\rfloor.$$

Por lo tanto,

$$M = 2k \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor.$$

Si M es impar, no usamos la desigualdad de Cauchy-Schwartz. En lugar de eso, por (3.3)

$$\begin{aligned} S &= \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_2} \eta_{i,\alpha} (M - \eta_{i,\alpha}) = \sum_{i=1}^n (\eta_{i,0}(M - \eta_{i,0}) + \eta_{i,1}(M - \eta_{i,1})) \\ &= \sum_{i=1}^n (\eta_{i,0}(\eta_{i,0} + \eta_{i,1} - \eta_{i,0}) + \eta_{i,1}(\eta_{i,0} + \eta_{i,1} - \eta_{i,1})) \\ &= \sum_{i=1}^n (\eta_{i,0}\eta_{i,1} + \eta_{i,1}\eta_{i,0}) \\ &= 2 \sum_{i=1}^n \eta_{i,0}\eta_{i,1}. \end{aligned}$$

Dado que M es impar y que para cada $1 \leq i \leq n$, $M = \eta_{i,0} + \eta_{i,1}$ con $\eta_{i,0}, \eta_{i,1} \in \mathbb{Z}$, del Lema 3.14 se sigue que

$$\eta_{i,0} + \eta_{i,1} \leq \left(\frac{M-1}{2} \right) \left(\frac{M+1}{2} \right), \text{ para todo } 1 \leq i \leq n.$$

Luego,

$$S = 2 \sum_{i=1}^n \eta_{i,0}\eta_{i,1} \leq \frac{1}{2} \sum_{i=1}^n (M-1)(M+1) = \frac{1}{2}n(M-1)(M+1).$$

La desigualdad (3.2) implica que

$$M(M-1)d \leq \frac{n}{2}(M-1)(M+1).$$

Simplificando y dado que $2d - n > 0$, obtenemos

$$M \leq \frac{n}{2d - n} = \frac{2d}{2d - n} - 1.$$

Si $M = 2k + 1$ con k un entero no negativo. Entonces

$$2k \leq \frac{2d}{2d-n} - 2.$$

Luego,

$$k \leq \left\lfloor \frac{d}{2d-n} - 1 \right\rfloor = \left\lfloor \frac{d}{2d-n} \right\rfloor - 1.$$

Por lo tanto,

$$M = 2k + 1 \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor - 1 \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

En cualquier caso,

$$A_2(n, d) \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

□

Corolario 3.16.

- i) $A_2(2d, d) \leq 4d$. Si d es impar, $A_2(2d, d) \leq 2d + 2$.
- ii) Si d es impar entonces $A_2(2d + 1, d) \leq 4d + 4$.

Demostración.

- i) Por el *Teorema 3.7*, $A_2(2d, d) \leq 2A_2(2d - 1, d)$ y por la Cota de Plotkin,

$$A_2(2d - 1, d) \leq 2 \left\lfloor \frac{d}{2d - (2d - 1)} \right\rfloor = 2d,$$

luego $A_2(2d, d) \leq 4d$. Ahora, si d es impar, entonces $d + 1$ es par y por el *Teorema 3.5*, $A_2(2d + 1, d + 1) = A_2(2d, d)$, de nuevo por la Cota de Plotkin

$$A_2(2d + 1, d + 1) \leq 2 \left\lfloor \frac{d + 1}{2(d + 1) - (2d + 1)} \right\rfloor = 2(d + 1).$$

Por lo tanto, $A_2(2d, d) \leq 2(d + 1)$.

- ii) Por hipótesis $d+1$ es par. Entonces, por el *Teorema 3.5* tenemos que $A_2(2d+2, d+1) = A_2(2d+1, d)$.
Por i) $A_2(2d + 2, d + 1) \leq 4(d + 1)$ y $A_2(2d + 1, d) \leq 4(d + 1)$.

□

Ejemplo 3.17. En el *Ejemplo 3.9* vimos que $B_2(7, 4) = 8$ y que $A_2(7, 4) \leq 9$, por la Cota de Plotkin $A_2(7, 4) \leq 2 \lfloor 4/(8 - 7) \rfloor = 8$, por lo tanto $A_2(7, 4) = 8$. ■

Ejemplo 3.18. La Cota de Hamming garantiza que $A_2(14, 7) \leq 34$, ahora por el *Teorema 3.5* tenemos que $A_2(15, 8) = A_2(14, 7) \leq 34$ y por el *Corolario 3.16*, $A_2(14, 7) \leq 16$, por lo tanto $A_2(15, 8) \leq 16$. ■

3.5 COTA DE ELIAS

La Cota de Elias suele dar valores más grandes que las cotas de Hamming y Plotkin. Sin embargo, veremos en el siguiente capítulo que es la mejor cota superior asintótica, de ahí su importancia.

Lema 3.19. Sean $A = \{a_1, \dots, a_s\}$ y $B = \{b_1, \dots, b_t\}$ tales que $a_i \neq a_{i'}$ para todo $i \neq i'$ con $1 \leq i, i' \leq s$ y $b_j \neq b_{j'}$ para todo $j \neq j'$ con $1 \leq j, j' \leq t$. Entonces

$$|A \cap B| = \sum_{i=1}^s \sum_{j=1}^t |\{a_i\} \cap \{b_j\}|.$$

Demostración. Observe que

$$A \cap B = \bigcup_{i=1}^s \bigcup_{j=1}^t \{a_i\} \cap \{b_j\}.$$

Sea

$$C_i = \bigcup_{j=1}^t \{a_i\} \cap \{b_j\}, \quad \text{para todo } 1 \leq i \leq s,$$

dados C_i y $C_{i'}$ con $i \neq i'$ tenemos que $C_i \cap C_{i'} = \emptyset$ pues de lo contrario tendríamos que $a_i = a_{i'}$ y esto contradice la hipótesis, por lo tanto

$$|A \cap B| = \sum_{i=1}^s |C_i| = \sum_{i=1}^s \left| \bigcup_{j=1}^t \{a_i\} \cap \{b_j\} \right|,$$

ahora dados $\{a_i\} \cap \{b_j\}$ y $\{a_i\} \cap \{b_{j'}\}$ con $j \neq j'$ e i fijo tenemos que su intersección es vacía pues de lo contrario tendríamos que $b_j = b_{j'}$ y esto contradice la hipótesis. Así las cosas

$$|A \cap B| = \sum_{i=1}^s \sum_{j=1}^t |\{a_i\} \cap \{b_j\}|.$$

□

Lema 3.20. Sean $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ y $\mathbf{x} \in \mathbb{F}_q^n$. Entonces $\mathbf{x} + \mathcal{C}$ es un (n, M, d) código sobre $\mathbb{F}_q$.

Demostración. Recordemos que $\mathbf{x} + \mathcal{C} = \{\mathbf{x} + \mathbf{c} : \mathbf{c} \in \mathcal{C}\}$. Sea $f : \mathcal{C} \rightarrow \mathbf{x} + \mathcal{C}$ tal que $f(\mathbf{c}) = \mathbf{x} + \mathbf{c}$, claramente f es sobreyectiva y se puede verificar que es inyectiva, así $|\mathbf{x} + \mathcal{C}| = M$. Si $\mathbf{x} + \mathbf{c}_1, \mathbf{x} + \mathbf{c}_2 \in \mathbf{x} + \mathcal{C}$ entonces $d(\mathbf{x} + \mathbf{c}_1, \mathbf{x} + \mathbf{c}_2) = wt(\mathbf{c}_1 - \mathbf{c}_2) = d(\mathbf{c}_1, \mathbf{c}_2)$, de aquí que $d(\mathbf{x} + \mathcal{C}) = d$. □

Proposición 3.21. Sean $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ y $w \in \{1, \dots, n\}$ fijo. Entonces existe un (n, M, d) código $\mathcal{C}'$ sobre $\mathbb{F}_q$ con un (n, K, d') subcódigo $\mathcal{A}$, donde $d' \geq d$, que contiene solo palabras de peso a lo más w y tal que $K \geq MV_q(n, w)/q^n$.

Demostración. Sea $B_w(\mathbf{0})$ la bola cerrada en $\mathbb{F}_q^n$ de radio w centrada en $\mathbf{0}$. Claramente, $B_w(\mathbf{0}) \neq \emptyset$. Elegimos $\mathbf{x} \in \mathbb{F}_q^n$ de tal manera que $|B_w(\mathbf{0}) \cap (\mathbf{x} + \mathcal{C})|$ es maximal, luego

$$q^n |B_w(\mathbf{0}) \cap (\mathbf{x} + \mathcal{C})| \geq \sum_{\mathbf{y} \in \mathbb{F}_q^n} |B_w(\mathbf{0}) \cap (\mathbf{y} + \mathcal{C})|,$$

esto implica que

$$|B_w(\mathbf{0}) \cap (\mathbf{x} + \mathcal{C})| \geq \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{F}_q^n} |B_w(\mathbf{0}) \cap (\mathbf{y} + \mathcal{C})|. \quad (3.5)$$

Por el *Lema 3.19*

$$|B_w(\mathbf{0}) \cap (\mathbf{y} + \mathcal{C})| = \sum_{\mathbf{b} \in B_w(\mathbf{0})} \sum_{\mathbf{c} \in \mathcal{C}} |\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\}|.$$

Al reemplazar en (3.5) obtenemos

$$|B_w(\mathbf{0}) \cap (\mathbf{x} + \mathcal{C})| \geq \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{F}_q^n} \sum_{\mathbf{b} \in B_w(\mathbf{0})} \sum_{\mathbf{c} \in \mathcal{C}} |\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\}| = \frac{1}{q^n} \sum_{\mathbf{b} \in B_w(\mathbf{0})} \sum_{\mathbf{c} \in \mathcal{C}} \sum_{\mathbf{y} \in \mathbb{F}_q^n} |\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\}|.$$

Dados $\mathbf{b} \in B_w(\mathbf{0})$ y $\mathbf{c} \in \mathcal{C}$ tenemos que $\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\} \neq \emptyset$ si y solo si $\mathbf{y} = \mathbf{b} - \mathbf{c}$, luego

$$|\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\}| = \begin{cases} 1 & \text{si } \mathbf{y} = \mathbf{b} - \mathbf{c} \\ 0 & \text{en otro caso} \end{cases}$$

Por lo tanto

$$\begin{aligned} |B_w(\mathbf{0}) \cap (\mathbf{x} + \mathcal{C})| &\geq \frac{1}{q^n} \sum_{\mathbf{b} \in B_w(\mathbf{0})} \sum_{\mathbf{c} \in \mathcal{C}} \left(|\{\mathbf{b}\} \cap \{\mathbf{b}\}| + \sum_{\mathbf{y} \neq \mathbf{b} - \mathbf{c}} |\{\mathbf{b}\} \cap \{\mathbf{y} + \mathbf{c}\}| \right) \\ &= \frac{1}{q^n} \sum_{\mathbf{b} \in B_w(\mathbf{0})} \sum_{\mathbf{c} \in \mathcal{C}} 1 \\ &= \frac{1}{q^n} V_q(n, w) M. \end{aligned}$$

Sean $\mathcal{C}' = \mathbf{x} + \mathcal{C}$ y $\mathcal{A} = B_w(\mathbf{0}) \cap \mathcal{C}'$. Por el *Lema 3.20* $\mathcal{C}'$ es un (n, M, d) código sobre $\mathbb{F}_q$, como $\mathcal{A} \subseteq \mathcal{C}'$ tenemos que $d' = d(\mathcal{A}) \geq d(\mathcal{C}) = d$, ahora si $\mathbf{y} \in \mathcal{A}$ tenemos que $\mathbf{y} \in B_w(\mathbf{0})$, luego $wt(\mathbf{y}) = d(\mathbf{y}, \mathbf{0}) \leq w$, esto muestra que el peso de toda palabra de $\mathcal{A}$ es a lo más w . $\square$

Lema 3.22. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ tal que el peso de cada una de sus palabras es a lo más w , donde $w \leq rn$ con $r = 1 - q^{-1}$. Entonces

$$d \leq \frac{Mw}{M-1} \left(2 - \frac{w}{rn} \right).$$

Demostración. Al igual que en la prueba de la Cota de Plotkin, sea μ la matriz de $M \times n$ cuyas filas son las M palabras de $\mathcal{C}$. Para cada $1 \leq i \leq n$, sea $\eta_{i,\alpha}$ el número de veces en que $\alpha \in \mathbb{F}_q$ aparece en la columna i de μ . Es claro que

$$M = \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}, \quad (3.6)$$

para todo $1 \leq i \leq n$. Sea

$$T = \sum_{i=1}^n \eta_{i,0}.$$

Note que T es el número de ceros en la matriz μ , por ende T se puede calcular de la siguiente manera

1. se fija una fila j de μ y se cuentan cuántos ceros hay en ella. Si la palabra de $\mathcal{C}$ correspondiente a la fila j es $\mathbf{c}$ entonces la cantidad de ceros en j es $n - wt(\mathbf{c})$;
2. se repite el proceso con las demás $M - 1$ filas de μ ;
3. finalmente, se suman los $M - 1$ resultados.

Por consiguiente, $T = \sum_{\mathbf{c} \in \mathcal{C}} n - wt(\mathbf{c})$. Ahora bien, por hipótesis

$$\sum_{\mathbf{c} \in \mathcal{C}} n - wt(\mathbf{c}) = \sum_{\mathbf{c} \in \mathcal{C}} n - \sum_{\mathbf{c} \in \mathcal{C}} wt(\mathbf{c}) = nM - \sum_{\mathbf{c} \in \mathcal{C}} wt(\mathbf{c}) \geq nM - \sum_{\mathbf{c} \in \mathcal{C}} w = nM - wM = M(n - w),$$

por lo tanto

$$T \geq M(n - w). \quad (3.7)$$

Para cada $1 \leq i \leq n$, sean $\mathbf{u} = (1, \dots, 1) \in \mathbb{R}^{q-1}$ y $\mathbf{v} \in \mathbb{R}^{q-1}$ el vector cuyas componentes son los $q - 1$ valores que resultan al calcular $\eta_{i,\alpha}$, para cada α en el grupo multiplicativo $\mathbb{F}_q^*$ entonces, por la desigualdad de Cauchy-Schwartz

$$\left(\sum_{\alpha \in \mathbb{F}_q^*} (\eta_{i,\alpha})(1) \right)^2 \leq \sum_{\alpha \in \mathbb{F}_q^*} 1^2 \sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha}^2,$$

lo cual equivale a

$$\frac{1}{q-1} \left(\sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha} \right)^2 \leq \sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha}^2.$$

Como

$$\sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha} = \left(\sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} \right) - \eta_{i,0} \quad \text{y} \quad \sum_{\alpha \in \mathbb{F}_q} (\eta_{i,\alpha}) = M,$$

tenemos que

$$\frac{1}{q-1} (M - \eta_{i,0})^2 \leq \sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha}^2. \quad (3.8)$$

Por otra parte, sean $\mathbf{u} = (1, \dots, 1) \in \mathbb{R}^n$ y $\mathbf{v} \in \mathbb{R}^n$ el vector cuyas componentes son los n valores que resultan al calcular $\eta_{i,0}$, para cada $1 \leq i \leq n$, entonces, por la desigualdad de Cauchy-Schwartz

$$\left(\sum_{i=1}^n (\eta_{i,0})(1) \right)^2 \leq \sum_{i=1}^n 1^2 \sum_{i=1}^n \eta_{i,0}^2.$$

Luego,

$$\frac{1}{n} \left(\sum_{i=1}^n \eta_{i,0} \right)^2 \leq \sum_{i=1}^n \eta_{i,0}^2.$$

Así,

$$\frac{1}{n} T^2 \leq \sum_{i=1}^n \eta_{i,0}^2. \quad (3.9)$$

Al igual que en la prueba de la Cota de Plotkin, por (3.2) y (3.3)

$$M(M-1)d \leq \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\mathbf{y} \in \mathcal{C}} d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} (M - \eta_{i,\alpha}). \quad (3.10)$$

Usando primero (3,6), luego (3,8) y finalmente (3,9), obtenemos

$$\begin{aligned}
\sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} (M - \eta_{i,\alpha}) &= \sum_{i=1}^n M \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2 \\
&= \sum_{i=1}^n M^2 - \sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha}^2 \\
&= nM^2 - \sum_{i=1}^n \left(\eta_{i,0}^2 + \sum_{\alpha \in \mathbb{F}_q^*} \eta_{i,\alpha}^2 \right) \\
&\leq nM^2 - \sum_{i=1}^n \left(\eta_{i,0}^2 + \frac{1}{q-1} (M - \eta_{i,0})^2 \right) \\
&= nM^2 - \frac{1}{q-1} \sum_{i=1}^n \left((q-1)\eta_{i,0}^2 + M^2 - 2M\eta_{i,0} + \eta_{i,0}^2 \right) \\
&= nM^2 - \frac{1}{q-1} \sum_{i=1}^n \left(q\eta_{i,0}^2 + M^2 - 2M\eta_{i,0} \right) \\
&\leq nM^2 - \frac{1}{q-1} \left(\frac{q}{n} T^2 + nM^2 - 2M \sum_{i=1}^n \eta_{i,0} \right) \\
&= nM^2 - \frac{1}{q-1} \left(\frac{q}{n} T^2 + nM^2 - 2MT \right).
\end{aligned}$$

Esto es,

$$\sum_{i=1}^n \sum_{\alpha \in \mathbb{F}_q} \eta_{i,\alpha} (M - \eta_{i,\alpha}) \leq nM^2 - \frac{1}{q-1} \left(\frac{q}{n} T^2 + nM^2 - 2MT \right). \quad (3.11)$$

Por hipótesis, $w \leq rn$ y $r = 1 - q^{-1}$, luego

$$qw \leq qrn = q \left(1 - \frac{1}{q} \right) n = (q-1)n.$$

Lo cual implica que $n \leq qn - qw = q(n-w)$. Multiplicando a ambos lados de esta desigualdad por M , obtenemos $Mn \leq Mq(n-w)$, así

$$M \leq \frac{q}{n} M(n-w); \quad (3.12)$$

por (3,7) y dado que como $w \leq rn$, tenemos que

$$M \leq \frac{q}{n} T. \quad (3.13)$$

Al sumar (3.12) y (3.13) resulta $2M \leq qn^{-1}(T + M(n-w))$; multiplicando a ambos lados por $T - M(n-w)$, que es no negativo por (3.7), obtenemos

$$2M(T - M(n-w)) \leq \frac{q}{n} (T^2 - M^2(n-w)^2),$$

y por ende

$$\frac{q}{n} M^2(n-w)^2 - 2M^2(n-w) \leq \frac{q}{n} T^2 - 2MT.$$

Sustituyendo esto en (3.11) y usando (3,10)

$$M(M-1)d \leq nM^2 - \frac{1}{q-1} \left(\frac{q}{n} M^2(n-w)^2 + nM^2 - 2M^2(n-w) \right).$$

Al simplificar el lado derecho de de esta expresión tenemos que

$$M(M-1)d \leq M^2w \left(2 - \frac{q}{q-1} \frac{w}{n}\right) = M^2w \left(2 - \frac{w}{rn}\right).$$

Por lo tanto,

$$d \leq \frac{Mw}{M-1} \left(2 - \frac{w}{rn}\right).$$

□

Teorema 3.23. (Cota de Elias) Sea $r = 1 - q^{-1}$. Si $w \leq rn$ y $w^2 - 2rnw + rnd > 0$. Entonces

$$A_q(n, d) \leq \left(\frac{rnd}{w^2 - 2rnw + rnd} \right) \left(\frac{q^n}{V_q(n, w)} \right).$$

Demostración. Sea $M = A_q(n, d)$, así existe un (n, M, d) código sobre $\mathbb{F}_q$. Por la *Proposición 3.21* existe un (n, K, d') código sobre $\mathbb{F}_q$ con $d' \geq d$ que contiene solo palabras de peso a lo más w y tal que

$$\frac{MV_q(n, w)}{q^n} \leq K. \quad (3.14)$$

Como $w \leq rn$ y $r = 1 - q^{-1}$, por el *Lema 3.22* tenemos que

$$d \leq \frac{Kw}{K-1} \left(2 - \frac{w}{rn}\right).$$

Despejando K de esta expresión y teniendo en cuenta que $w^2 - 2rnw + rnd > 0$ llegamos a

$$K \leq \frac{rnd}{w^2 - 2rnw + rnd}. \quad (3.15)$$

Por las desigualdades (3.14) y (3.15)

$$\frac{MV_q(n, w)}{q^n} \leq \frac{rnd}{w^2 - 2rnw + rnd}.$$

Por lo tanto

$$M \leq \left(\frac{rnd}{w^2 - 2rnw + rnd} \right) \left(\frac{q^n}{V_q(n, w)} \right).$$

□

3.6 COTA DE SINGLETON

La cota de Singleton es mucho más fácil de probar que las cotas anteriores. Se usa para el almacenamiento de información en discos compactos.

Teorema 3.24. (Cota de Singleton) Para $n \geq d$

$$A_q(n, d) \leq q^{n-d+1}.$$

Además, si existe un $[n, k, d]_q$ código entonces $k \leq n - d + 1$.

Demostración. Si $d = n$ entonces por la *Proposición 3.1*, $A_q(n, n) = q = q^{n-n+1}$. Supongamos que $n > d$ y mediante inducción sobre r veamos que

$$A_q(n, d) \leq q^r A_q(n - r, d),$$

para cada r entero positivo tal que $1 \leq r \leq n - d$.

Si $r = 1$, entonces la desigualdad se cumple por el *Teorema 3.7*. Supongamos que el resultado es cierto para $k < n - d$. Por la hipótesis inductiva y por el *Teorema 3.7*

$$A_q(n, d) \leq q^k A_q(n - k, d) \leq q^{k+1} A_q(n - (k + 1), d),$$

lo cual muestra que la desigualdad es cierta para $k + 1$. Por lo tanto,

$$A_q(n, d) \leq q^{n-d} A_q(n - (n - d), d) = q^{n-d} A_q(d, d) = q^{n-d+1}.$$

Si $\mathcal{C}$ un $[n, k, d]_q$ código, entonces

$$q^k \leq B_q(n, d) \leq A_q(n, d) \leq q^{n-d+1},$$

y dado que la función logaritmo es creciente,

$$k = \log_q q^k \leq \log_q q^{n-d+1} = n - d + 1.$$

□

Ejemplo 3.25. El hexacódigo (*Ejemplo 2.47*) es un $[6, 3, 4]$ código cuaternario que alcanza la Cota de Singleton. En efecto, $k = 3 = 6 - 4 + 1 = n - d + 1$. ■

Sea $\mathcal{C}$ un $[n, k, d]_q$ código con matriz de chequeo de paridad H entonces, por el *Corolario 2.6*, cualquier conjunto de $d - 1$ columnas de H es linealmente independiente. Por la *Proposición 2.5*, el mayor número de columnas linealmente independientes de H es $\rho(H) = n - k$ y $d - 1 \leq n - k$, esto muestra de forma directa la versión lineal de la Cota de Singleton.

El siguiente teorema será fundamental para el estudio de la función de Manin.

Teorema 3.26. Dado un $[n, k, d]_q$ código con $k > 1$ existe un $[n - 1, k - 1, d]_q$ código.

Demostración. Sean $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ tal que $k > 1$, H una matriz de chequeo de paridad para $\mathcal{C}$ y $\mathbf{h}_1, \dots, \mathbf{h}_n$ las columnas de H . Por el *Teorema 2.46*, existe $A \subseteq \{1, \dots, n\}$ con $|A| = d$ tal que $\{\mathbf{h}_i : i \in A\}$ es linealmente dependiente, por la Cota de Singleton y la hipótesis $n + 1 \geq d + k > d + 1$ y por ende $n > d$, de aquí que $n > |A|$, luego existe $j \in \{1, \dots, n\}$ tal que $j \notin A$. Sean H' la matriz de tamaño $(n - k) \times (n - 1)$ que tiene por columnas al conjunto $\{\mathbf{h}_1, \dots, \mathbf{h}_n\} \setminus \{\mathbf{h}_j\}$ y $\mathcal{C}' = \text{Nu}(H')$. Como $\{\mathbf{h}_i : i \in A\} \subseteq \{\mathbf{h}_1, \dots, \mathbf{h}_n\} \setminus \{\mathbf{h}_j\}$ tenemos que de H' se puede extraer un conjunto de d columnas linealmente dependientes; ahora, si existiese $B \subseteq \{1, \dots, n\} \setminus \{j\}$ con $|B| = d - 1$ tal que $\{\mathbf{h}_i : i \in B\}$ sea linealmente dependiente tendríamos que H tiene un conjunto formado por $d - 1$ columnas que es linealmente dependiente puesto que $\{\mathbf{h}_i : i \in B\} \subseteq \{\mathbf{h}_1, \dots, \mathbf{h}_n\}$, lo cual es una contradicción y por ende todo conjunto formado por $d - 1$ columnas de H' es linealmente independiente. Luego, por el *Teorema 2.46*, $\dim(\mathcal{C}') = d$ y por lo tanto, $\mathcal{C}'$ es un $[n - 1, k - 1, d]_q$ código sobre $\mathbb{F}_q$. □

Corolario 3.27. Sea $\mathcal{C}$ un $[n, k, d]_q$ código con $k > 1$, si l es un entero tal que $0 < l < k$ entonces existe un $[n - l, k - l, d]_q$ código.

Demostración. Haremos la prueba mediante inducción sobre l . Si $l = 1$ entonces el *Teorema 3.26* garantiza que existe un $[n - 1, k - 1, d]_q$ código. Supongamos que existe un $[n - l, k - l, d]_q$ código con $0 < l < k - 1$, de aquí que $k - l > 1$ y por el *Teorema 3.26* tenemos que existe un $[n - (l + 1), k - (l + 1), d]_q$ código, lo que concluye la prueba. □

3.7 COTA DE GRIESMER

Esta cota es una generalización de la Cota de Singleton, en su versión lineal. Para probar esta cota hablaremos primero de la idea de código residual. Sean $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ con $k \geq 1$, $\mathbf{c} = c_1 \cdots c_n$ una palabra código de peso $w \neq 0$ e $i_1, \dots, i_w$ tales que $c_{i_j} \neq 0$ para todo $1 \leq j \leq w$. Consideremos $\sigma \in S_n$ tal que $\sigma(i_j) = j$ para todo $1 \leq j \leq w$, P la matriz asociada a σ y

$$D = \text{diag}\left((c_{i_1})^{-1}, \dots, (c_{i_w})^{-1}, 1, \dots, 1\right).$$

Si $\mathcal{C}' = \{\mathbf{y}PD : \mathbf{y} \in \mathcal{C}\}$ entonces $\mathbf{u} = 1 \cdots 10 \cdots 0 \in \mathcal{C}'$ con $\text{wt}(\mathbf{u}) = w$ y, por el Corolario 2.59, $\mathcal{C}'$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$. El *código residual de $\mathcal{C}$ con respecto a $\mathbf{c}$* se define como

$$\text{Res}(\mathcal{C}, \mathbf{c}) := \{y_{w+1} \cdots y_n : y_1 \cdots y_w y_{w+1} \cdots y_n \in \mathcal{C}'\}.$$

Si $k = 1$ entonces $w = d$ y $\text{Res}(\mathcal{C}, \mathbf{c})$ es el código trivial de $\mathbb{F}_q^{n-d}$.

Teorema 3.28. Sea $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ con $k > 1$ y sea $\mathbf{c}$ una palabra de peso $w < qd/(q-1)$ con $w \neq 0$. Entonces $\text{Res}(\mathcal{C}, \mathbf{c})$ es un $[n-w, k-1, d']$ código sobre $\mathbb{F}_q$, con $d' \geq d-w + \lceil w/q \rceil$.

Demostración. Si $w = 1$ el Corolario 2.64 muestra que $\text{Res}(\mathcal{C}, \mathbf{c})$ es un código lineal sobre $\mathbb{F}_q$ de longitud $n-1$. Mediante inducción sobre w tenemos que $\text{Res}(\mathcal{C}, \mathbf{c})$ es un código lineal sobre $\mathbb{F}_q$ de longitud $n-w$. Sean $r = \dim(\text{Res}(\mathcal{C}, \mathbf{c}))$ y $f : \mathcal{C}' \rightarrow \text{Res}(\mathcal{C}, \mathbf{c})$ la función dada por

$$x_1 \cdots x_w \cdots x_n \xrightarrow{f} x_{w+1} \cdots x_n.$$

Es claro que f es sobreyectiva, como $f(\mathbf{u}) = f(\mathbf{0}) = \mathbf{0}$ tenemos que f no es inyectiva. Por lo tanto, $q^r = |\text{Res}(\mathcal{C}, \mathbf{c})| < |\mathcal{C}'| = q^k$ y $r < k$.

Supongamos que $r < k-1$. y completemos el conjunto $\{\mathbf{u}\}$ a una base $\{\mathbf{u}, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ para $\mathcal{C}'$, como $r < k-1$ tenemos que $\{f(\mathbf{v}_2), \dots, f(\mathbf{v}_k)\}$ es linealmente dependiente. Luego, existen escalares $\alpha_2, \dots, \alpha_k$ en $\mathbb{F}_q$, no todos cero tales que

$$\mathbf{0} = \alpha_2 f(\mathbf{v}_2) + \cdots + \alpha_k f(\mathbf{v}_k) = f(\alpha_2 \mathbf{v}_2 + \cdots + \alpha_k \mathbf{v}_k).$$

Si $\mathbf{y} = \alpha_2 \mathbf{v}_2 + \cdots + \alpha_k \mathbf{v}_k \in \mathcal{C}'$ entonces $\mathbf{y}$ no es un múltiplo de $\mathbf{u}$ y $f(\mathbf{y}) = \mathbf{0}$. Así, si $\mathbf{y} = y_1 \cdots y_w \cdots y_n$ tenemos que $f(\mathbf{y}) = y_1 \cdots y_w 0 \cdots 0$. Note que existe $\beta \in \mathbb{F}_q$ tal que $|\{1 \leq j \leq w : y_j = \beta\}| \geq w/q$, pues si para todo $\alpha \in \mathbb{F}_q$ se cumpliera que $|\{1 \leq j \leq w : y_j = \alpha\}| < w/q$ tendríamos que

$$w = \left| \bigcup_{\alpha \in \mathbb{F}_q} \{1 \leq j \leq w : y_j = \alpha\} \right| = \sum_{\alpha \in \mathbb{F}_q} |\{1 \leq j \leq w : y_j = \alpha\}| < q \left(\frac{w}{q} \right) = w,$$

pero esto no puede ser. Luego

$$\begin{aligned} 0 < d(\mathbf{y}, \beta \mathbf{u}) &= \text{wt}(\mathbf{y} - \beta \mathbf{u}) \\ &= |\{1 \leq j \leq w : y_j \neq \beta\}| + |\{w+1 \leq j \leq n : y_j \neq 0\}| \\ &= w - |\{1 \leq j \leq w : y_j = \beta\}| \\ &\leq w - \frac{w}{q} \\ &= \frac{w(q-1)}{q}. \end{aligned}$$

De aquí que, $d \leq (w(q-1))/q$, esto contradice nuestra hipótesis. Por lo tanto, $r = k-1$.

Resta establecer una cota inferior para d' . Sea $\mathbf{x} \in \text{Res}(\mathcal{C}, \mathbf{c})$ con $\mathbf{x} \neq \mathbf{0}$. Luego, existe $\mathbf{z} = z_1 \cdots z_w \cdots z_n$ en $\mathcal{C}'$ tal que $\mathbf{x} = z_{w+1} \cdots z_n$. Ahora, $\mathbf{z}$ no es un múltiplo de $\mathbf{u}$ puesto que $\mathbf{x} \neq \mathbf{0}$. Si para todo $\alpha \in \mathbb{F}_q$ se cumple que $|\{1 \leq j \leq w : z_j = \alpha\}| < w/q$ entonces, como antes, llegamos a una contradicción. Por ende, existe $\gamma \in \mathbb{F}_q$ tal que $|\{1 \leq j \leq w : z_j = \gamma\}| \geq w/q$ y

$$\begin{aligned} d &\leq d(\mathbf{z}, \gamma \mathbf{u}) = wt(\mathbf{z} - \gamma \mathbf{u}) \\ &= |\{1 \leq j \leq w : z_j \neq \gamma\}| + |\{w+1 \leq j \leq n : z_j \neq 0\}| \\ &= w - |\{1 \leq j \leq w : z_j = \gamma\}| + wt(\mathbf{x}) \\ &\leq w - \frac{w}{q} + wt(\mathbf{x}). \end{aligned}$$

De aquí que $wt(\mathbf{x}) \geq d - w + (w/q)$, esto implica, por ser $wt(\mathbf{x})$ un entero positivo, que $wt(\mathbf{x}) \geq d - w + \lceil w/q \rceil$. Finalmente, si $\mathbf{v} \in \text{Res}(\mathcal{C}, \mathbf{c})$ es tal que $wt(\mathbf{v}) = d'$ concluimos que $d' \geq d - w + \lceil w/q \rceil$. $\square$

Corolario 3.29. Si $\mathcal{C}$ es un $[n, k, d]_q$ código con $k \geq 1$ y $\mathbf{c} \in \mathcal{C}$ tiene peso d , entonces $\text{Res}(\mathcal{C}, \mathbf{c})$ es un $[n - d, k - 1, d']$ código sobre $\mathbb{F}_q$, donde $d' \geq \lceil d/q \rceil$.

Demostración. Se tiene por el Teorema 3.28, al tomar $w = d$. $\square$

Ejemplo 3.30. Sean $n = 16, q = 2$ y $d = 6$. Por la Cota de Hamming, $A_2(16, 6) \leq 478$, luego, por la Proposición 3.1, $B_2(16, 6) \leq 2^8$. Supongamos que $B_2(16, 6) = 2^8$, sean $\mathcal{C}$ un $[16, 8, 6]$ código binario y $\mathbf{c} \in \mathcal{C}$ tal que $wt(\mathbf{c}) = 6$, así, por el Corolario 3.29, $\text{Res}(\mathcal{C}, \mathbf{c})$ es un $[10, 7, d']$ código binario con $d' \geq 3$ y por la Cota de Singleton, $d' \leq 10 - 7 + 1$. Así las cosas, $\text{Res}(\mathcal{C}, \mathbf{c})$ es un $[10, 7, d']$ código binario con $3 \leq d' \leq 4$, pero, de la Cota de Hamming, $A_2(10, 4) = A_2(10, 3) \leq 93 < 2^7$, esto significa que no existe ningún $[10, 7, 4]_2$ código ni ningún $[10, 7, 3]_2$ código y por lo tanto $B_2(16, 6) \leq 2^7$.

Teorema 3.31. (Cota de Griesmer) Sea $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$ con $k \geq 1$. Entonces

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

Demostración. Haremos inducción sobre k . Si $k = 1$ entonces el resultado es inmediato. Sea $\mathcal{C}$ un $[n, k + 1, d]$ código sobre $\mathbb{F}_q$ con $k \geq 1$ y veamos que

$$n \geq \sum_{i=0}^k \left\lceil \frac{d}{q^i} \right\rceil.$$

Sea $\mathbf{c} \in \mathcal{C}$ tal que $wt(\mathbf{c}) = d$, por el Corolario 3.29, $\text{Res}(\mathcal{C}, \mathbf{c})$ es un $[n - d, k, d']$ código sobre $\mathbb{F}_q$, donde $d' \geq \lceil d/q \rceil$. Al aplicar la hipótesis inductiva a $\text{Res}(\mathcal{C}, \mathbf{c})$, resulta

$$n - d \geq \sum_{i=0}^{k-1} \left\lceil \frac{d'}{q^i} \right\rceil. \quad (3.16)$$

Por otra parte, dado que $d' \geq \lceil d/q \rceil$ tenemos que

$$\left\lceil \frac{d'}{q^i} \right\rceil \geq \frac{d'}{q^i} \geq \frac{1}{q^i} \left\lceil \frac{d}{q} \right\rceil \geq \frac{d}{q^{i+1}}, \text{ para todo } 0 \leq i \leq k - 1.$$

Así, por definición de la función techo

$$\left\lceil \frac{d'}{q^i} \right\rceil \geq \left\lceil \frac{d}{q^{i+1}} \right\rceil, \text{ para todo } 0 \leq i \leq k - 1.$$

Reemplazando en (3.16)

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

Al hacer el cambio de variable $t = i + 1$, obtenemos

$$n - d \geq \sum_{t=1}^k \left\lceil \frac{d}{q^t} \right\rceil.$$

Por lo tanto

$$n \geq d + \sum_{t=1}^k \left\lceil \frac{d}{q^t} \right\rceil = \sum_{t=0}^k \left\lceil \frac{d}{q^t} \right\rceil.$$

□

Corolario 3.32. Sea $d > 0$. Entonces

$$B_q(n, d) \leq q^k,$$

donde

$$k = \max \left\{ r \geq 1 : n \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil \right\}.$$

Demostración. Sea

$$A = \left\{ r \geq 1 : n \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil \right\},$$

como $n \geq d$ tenemos que $1 \in A$ y por ende A es un conjunto no vacío; así y dado que para cualquier i $\lceil d/q^i \rceil$ es un entero positivo tenemos que $\max A$ existe. Sean $k = \max A$ y $\mathcal{C}$ un $[n, r, d]$ código sobre $\mathbb{F}_q$ con $q^r = B_q(n, d)$, como $d > 0$ que $r \geq 1$ y por la Cota de Griesmer,

$$n \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Así, $r \in A$, luego $r \leq k$, por lo tanto $B_q(n, d) \leq q^k$. □

Observación 3.33. Sea $\mathcal{C}$ un $[n, k, d]_q$ código con $k \geq 1$, dado que $\lceil d/q^0 \rceil = d$ y que para todo $1 \leq i \leq n$ se cumple que $\lceil d/q^i \rceil \geq 1$ (ya que $d > 0$ por ser $k \geq 1$) tenemos, por la Cota de Griesmer, que

$$n \geq d + \sum_{i=1}^r \left\lceil \frac{d}{q^i} \right\rceil \geq d + \sum_{i=1}^r 1 = d + k - 1.$$

Así, la Cota de Griesmer implica la versión lineal de la Cota de Singleton.

3.8 COTA DE GILBERT

Finalizamos este capítulo estudiando dos cotas inferiores para $B_q(n, d)$, la primera de ellas es la Cota de Gilbert.

Teorema 3.34. (Cota de Gilbert) Sea $d > 0$. Entonces

$$B_q(n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}.$$

Demostración. Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$ con $B_q(n, d)$ palabras. Por el Teorema 3.13, el radio de cubrimiento de $\mathcal{C}$ es a lo más $d - 1$, luego las bolas cerradas centradas en las palabras de $\mathcal{C}$ de radio $d - 1$ cubren a $\mathbb{F}_q^n$, es decir

$$\mathbb{F}_q^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_{d-1}(\mathbf{c}).$$

Por la Proposición 2.92, el número de vectores en cada una de las $B_q(n, d)$ bolas cerradas es

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \neq 0.$$

Como puede que las bolas no sean disjuntas dos a dos, concluimos que

$$q^n = |\mathbb{F}_q^n| = \left| \bigcup_{\mathbf{c} \in \mathcal{C}} B_{d-1}(\mathbf{c}) \right| \leq \sum_{\mathbf{c} \in \mathcal{C}} |B_{d-1}(\mathbf{c})| = B_q(n, d) \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i.$$

□

Observación 3.35. Dado que $q^n/\alpha > 0$, siendo $\alpha = \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i$, tenemos que

$$\frac{q^n}{\alpha} = q^{\log_q(q^n/\alpha)} = q^{n - \log_q \alpha},$$

por lo que la Cota de Gilbert también puede expresarse de la siguiente manera

$$B_q(n, d) \geq q^{n - \log_q \alpha}.$$

3.9 COTA DE VARSHAMOV

La Cota de Varshamov es una cota inferior para $B_q(n, d)$ y coincide asintóticamente con la Cota de Gilbert, tal y como veremos en el siguiente capítulo.

Lema 3.36. Sean n y m enteros positivos, y $\{\mathbf{h}_1, \dots, \mathbf{h}_{m+1}\} \subseteq \mathbb{F}_q^n$ tales que $\mathbf{h}_1 \neq \mathbf{0}$ y $\mathbf{h}_s$ no es combinación lineal de $\{\mathbf{h}_1, \dots, \mathbf{h}_{s-1}\}$ para todo $2 \leq s \leq m+1$. Entonces $\{\mathbf{h}_1, \dots, \mathbf{h}_{m+1}\}$ es un conjunto linealmente independiente.

Demostración. Supongamos que $\{\mathbf{h}_1, \dots, \mathbf{h}_{m+1}\}$ es linealmente dependiente, luego existen escalares $\alpha_1, \dots, \alpha_{m+1}$ no todos cero tales que $\alpha_1 \mathbf{h}_1 + \dots + \alpha_{m+1} \mathbf{h}_{m+1} = \mathbf{0}$. Sea $t = \max\{1 \leq s \leq m+1 : \alpha_s \neq 0\}$, como $\mathbf{h}_1 \neq \mathbf{0}$ tenemos que $t > 1$, así $\mathbf{h}_t = \beta_1 \mathbf{h}_1 + \dots + \beta_{t-1} \mathbf{h}_{t-1}$ con $\beta_s = -\alpha_s/\alpha_t$ para todo $1 \leq s \leq t-1$, lo cual es una contradicción. □

Lema 3.37. Sea $\{\mathbf{h}_1, \dots, \mathbf{h}_m, \dots, \mathbf{h}_j\} \subseteq \mathbb{F}_q^n$ con $m < j$ y $\mathbf{h}_s \neq \mathbf{h}_t$ para todo $1 \leq s, t \leq j$. Entonces el número de combinaciones lineales distintas de m vectores tomados del conjunto $\{\mathbf{h}_1, \dots, \mathbf{h}_j\}$ es a lo más

$$\sum_{i=0}^m \binom{j}{i} (q-1)^i.$$

Demostración. Sean

$$A = \left\{ \sum_{s=1}^m \alpha_s \mathbf{h}_{i_s} : \alpha_s \in \mathbb{F}_q, \mathbf{h}_{i_s} \neq \mathbf{h}_{i_t} \text{ para todo } 1 \leq s, t \leq m, \{\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_m}\} \subseteq \{\mathbf{h}_1, \dots, \mathbf{h}_j\} \right\},$$

$$B_r = \left\{ \sum_{s=1}^r \alpha_s \mathbf{h}_{i_s} : \alpha_s \in \mathbb{F}_q \setminus \{0\}, \mathbf{h}_{i_s} \neq \mathbf{h}_{i_t} \text{ para todo } 1 \leq s, t \leq r, \{\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_r}\} \subseteq \{\mathbf{h}_1, \dots, \mathbf{h}_j\} \right\},$$

para todo $1 \leq r \leq m$. Observe que

$$A \subseteq \{\mathbf{0}\} \cup \bigcup_{r=1}^m B_r,$$

luego

$$|A| \leq \left| \{\mathbf{0}\} \cup \bigcup_{r=1}^m B_r \right| \leq 1 + \sum_{r=1}^m |B_r|.$$

Ahora,

$$|B_r| = \binom{j}{r} (q-1)^r, \text{ para todo } 1 \leq r \leq m,$$

así

$$|A| \leq 1 + \sum_{r=1}^m \binom{j}{r} (q-1)^r = \sum_{r=0}^m \binom{j}{r} (q-1)^r. \quad (3.17)$$

Sea A' el conjunto de combinaciones lineales distintas de m vectores tomados del conjunto $\{\mathbf{h}_1, \dots, \mathbf{h}_j\}$, es claro que $A' \subseteq A$. Por lo tanto, por (3.17) el número de combinaciones lineales distintas de m vectores tomados del conjunto $\{\mathbf{h}_1, \dots, \mathbf{h}_j\}$ es a lo más

$$\sum_{r=0}^m \binom{j}{r} (q-1)^r.$$

□

Proposición 3.38. Sean n, k y d enteros con $2 \leq d \leq n$ y $1 \leq k \leq n$. Si

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k},$$

entonces existe una matriz H con entradas en $\mathbb{F}_q$ y tamaño $(n-k) \times n$ tal que todo conjunto de $d-1$ columnas de H es linealmente independiente.

Demostración. Por hipótesis,

$$1 \leq \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}.$$

Queremos encontrar n vectores (no necesariamente distintos) $\mathbf{h}_1, \dots, \mathbf{h}_n$ de $\mathbb{F}_q^{n-k}$ tales que si H es la matriz cuyas columnas son $\mathbf{h}_1, \dots, \mathbf{h}_n$ entonces cualquier conjunto de $d-1$ columnas de H es linealmente independiente. Si $d = 2$ el resultado se sigue de manera inmediata al tomar cualquier vector no nulo de $\mathbb{F}_q^{n-k}$, digamos $\mathbf{x}$, y hacer $\mathbf{h}_1 = \dots = \mathbf{h}_n = \mathbf{x}$, supongamos que $d > 2$, para este caso haremos uso del siguiente algoritmo

Sean $\mathbf{h}_1$ cualquier vector no nulo de $\mathbb{F}_q^{n-k}$ y $2 \leq j \leq n$.

- i) Si $j \leq d-2$, sea $\mathbf{h}_j$ cualquier vector de $\mathbb{F}_q^{n-k}$ que no es combinación lineal de $\mathbf{h}_1, \dots, \mathbf{h}_{j-1}$.
- ii) Si $j > d-2$, sea $\mathbf{h}_j$ cualquier vector de $\mathbb{F}_q^{n-k}$ que no es combinación lineal de $d-2$ de los $j-1$ vectores $\mathbf{h}_1, \dots, \mathbf{h}_{j-1}$.

Mediante inducción sobre j veamos que el algoritmo puede ser efectuado. Según el algoritmo, $\mathbf{h}_2$ es cualquier vector de $\mathbb{F}_q^{n-k}$ que no es múltiplo escalar de $\mathbf{h}_1$. En efecto, si $d-2=1$ entonces considere ii) en caso contrario, esto es si $d-2 \geq 2$ entonces considere i) Como $d > 2$ tenemos que

$$q = 1 + (q-1) \leq 1 + (n-1)(q-1) \leq \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}.$$

Así, $n-k > 1$ y por ende $\mathbf{h}_2$ existe. Sea $2 \leq j \leq n-1$ y supongamos que $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_j$ han sido encontrados. Ahora,

1. Si $j \leq d-2$ entonces por i) $\mathbf{h}_t$ no es combinación lineal de $\mathbf{h}_1, \dots, \mathbf{h}_{t-1}$ para todo $2 \leq t \leq j$, luego, por el Lema 3.36 $\{\mathbf{h}_1, \dots, \mathbf{h}_j\}$ es un conjunto linealmente independiente, de aquí que el número de combinaciones lineales distintas que se pueden formar con los j vectores $\mathbf{h}_1, \dots, \mathbf{h}_j$ es

$$q^j = ((q-1) + 1)^j = \sum_{i=0}^j \binom{j}{i} (q-1)^i + 0 + \dots + 0 = \sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i.$$

2. Si $j > d-2$ entonces por el Lema 3.37 el número de combinaciones lineales distintas que se pueden formar con $(d-2)$ vectores tomados de $\{\mathbf{h}_1, \dots, \mathbf{h}_j\}$ es a lo más

$$\sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i.$$

Dado que $j \leq n-1$ tenemos por la hipótesis que

$$\sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i \leq \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}.$$

En resumen, la cantidad de combinaciones lineales distintas que se pueden formar ya sea con todos los j o con $(d-2)$ de los j (dependiendo el caso) vectores $\mathbf{h}_1, \dots, \mathbf{h}_j$ es menor que la cardinalidad de $\mathbb{F}_q^{n-k}$, de aquí que $\mathbf{h}_{j+1}$ existe.

Sean $\mathbf{h}_1, \dots, \mathbf{h}_{d-2}, \dots, \mathbf{h}_n$ formados mediante el algoritmo. Supongamos que existe un conjunto formado por $d-1$ de estos vectores que es linealmente dependiente, digamos $\{\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_{d-1}}\}$ y que si $s < r$ entonces $i_s < i_r$, luego existen escalares $\alpha_1, \dots, \alpha_{d-1}$ no todos cero tales que

$$\mathbf{0} = \alpha_1 \mathbf{h}_{i_1} + \dots + \alpha_{d-1} \mathbf{h}_{i_{d-1}}.$$

Sea $t = \max\{1 \leq s \leq d-1 : \alpha_s \neq 0\}$, como $\mathbf{h}_1 \neq \mathbf{0}$ tenemos que $t > 1$, así $\mathbf{h}_{i_t} = \beta_1 \mathbf{h}_{i_1} + \dots + \beta_{t-1} \mathbf{h}_{i_{t-1}}$ con $\beta_s = -\alpha_s/\alpha_t$ para todo $1 \leq s \leq t-1$. Si $i_t \leq d-2$ entonces se contradice i) y si $i_t > d-2$ entonces se contradice ii) Por lo tanto, cualquier conjunto formado por $d-1$ de los n vectores $\mathbf{h}_1, \dots, \mathbf{h}_n$ es linealmente independiente, $\square$

Corolario 3.39. Sean n, k y d enteros con $d > 1$ y $k \geq 1$. Entonces existe un $[n, k]$ código sobre $\mathbb{F}_q$ con distancia mínima al menos d , siempre que

$$1 + \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i \leq q^{n-k}.$$

Demostración. Por la *Proposición 3.38* existe una matriz H con entradas en $\mathbb{F}_q$ y tamaño $(n - k) \times n$ tal que todo conjunto de $d - 1$ columnas de H es linealmente independiente. Sean $\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n : H\mathbf{x}^T = \mathbf{0}\}$ y $k' = \dim(\mathcal{C})$, por el Teorema de la dimensión $\rho(H) = n - k'$, dado que el rango de una matriz es igual a la dimensión de su espacio fila tenemos que el mayor número de filas linealmente independientes de H es $n - k'$, ahora como el número total de filas de H es $n - k$ se sigue que $n - k' \leq n - k$ y por ende $k' \geq k$; por otra parte, el *Teorema 2.46* garantiza que existe un conjunto de $d(\mathcal{C})$ columnas de H que es linealmente dependiente, si $d(\mathcal{C}) \leq d - 1$ tendríamos que existe un conjunto de $d - 1$ columnas de H linealmente dependiente, lo cual no puede ser, por lo tanto, $d(\mathcal{C}) \geq d$. Si $\mathcal{C}'$ es cualquier subcódigo de $\mathcal{C}$ de dimensión k concluimos que $\mathcal{C}'$ es un $[n, k]_q$ código con distancia mínima al menos d . $\square$

Teorema 3.40. (Cota de Varshamov) Sea $d > 1$. Entonces

$$B_q(n, d) \geq q^{n - \lceil \log_q (1 + \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i) \rceil}.$$

Demostración. Claramente, $\log_q L \leq \lceil \log_q L \rceil$ para todo $L > 0$, luego $L \leq q^{n - (n - \lceil \log_q L \rceil)}$. Si $L = 1 + \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$ entonces

$$1 + \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i \leq q^{n - (n - \lceil \log_q L \rceil)}.$$

Como $n \geq d$ tenemos que $n - 1 \geq d - 1 > d - 2$ y

$$q^{n-1} = ((q-1) + 1)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} (q-1)^i > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i,$$

luego $q^{n-1} \geq L$ y por ende $n - 1 \geq \log_q L$, esto último implica que $n > n - 1 \geq \lceil \log_q L \rceil$. Así las cosas, $0 < n - \lceil \log_q L \rceil < n$ y por el *Corolario 3.39* existe un $[n, n - \lceil \log_q L \rceil]$ código sobre $\mathbb{F}_q$ con distancia mínima al menos d , así

$$B_q(n, d) \geq q^{n - \lceil \log_q L \rceil}.$$

$\square$

4

COTAS ASINTÓTICAS

En la primera sección de este capítulo expondremos el principal problema asintótico de la teoría de códigos y la función de Manin, tomando como referencia [8]. Luego, estudiaremos cotas para la función de Manin, en esta parte seguiremos [[2], capítulo 2, sección 10]. Finalmente, presentaremos las propiedades de la función de Manin establecidas en [6], apoyándonos en [8].

4.1 EL PRINCIPAL PROBLEMA ASINTÓTICO Y LA FUNCIÓN DE MANIN

En aras de encontrar buenos códigos lineales, en el capítulo anterior fijábamos una longitud n y una potencia prima q , y dado un entero no negativo d intentábamos calcular $B_q(n, d)$, de hecho como esto no siempre era sencillo nos enfocábamos en dar cotas tanto superiores como inferiores para esta cantidad. Ahora bien, al fijar n la cota de Singleton produce una restricción sobre la dimensión y la distancia mínima de cualquier $[n, k, d]_q$ código y recordemos que al buscar buenos códigos lineales pretendemos que k y d sean muy grandes con el fin de transmitir una amplia variedad de mensajes y corregir una gran cantidad de errores, es por esto que en este capítulo para la búsqueda de buenos códigos lineales no fijaremos n sino que trabajaremos con algo del estilo $n \rightarrow \infty$, la siguiente proposición muestra que para esto debemos trabajar con sucesiones de códigos lineales distintos.

Proposición 4.1. Sea $\{\mathcal{C}_i\}_i$ una sucesión de códigos lineales (distintos) sobre un mismo cuerpo $\mathbb{F}_q$ tal que la longitud de $\mathcal{C}_i$ es n_i para cada i . Entonces $n_i \rightarrow \infty$ cuando $i \rightarrow \infty$.

Demostración. Debemos mostrar que dado $M > 0$ existe un entero positivo N tal que $n_i > M$ siempre que $i > N$. Supongamos lo contrario, así existe $M > 0$ tal que $n_i \leq M$ para todo $i > 1$, como

$$\{i : n_i \leq M\} = \bigcup_{L=1}^{\lfloor M \rfloor} \{i : n_i = L\},$$

tenemos que

$$\sum_{L=1}^{\lfloor M \rfloor} |\{i : n_i = L\}| = \infty.$$

Por lo tanto, existe un entero positivo $L' \leq \lfloor M \rfloor$ tal que $|\{i : n_i = L'\}| = \infty$; en otras palabras, existe una cantidad infinita de códigos lineales sobre $\mathbb{F}_q$ cuya longitud es L' , esto contradice la *Proposición 2.11*, por lo tanto, $n_i \rightarrow \infty$ cuando $i \rightarrow \infty$. $\square$

Cabe aclarar que lo hecho en el capítulo anterior no fue en vano pues muchas de las cotas vistas previamente nos serán de utilidad. Los conceptos de tasa de transmisión y distancia relativa que veremos a continuación nos permitirán establecer el principal problema asintótico de la teoría de códigos.

Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$, la *tasa de transmisión* y la *distancia relativa* de $\mathcal{C}$ se definen como

$$R := R(\mathcal{C}) := \frac{\log_q M}{n} \quad \text{y} \quad \delta = \delta(\mathcal{C}) := \frac{d}{n},$$

respectivamente.

Observación 4.2. Sea $\mathcal{C}$ un (n, M, d) código sobre $\mathbb{F}_q$ entonces $R(\mathcal{C}), \delta(\mathcal{C}) \in [0, 1] \cap \mathbb{Q}$ puesto que $1 \leq M \leq q^n$ y $0 \leq d \leq n$. Si $\mathcal{C}$ es lineal y $k = \dim(\mathcal{C})$ entonces $R(\mathcal{C}) = k/n$.

De todas las posibles sucesiones de códigos lineales sobre un mismo cuerpo, estudiaremos aquellas sucesiones cuyas tasas de transmisión y distancias relativas tiendan a constantes positivas, pues en virtud del siguiente lema en dichas sucesiones hay buenos códigos lineales, ya que en dichas sucesiones hay códigos lineales cuya tasa de transmisión y distancia relativa son tan grandes como se quiera.

Lema 4.3. Sea $\{\mathcal{C}_i\}_i$ una sucesión (sucesión) de códigos lineales sobre un mismo cuerpo $\mathbb{F}_q$ tal que cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]_q$ código, si $d_i/n_i \rightarrow \delta$ y $k_i/n_i \rightarrow R$ cuando $i \rightarrow \infty$, con δ y R constantes positivas entonces $k_i \rightarrow \infty$ y $d_i \rightarrow \infty$ cuando $i \rightarrow \infty$.

Demostración. Por la *Proposición 4.1* tenemos que

$$\lim_{i \rightarrow \infty} k_i = \lim_{i \rightarrow \infty} \frac{k_i n_i}{n_i} = R \lim_{i \rightarrow \infty} n_i = \infty.$$

Análogamente, se verifica que $d_i \rightarrow \infty$ cuando $i \rightarrow \infty$. □

Ahora, dada una potencia prima q , sean

$$C_q := \{\mathcal{C} : \mathcal{C} \text{ es un código lineal sobre } \mathbb{F}_q\},$$

$$V_q := \text{Im}(\psi),$$

siendo $\psi : C_q \rightarrow [0, 1]^2$ la función dada por $\psi(\mathcal{C}) = (\delta(\mathcal{C}), R(\mathcal{C}))$ para todo $\mathcal{C} \in C_q$, y

$$U_q := \{x : x \text{ es un punto de acumulación de } V_q\}^1.$$

La siguiente proposición caracteriza los puntos de acumulación U_q de V_q .

Proposición 4.4. $(\delta, R) \in U_q$ si y solo si existe una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que

$$\delta(\mathcal{C}_i) \rightarrow \delta, \quad R(\mathcal{C}_i) \rightarrow R,$$

cuando $i \rightarrow \infty$. Más aún, $(\delta(\mathcal{C}_i), R(\mathcal{C}_i)) \neq (\delta, R)$ para todo i .

Demostración. Por la definición de punto de acumulación, $(\delta, R) \in U_q$ si y solo si existe una sucesión $\{(a_i, b_i)\}_i \subseteq V_q \setminus \{(\delta, R)\}$ tal que $(a_i, b_i) \rightarrow (\delta, R)$ cuando $i \rightarrow \infty$. Como $\{(a_i, b_i)\}_i \subseteq V_q$ tenemos que para cada entero positivo i existe un código lineal sobre $\mathbb{F}_q$, digamos $\mathcal{C}_i$, tal que $\delta(\mathcal{C}_i) = a_i$ y $R(\mathcal{C}_i) = b_i$. Así las cosas, $(\delta, R) \in U_q$ si y solo si existe una sucesión $\{\mathcal{C}_i\}_i$ de códigos lineales sobre $\mathbb{F}_q$ tal que $(\delta(\mathcal{C}_i), R(\mathcal{C}_i)) \neq (\delta, R)$ para todo i y

$$(\delta(\mathcal{C}_i), R(\mathcal{C}_i)) \rightarrow (\delta, R), \quad \text{siempre que } i \rightarrow \infty.$$

Luego, dado $\varepsilon > 0$ existe un entero positivo I tal que

$$\sqrt{(\delta(\mathcal{C}_i) - \delta)^2 + (R(\mathcal{C}_i) - R)^2} < \varepsilon, \quad \text{para todo } i \geq I.$$

Claramente, $(\delta(\mathcal{C}_i) - \delta)^2 \leq (\delta(\mathcal{C}_i) - \delta)^2 + (R(\mathcal{C}_i) - R)^2$ para todo i . Luego

$$|\delta(\mathcal{C}_i) - \delta| < \varepsilon, \quad \text{para todo } i \geq I.$$

Análogamente, $|R(\mathcal{C}_i) - R| < \varepsilon$ para todo $i \geq I$ y por lo tanto $\delta(\mathcal{C}_i) \rightarrow \delta$ y $R(\mathcal{C}_i) \rightarrow R$ cuando $i \rightarrow \infty$. □

¹Consideraremos la métrica Euclidiana sobre $\mathbb{R}^2$ para $t = 1, 2$

Así las cosas, el *principal problema asintótico* de la teoría de códigos consiste en determinar los puntos de acumulación (con ambas componentes no nulas) de V_q .

Manin demostró en el artículo [6] que existe una función continua $\alpha_q : [0, 1] \rightarrow [0, 1]$ tal que el conjunto de puntos de acumulación de V_q es

$$U_q = \{(\delta, R) : 0 \leq \delta \leq 1 \text{ y } 0 \leq R \leq \alpha_q(\delta)\},$$

además $\alpha_q(0) = 1$, α_q es estrictamente decreciente en $[0, 1 - q^{-1}]$ y $\alpha_q(\delta) = 0$ para $1 - q^{-1} \leq \delta \leq 1$. La prueba de estos resultados se encuentra en los *Teoremas* 4.5, 4.7, 4.26 y 4.28, y en el *Corolario* 4.25.

La *función de Manin*, denotada por α_q , se define como

$$\begin{aligned} \alpha_q : [0, 1] &\rightarrow [0, 1] \\ \delta &\mapsto \sup \{R : (\delta, R) \in U_q\}. \end{aligned}$$

El siguiente teorema garantiza la existencia de esta función y muestra que $\alpha_q(0) = 1$.

Teorema 4.5. Sea $\delta \in [0, 1]$. Entonces $\sup \{R : (\delta, R) \in U_q\}$ existe, más aún $\sup \{R : (\delta, R) \in U_q\} \in [0, 1]$ y $\sup \{R : (0, R) \in U_q\} = 1$.

Demostración. Sean $\delta \in (0, 1]$ y $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que $\mathcal{C}_i = \text{Gen}\{\mathbf{c}_i\}$ siendo $\mathbf{c}_i$ cualquier vector en $\mathbb{F}_q^i$ de peso $[\delta i]$, así $\delta(\mathcal{C}_i) = [\delta i]/i$ y $R(\mathcal{C}_i) = 1/i$ para todo i . Como $\delta \leq [\delta i]/i < \delta + 1/i$ tenemos por el Teorema del encaje y la *Proposición* 4.1 que $\delta(\mathcal{C}_i) \rightarrow \delta$ y $R(\mathcal{C}_i) \rightarrow 0$ cuando $i \rightarrow \infty$, luego la *Proposición* 4.4 garantiza que $(\delta, 0) \in U_q$. Por otra parte, sea $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que $\mathcal{C}_i = \mathbb{F}_q^i$, luego $\delta(\mathcal{C}_i) = 1/i$ y $R(\mathcal{C}_i) = 1$ para todo i lo cual implica, por las *Proposiciones* 4.1 y 4.4, que $(0, 1) \in U_q$.

En resumen, si $\delta \in [0, 1]$ entonces $\{R : (\delta, R) \in U_q\} \neq \emptyset$, además $1 \in \{R : (0, R) \in U_q\}$; por otra parte, por la *Observación* 4.2 y la *Proposición* 4.4 tenemos que si $R \in \{R : (\delta, R) \in U_q\}$ entonces $0 \leq R \leq 1$. Así las cosas, el Axioma de completitud garantiza que $\{R : (\delta, R) \in U_q\}$ existe para todo $\delta \in [0, 1]$, por la definición de supremo concluimos que $\{R : (\delta, R) \in U_q\} \in [0, 1]$ y que $\sup \{R : (0, R) \in U_q\} = 1$. $\square$

4.2 COTA ASINTÓTICA DE SINGLETON

El valor exacto de $\alpha_q(\delta)$ es desconocido para $0 < \delta < 1 - q^{-1}$, por ello en esta y en las siguientes secciones nos enfocaremos en dar cotas superiores e inferiores para la función de Manin. La primera cota superior que veremos es la cota asintótica de Singleton.

Teorema 4.6. (Cota asintótica de Singleton) Sea $0 \leq \delta \leq 1$. Entonces $\alpha_q(\delta) \leq 1 - \delta$.

Demostración. Sea R tal que $(\delta, R) \in U_q$. Por la *Proposición* 4.4, existe una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]_q$ código entonces

$$\frac{d_i}{n_i} \rightarrow \delta, \quad \frac{k_i}{n_i} \rightarrow R, \quad \text{cuando } i \rightarrow \infty$$

además $(d_i/n_i, k_i/n_i) \neq (\delta, R)$ para todo i , por la cota de Singleton tenemos que

$$\frac{k_i}{n_i} \leq 1 - \frac{d_i}{n_i} + \frac{1}{n_i} \quad \text{para todo } i.$$

Luego

$$\lim_{i \rightarrow \infty} \frac{k_i}{n_i} \leq \lim_{i \rightarrow \infty} \left(1 - \frac{d_i}{n_i} + \frac{1}{n_i}\right),$$

de la *Proposición* 4.1 se sigue que $R \leq 1 - \delta$, por lo tanto $1 - \delta$ es una cota superior de $\{R : (\delta, R) \in U_q\}$, por la definición de supremo concluimos que $\alpha_q(\delta) \leq 1 - \delta$. $\square$

4.3 COTA ASINTÓTICA DE PLOTKIN

La cota asintótica de Plotkin además de mejorar la cota asintótica de Singleton nos muestra que la función de Manin es nula en $[1 - q^{-1}, 1]$.

Teorema 4.7. (Cota asintótica de Plotkin) Sean $0 \leq \delta \leq 1$ y $r = 1 - q^{-1}$. Entonces

$$\alpha_q(\delta) \leq \max \left\{ 1 - \frac{\delta}{r}, 0 \right\}.$$

Demostración. Si $\delta = r$ el resultado es inmediato. Sea R tal que $(\delta, R) \in U_q$, luego la *Proposición 4.4* garantiza la existencia de una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]_q$ código entonces

$$\frac{d_i}{n_i} \rightarrow \delta, \quad \frac{k_i}{n_i} \rightarrow R, \quad \text{cuando } i \rightarrow \infty. \quad (4.1)$$

En primer lugar, supongamos que $r < \delta$, así $\max \{1 - \delta/r, 0\} = 0$ y veamos que $R = 0$. Como $\delta - r > 0$, por (4.1) tenemos que existe un entero positivo I tal que

$$\left| \frac{d_i}{n_i} - \delta \right| < \delta - r \quad \text{siempre que } i > I.$$

De aquí que

$$r - \delta < \frac{d_i}{n_i} - \delta \quad \text{para todo } i > I.$$

En otras palabras, $rn_i < d_i$ para todo $i > I$, luego, por la cota de Plotkin

$$A_q(n_i, d_i) \leq \left\lfloor \frac{d_i}{d_i - rn_i} \right\rfloor \quad \text{para todo } i > I, \quad (4.2)$$

esto implica, por la *Proposición 3.1* y la definición de parte entera, que

$$q^{k_i} \leq \frac{d_i}{d_i - rn_i} \quad \text{para todo } i > I.$$

Como la función logaritmo en base q es creciente se sigue que

$$\frac{k_i}{n_i} \leq \frac{1}{n_i} \log_q \left(\frac{d_i}{d_i - rn_i} \right) \quad \text{para todo } i > I,$$

y por ende

$$R \leq \lim_{i \rightarrow \infty} \left(\frac{1}{n_i} \log_q \left(\frac{d_i}{d_i - rn_i} \right) \right). \quad (4.3)$$

Ahora, como la función logaritmo en base q es continua tenemos que

$$\lim_{i \rightarrow \infty} \left(\log_q \left(\frac{d_i}{d_i - rn_i} \right) \right) = \log_q \left(\lim_{i \rightarrow \infty} \left(\frac{d_i}{d_i - rn_i} \right) \right) = \log_q \left(\lim_{i \rightarrow \infty} \left(\frac{\frac{d_i}{n_i}}{\frac{d_i}{n_i} - r} \right) \right) = \log_q \left(\frac{\delta}{\delta - r} \right),$$

así

$$\lim_{i \rightarrow \infty} \left(\frac{1}{n_i} \log_q \left(\frac{d_i}{d_i - rn_i} \right) \right) = \log_q \left(\frac{\delta}{\delta - r} \right) \lim_{i \rightarrow \infty} \frac{1}{n_i} = 0,$$

por esto y (4.3) obtenemos que $R \leq 0$, por consiguiente $R = 0$. En resumen, si $r < \delta$ tenemos que $\{R : (\delta, R) \in U_q\} = \{0\}$, por lo tanto $\alpha_q(\delta) = 0$.

Supongamos ahora que $\delta < r$, luego $\max\{1 - \delta/r, 0\} = 1 - \delta/r$. Veamos que $R \leq 1 - \delta/r$. El resultado es inmediato para $\delta = 0$; supongamos que $0 < \delta < r$, por el *Lema 4.3*, dado que $r + 1 > 0$ tenemos que existe un entero positivo I tal que

$$d_i > r + 1 \text{ siempre que } i > I.$$

Por otra parte, como $r - \delta > 0$ tenemos que existe un entero positivo I' tal que

$$\left| \frac{d_i}{n_i} - \frac{1}{n_i} - \delta \right| < r - \delta \text{ siempre que } i > I'$$

Sea $J = \max\{I, I'\}$, luego

$$d_i > r + 1 \quad \text{y} \quad \left| \frac{d_i - 1}{n_i} - \delta \right| < r - \delta \text{ para todo } i > J. \quad (4.4)$$

Para cada $i > J$, sean $\mathcal{C}_i$ un (n_i, M_i, d_i) código sobre $\mathbb{F}_q$ con $M_i = A_q(n_i, d_i)$ y

$$n'_i = \left\lfloor \frac{d_i - 1}{r} \right\rfloor,$$

por (4.4), $1 \leq n'_i < n_i$. Para cada $\beta_{n'_i+1} \cdots \beta_{n_i} \in \mathbb{F}_q^{n_i-n'_i}$, sea

$$\mathcal{C}_i(\beta_{n'_i+1}, \dots, \beta_{n_i}) = \{ \mathbf{c} = c_1 \cdots c_{n_i} \in \mathcal{C}_i : c_j = \beta_j, \text{ para todo } n'_i + 1 \leq j \leq n_i \},$$

luego

$$\mathcal{C}_i = \bigsqcup_{\beta_{n'_i+1} \cdots \beta_{n_i} \in \mathbb{F}_q^{n_i-n'_i}} \mathcal{C}_i(\beta_{n'_i+1}, \dots, \beta_{n_i}),$$

lo cual implica que

$$M_i = \sum_{\beta_{n'_i+1} \cdots \beta_{n_i} \in \mathbb{F}_q^{n_i-n'_i}} |\mathcal{C}_i(\beta_{n'_i+1}, \dots, \beta_{n_i})|. \quad (4.5)$$

Note que existe $\gamma_{n'_i+1} \cdots \gamma_{n_i} \in \mathbb{F}_q^{n_i-n'_i}$ tal que

$$|\mathcal{C}_i(\gamma_{n'_i+1}, \dots, \gamma_{n_i})| = M'_i \geq \frac{M_i}{q^{n_i-n'_i}}, \quad (4.6)$$

pues si para todo $\beta_{n'_i+1}, \dots, \beta_{n_i} \in \mathbb{F}_q^{n_i-n'_i}$ se cumpliera que $|\mathcal{C}_i(\beta_{n'_i+1}, \dots, \beta_{n_i})| < M_i/q^{n_i-n'_i}$ tendríamos que

$$\sum_{\beta_{n'_i+1} \cdots \beta_{n_i} \in \mathbb{F}_q^{n_i-n'_i}} |\mathcal{C}_i(\beta_{n'_i+1}, \dots, \beta_{n_i})| < q^{n_i-n'_i} \left(\frac{M_i}{q^{n_i-n'_i}} \right) = M_i,$$

lo que contradice (4.5). Así las cosas,

$$\mathcal{C}'_i = \{ c_1 \cdots c_{n'_i} : c_1 \cdots c_{n_i} \in \mathcal{C}_i(\gamma_{n'_i+1}, \dots, \gamma_{n_i}) \}.$$

es un código sobre $\mathbb{F}_q$ de longitud n'_i . Claramente, la función

$$\begin{aligned} f : \mathcal{C}_i(\gamma_{n'_i+1}, \dots, \gamma_{n_i}) &\rightarrow \mathcal{C}'_i \\ c_1 \cdots c_{n'_i} \gamma_{n'_i+1} \cdots \gamma_{n_i} &\mapsto c_1 \cdots c_{n'_i}, \end{aligned}$$

es sobreyectiva; supongamos que existen $\mathbf{u} = u_1 \cdots u_{n_i}, \mathbf{v} = v_1 \cdots v_{n_i}$ en $\mathcal{C}_i(\gamma_{n'_i+1}, \dots, \gamma_{n_i})$ tales que $u_j = v_j$ para todo $1 \leq j \leq n'_i$. Como $u_j = v_j = \gamma_j$ para todo $n'_i + 1 \leq j \leq n_i$ tenemos que $\mathbf{u} = \mathbf{v}$, de aquí que f es inyectiva y

$$|\mathcal{C}'_i| = |\mathcal{C}_i(\gamma_{n'_i+1}, \dots, \gamma_{n_i})| = M'_i.$$

Si $M_i/(q^{n_i-n'_i}) \leq 1$ tendríamos que $q^{n_i} \leq M_i \leq q^{n_i-n'_i}$, luego $n'_i \leq 0$ pero $n'_i \geq 1$, por ende $M_i/(q^{n_i-n'_i}) > 1$ y por (4.6) $M'_i > 1$, así $d(\mathcal{C}'_i) > 0$. Si $d(\mathcal{C}'_i) < d_i$ tendríamos que existen $\mathbf{u} = u_1 \cdots u_{n'_i}, \mathbf{v} = v_1 \cdots v_{n'_i}$ en $\mathcal{C}'_i$ tales que $d(\mathcal{C}'_i) = d(\mathbf{u}, \mathbf{v})$, luego $\mathbf{u}' = u_1 \cdots u_{n'_i} \gamma_{n'_i+1} \cdots \gamma_{n_i}, \mathbf{v}' = v_1 \cdots v_{n'_i} \gamma_{n'_i+1} \cdots \gamma_{n_i} \in \mathcal{C}_i$ y $0 < d(\mathbf{u}', \mathbf{v}') < d_i$ pero esto contradice la minimalidad de d_i , por lo tanto $d(\mathcal{C}'_i) \geq d_i$.

En resumen, para cada $i > J$ existe un (n'_i, M'_i, d'_i) código sobre $\mathbb{F}_q$ con $M'_i \geq M_i/q^{n_i-n'_i}$ y $d'_i \geq d_i$, luego, por la *Proposición 3.4*

$$A_q(n'_i, d_i) \geq M'_i \geq \frac{M_i}{q^{n_i-n'_i}} \text{ para todo } i > J. \quad (4.7)$$

Como

$$rn'_i = r \left\lfloor \frac{d_i - 1}{r} \right\rfloor \leq r \left(\frac{d_i - 1}{r} \right) = d_i - 1 < d_i, \quad (4.8)$$

tenemos, por la cota de Plotkin, que

$$A_q(n'_i, d_i) \leq \left\lfloor \frac{d_i}{d_i - rn'_i} \right\rfloor \text{ para todo } i > J. \quad (4.9)$$

Por las desigualdades (4.7) y (4.9)

$$M_i \leq \left\lfloor \frac{d_i}{d_i - rn'_i} \right\rfloor q^{n_i-n'_i} \text{ para todo } i > J.$$

Por (4.8) $d_i - rn'_i \geq 1$, luego

$$\left\lfloor \frac{d_i}{d_i - rn'_i} \right\rfloor \leq \frac{d_i}{d_i - rn'_i} \leq d_i.$$

Así, $M_i \leq d_i q^{n_i-n'_i}$ y $A_q(n_i, d_i) \leq d_i q^{n_i-n'_i}$ para todo $i > J$; por la *Proposición 3.1* se tiene que $q^{k_i} \leq d_i q^{n_i-n'_i}$ y como la función logaritmo en base q es creciente entonces

$$\frac{k_i}{n_i} \leq \frac{\log_q d_i}{n_i} + 1 - \frac{n'_i}{n_i} \text{ para todo } i > J,$$

esto implica que

$$R \leq \lim_{i \rightarrow \infty} \left(\frac{\log_q d_i}{n_i} + 1 - \frac{n'_i}{n_i} \right). \quad (4.10)$$

Observe que

$$\frac{\left\lfloor \frac{d_i-1}{r} \right\rfloor}{n_i} \leq \frac{d_i-1}{rn_i} = \frac{d_i}{rn_i} - \frac{1}{rn_i},$$

y

$$\frac{\left\lfloor \frac{d_i-1}{r} \right\rfloor}{n_i} > \frac{\frac{d_i-1}{r} - 1}{n_i} = \frac{d_i}{rn_i} - \frac{1}{rn_i} - \frac{1}{n_i},$$

así, por el Teorema del encaje

$$\lim_{i \rightarrow \infty} \frac{n'_i}{n_i} = \frac{\delta}{r}. \quad (4.11)$$

Concluimos de (4.10), (4.11) y del *Lema* 4.3 que

$$R \leq 1 - \frac{\delta}{r}.$$

Así las cosas, si $0 < \delta < r$ entonces $1 - \delta/r$ es una cota superior de $\{R : (\delta, R) \in U_q\}$. Por lo tanto, si $0 < \delta < r$ entonces $\alpha_q(\delta) \leq 1 - \delta/r$. $\square$

Corolario 4.8. Sea $(\delta, R) \in U_q$ con $\delta > 0$ y $R > 0$. Entonces $\delta < 1$, $R < 1$ y $\delta + R < 1$.

Demostración. Como $\delta > 0$ tenemos por la cota asintótica de Singleton que $R < 1$; sea $r = 1 - q^{-1}$, si $\delta \geq r$ tendríamos por la cota asintótica de Plotkin que $R = 0$ pero esto contradice la hipótesis, luego $0 < \delta < r < 1$, por ende $R \leq \alpha_q(\delta) \leq 1 - \delta/r$, como $r < 1$ tenemos que $1 - \delta/r < 1 - \delta$, por lo tanto $R < 1 - \delta$. $\square$

4.4 LA FUNCIÓN DE ENTROPÍA DE HILBERT

La función de entropía de Hilbert nos permitirá establecer más adelante las cotas asintóticas de Hamming, Elias y Gilbert-Varshamov.

Proposición 4.9. Sean n y d enteros positivos tales que $n > d > 2$. Entonces

$$n \log_q n - d \log_q d - (n - d) \log_q (n - d) < \log_q n - (d - 1) \log_q \left(\frac{d - 1}{n} \right) - (n - d) \log_q \left(1 - \frac{d}{n} \right).$$

Demostración. Observe que

$$(d - 1) \log_q \left(\frac{d - 1}{n} \right) = \log_q (d - 1)^{(d-1)} - d \log_q n + \log_q n,$$

y

$$(n - d) \log_q \left(1 - \frac{d}{n} \right) = \log_q (n - d)^{(n-d)} - n \log_q n + d \log_q n,$$

luego, todo se reduce a probar que

$$\log_q (d - 1)^{(d-1)} < \log_q d^d.$$

Como $1 < d - 1 < d$ tenemos que la funciones

$$\begin{array}{ll} f : \mathbb{R} \rightarrow \mathbb{R}^+ & g : \mathbb{R} \rightarrow \mathbb{R}^+ \\ x \mapsto f(x) = x^{d-1} & x \mapsto g(x) = d^x \end{array}$$

son estrictamente crecientes, así

$$0 < (d - 1)^{(d-1)} < d^{(d-1)} < d^d.$$

Por lo tanto,

$$\log_q (d - 1)^{(d-1)} < \log_q d^d.$$

$\square$

Proposición 4.10. Sean n y d enteros positivos tales que $n > d$. Entonces

$$n \log_q n - d \log_q d - (n - d) \log_q (n - d) > -\log_q n - d \log_q \left(\frac{d}{n} \right) - (n - d + 1) \log_q \left(\frac{n - d + 1}{n} \right).$$

Demostración. Observe que

$$d \log_q \left(\frac{d}{n} \right) = d \log_q d - d \log_q n,$$

y

$$(n-d+1) \log_q \left(\frac{n-d+1}{n} \right) = \log_q (n-d+1)^{(n-d+1)} - n \log_q n + d \log_q n - \log_q n,$$

luego, es suficiente probar que

$$\log_q (n-d)^{(n-d)} < \log_q (n-d+1)^{(n-d+1)}.$$

Si $n-d=1$, el resultado es inmediato. Supongamos que $1 < n-d < n-d+1$ esto implica que las funciones

$$\begin{array}{ll} f: \mathbb{R} \rightarrow \mathbb{R}^+ & g: \mathbb{R} \rightarrow \mathbb{R}^+ \\ x \mapsto f(x) = x^{n-d} & x \mapsto g(x) = (n-d+1)^x \end{array}$$

son estrictamente crecientes, así

$$0 < (n-d)^{(n-d)} < (n-d+1)^{(n-d)} < (n-d+1)^{(n-d+1)}.$$

Por lo tanto,

$$\log_q (n-d)^{(n-d)} < \log_q (n-d+1)^{(n-d+1)}.$$

□

Proposición 4.11. Sean $0 < \delta < 1$, $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que cada $\mathcal{C}_i$ es un código de longitud n_i y distancia mínima d_i . Si $d_i/n_i \rightarrow \delta$ cuando $i \rightarrow \infty$ entonces

$$\lim_{i \rightarrow \infty} \frac{n_i \log_q n_i - d_i \log_q d_i - (n_i - d_i) \log_q (n_i - d_i)}{n_i} = -\delta \log_q \delta - (1 - \delta) \log_q (1 - \delta).$$

Demostración. Por el Lema 4.3 existe un entero positivo I tal que $d_i > 2$ siempre que $i > I$. Por otra parte, como $1 - \delta > 0$ y $d_i/n_i \rightarrow \delta$ cuando $i \rightarrow \infty$, tenemos que existe un entero positivo I' tal que

$$\left| \frac{d_i}{n_i} - \delta \right| < 1 - \delta \text{ siempre que } i > I',$$

así, $d_i < n_i$, para todo $i > I'$. Sea $J = \max\{I, I'\}$, luego

$$n_i > d_i > 2 \text{ para todo } i > J. \quad (4.12)$$

Sean

$$\begin{aligned} m(i) &= n_i \log_q n_i - d_i \log_q d_i - (n_i - d_i) \log_q (n_i - d_i), \\ m_1(i) &= -\log_q n_i - d_i \log_q \left(\frac{d_i}{n_i} \right) - (n_i - d_i + 1) \log_q \left(\frac{n_i - d_i + 1}{n_i} \right), \\ m_2(i) &= \log_q n_i - (d_i - 1) \log_q \left(\frac{d_i - 1}{n_i} \right) - (n_i - d_i) \log_q \left(1 - \frac{d_i}{n_i} \right). \end{aligned}$$

Por (4.12) y las *Proposiciones* 4.9 y 4.10 tenemos que

$$\frac{m_1(i)}{n_i} < \frac{m(i)}{n_i} < \frac{m_2(i)}{n_i} \text{ para todo } i > J.$$

Por la *Proposición 4.1*, el *Lema 4.3* y dado que logaritmo en base q es una función continua, se sigue que

$$\lim_{i \rightarrow \infty} \frac{m_1(i)}{n_i} = \lim_{i \rightarrow \infty} \frac{m_2(i)}{n_i} = -\delta \log_q \delta - (1 - \delta) \log_q (1 - \delta).$$

Del Teorema del encaje concluimos que

$$\lim_{i \rightarrow \infty} \frac{m(i)}{n_i} = -\delta \log_q \delta - (1 - \delta) \log_q (1 - \delta).$$

□

Proposición 4.12. Sean n y q enteros positivos con $q \geq 2$. Si i es un entero positivo tal que $i \leq (1 - q^{-1})n$ entonces

$$\binom{n}{i-1} (q-1)^{i-1} < \binom{n}{i} (q-1)^i.$$

Demostración. Claramente, $1 - q^{-1} < 1$, luego $i-1 < i < n$ y por consiguiente tiene sentido hablar de $\binom{n}{i-1}$ y $\binom{n}{i}$. Por la definición de coeficiente binomial, es suficiente probar que

$$i < (q-1)(n-i+1).$$

Como $i \leq (1 - q^{-1})n$ y $q-1 > 0$ tenemos que

$$iq \leq (q-1)n < (q-1)n + (q-1),$$

así,

$$i(q+1-1) < (q-1)(n+1),$$

lo cual equivale a

$$i + (q-1)i < (q-1)(n+1),$$

restando $(q-1)i$ a ambos lados de esta desigualdad obtenemos lo deseado. □

Dado $0 \leq \delta < r$ con $r = 1 - q^{-1}$ y $q \geq 2$ definimos la *función de Entropía de Hilbert* de δ , denotada por $H_q(\delta)$, como

$$H_q(\delta) = \begin{cases} \delta \log_q (q-1) - \delta \log_q \delta - (1 - \delta) \log_q (1 - \delta) & \text{si } 0 < \delta < r \\ 0 & \text{si } \delta = 0. \end{cases}$$

Proposición 4.13. Sea $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que cada $\mathcal{C}_i$ es un código de longitud n_i y distancia mínima d_i . Si $0 < d_i/n_i \leq 1 - q^{-1}$ para cada i y $d_i/n_i \rightarrow \delta$ cuando $i \rightarrow \infty$ entonces

$$\lim_{i \rightarrow \infty} \frac{\log_q (V_q(n_i, d_i))}{n_i} = H_q(\delta).$$

Demostración. Por (2.5)

$$V_q(n_i, d_i) = \sum_{r=0}^{d_i} \binom{n_i}{r} (q-1)^r \quad \text{para todo } i,$$

de aquí que

$$\binom{n_i}{d_i} (q-1)^{d_i} \leq V_q(n_i, d_i) \quad \text{para todo } i.$$

Como $0 < d_i - j < d_i \leq (1 - q^{-1})n_i$ para todo i y para todo $1 \leq j \leq d_i - 1$ tenemos, por la *Proposición 4.12*, que

$$1 < \binom{n_i}{1}(q-1) < \cdots < \binom{n_i}{d_i-2}(q-1)^{d_i-2} < \binom{n_i}{d_i-1}(q-1)^{d_i-1} < \binom{n_i}{d_i}(q-1)^{d_i} \text{ para todo } i,$$

por consiguiente

$$V_q(n_i, d_i) \leq (1 + d_i) \binom{n_i}{d_i} (q-1)^{d_i} \text{ para todo } i.$$

Así las cosas,

$$\binom{n_i}{d_i} (q-1)^{d_i} \leq V_q(n_i, d_i) \leq (1 + d_i) \binom{n_i}{d_i} (q-1)^{d_i} \text{ para todo } i.$$

Tomando logaritmos en base q y multiplicando por $1/n_i$, obtenemos

$$A + \frac{d_i \log_q (q-1)}{n_i} \leq \frac{\log_q V_q(n_i, d_i)}{n_i} \leq A + \frac{\log_q (1 + d_i)}{n_i} + \frac{d_i \log_q (q-1)}{n_i} \text{ para todo } i,$$

donde $A = (\log_q \binom{n_i}{d_i})/n_i$. Observe que

$$\frac{\log_q (1 + d_i)}{n_i} = \frac{\log_q \left(\frac{1}{n_i} + \frac{d_i}{n_i} \right)}{n_i} + \frac{\log_q n_i}{n_i} \text{ para todo } i,$$

luego, por la *Proposición 4.1* y el *Lema 4.3*

$$\lim_{i \rightarrow \infty} \frac{\log_q (1 + d_i)}{n_i} = 0.$$

Por lo tanto, del Teorema del encaje

$$\lim_{i \rightarrow \infty} \frac{\log_q V_q(n_i, d_i)}{n_i} = \lim_{i \rightarrow \infty} \left(A + \frac{d_i \log_q (q-1)}{n_i} \right) = \lim_{i \rightarrow \infty} A + \delta \log_q (q-1).$$

Resta verificar que

$$\lim_{i \rightarrow \infty} A = -\delta \log_q \delta - (1 - \delta) \log_q (1 - \delta).$$

La fórmula de Stirling establece que

$$n^{n+1/2} e^{-n+7/8} \leq n! \leq n^{n+1/2} e^{-n+1} \text{ para todo } n \in \mathbb{Z}^+,$$

por esto y la definición de coeficiente binomial, tenemos que

$$\frac{n_i^{n_i+1/2} e^{-n_i+7/8}}{d_i^{d_i+1/2} e^{-d_i+1} (n_i - d_i)^{(n_i-d_i)+1/2} e^{-(n_i-d_i)+1}} \leq \binom{n_i}{d_i},$$

y

$$\binom{n_i}{d_i} \leq \frac{n_i^{n_i+1/2} e^{-n_i+1}}{d_i^{d_i+1/2} e^{-d_i+7/8} (n_i - d_i)^{(n_i-d_i)+1/2} e^{-(n_i-d_i)+7/8}},$$

al simplificar, resulta

$$B e^{-9/8} \leq \binom{n_i}{d_i} \leq B e^{-3/4},$$

donde

$$B = \frac{n_i^{n_i+1/2}}{d_i^{d_i+1/2}(n_i - d_i)^{(n_i-d_i)+1/2}}.$$

Note que

$$\lim_{i \rightarrow \infty} \frac{\log_q B e^t}{n_i} = \lim_{i \rightarrow \infty} \frac{\log_q B}{n_i} + \lim_{i \rightarrow \infty} \frac{t \log_q e}{n_i} = \lim_{i \rightarrow \infty} \frac{\log_q B}{n_i} \text{ para todo } t \in \mathbb{R},$$

luego, por el Teorema del encaje

$$\begin{aligned} \lim_{i \rightarrow \infty} A &= \lim_{i \rightarrow \infty} \frac{\log_q B}{n_i} \\ &= \lim_{i \rightarrow \infty} \frac{n_i \log_q n_i - d_i \log_q d_i - (n_i - d_i) \log_q (n_i - d_i)}{n_i} \\ &\quad + \lim_{i \rightarrow \infty} \frac{\log_q n_i - \log_q d_i - \log_q (n_i - d_i)}{2n_i}. \end{aligned}$$

Como $\log_q (n_i - d_i) = \log_q (1 - (d_i/n_i)) + \log_q n_i$, por las *Proposiciones* 4.1, 4.11 y el *Lema* 4.3, concluimos que

$$\lim_{i \rightarrow \infty} A = -\delta \log_q \delta - (1 - \delta) \log_q (1 - \delta).$$

□

4.5 COTA ASINTÓTICA DE HAMMING

La cota asintótica de Hamming mejora en un intervalo la cota asintótica de Plotkin.

Lema 4.14. Sean n, d enteros tales que $n > 1$. Entonces

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \left\lfloor \frac{d}{2} \right\rfloor - 1 \geq \left\lfloor \frac{d}{2} - \frac{n}{n-1} \right\rfloor.$$

Demostración. En primer lugar, veamos que

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq \left\lfloor \frac{d}{2} \right\rfloor - 1.$$

Supongamos que d es par, esto es, $d = 2k$ con $k \in \mathbb{Z}^+$, entonces

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor k - \frac{1}{2} \right\rfloor = k - 1 = \left\lfloor \frac{d}{2} \right\rfloor - 1;$$

si por el contrario, d es de la forma $2k + 1$ con $k \in \mathbb{Z}^+$, tenemos que

$$\left\lfloor \frac{d-1}{2} \right\rfloor = k = \left\lfloor \frac{d}{2} \right\rfloor > \left\lfloor \frac{d}{2} \right\rfloor - 1.$$

Por otra parte, dado que $n > n-1 > 0$ tenemos que $n/(n-1) > 1$, luego

$$\frac{d}{2} - \frac{n}{n-1} < \frac{d}{2} - 1,$$

de aquí que

$$\left\lfloor \frac{d}{2} - \frac{n}{n-1} \right\rfloor < \frac{d}{2} - 1,$$

por la definición de la función parte entera, concluimos que

$$\left\lfloor \frac{d}{2} - \frac{n}{n-1} \right\rfloor \leq \left\lfloor \frac{d}{2} - 1 \right\rfloor = \left\lfloor \frac{d}{2} \right\rfloor - 1.$$

□

Teorema 4.15. (Cota asintótica de Hamming) Sea $0 < \delta < 1 - q^{-1}$. Entonces

$$\alpha_q(\delta) \leq 1 - H_q(\delta/2).$$

Demostración. Sea R tal que $(\delta, R) \in U_q$. Por la *Proposición* 4.4, existe una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]$ código sobre $\mathbb{F}_q$ entonces

$$\frac{d_i}{n_i} \rightarrow \delta, \quad \frac{k_i}{n_i} \rightarrow R \quad \text{cuando } i \rightarrow \infty.$$

Por la cota de Hamming

$$A_q(n_i, d_i) \leq \frac{q^{n_i}}{V_q\left(n_i, \left\lfloor \frac{d_i-1}{2} \right\rfloor\right)} \quad \text{para todo } i.$$

Por la *Proposición* 4.1 existe $I > 0$ tal que $n_i > 1$ siempre que $i > I$ y por el *Lema* 4.14

$$\left\lfloor \frac{d_i-1}{2} \right\rfloor \geq \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor \quad \text{para todo } i > I,$$

luego,

$$\sum_{r=0}^{\lfloor (d_i-1)/2 \rfloor} \binom{n_i}{r} (q-1)^r \geq \sum_{r=0}^{\lfloor (d_i/2) - (n_i/(n_i-1)) \rfloor} \binom{n_i}{r} (q-1)^r \quad \text{para todo } i > I,$$

así, por (2.5)

$$V_q\left(n_i, \left\lfloor \frac{d_i-1}{2} \right\rfloor\right) \geq V_q\left(n_i, \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor\right) \quad \text{para todo } i > I.$$

Así las cosas,

$$q^{k_i} \leq A_q(n_i, d_i) \leq \frac{q^{n_i}}{V_q\left(n_i, \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor\right)} \quad \text{para todo } i > I,$$

tomando logaritmo en base q y multiplicando a ambos lados por $1/n_i$, obtenemos

$$\frac{k_i}{n_i} \leq 1 - \frac{\log_q V_q\left(n_i, \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor\right)}{n_i} \quad \text{para todo } i > I,$$

por consiguiente,

$$R \leq 1 - \lim_{i \rightarrow \infty} \frac{\log_q V_q\left(n_i, \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor\right)}{n_i}.$$

Observe que

$$\left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i-1} \right\rfloor = \left\lfloor \frac{1}{2} \left(\frac{d_i}{n_i} - \frac{2}{n_i-1} \right) n_i \right\rfloor.$$

Ahora,

$$\frac{\frac{1}{2} \left(\frac{d_i}{n_i} - \frac{2}{n_i-1} \right) n_i}{n_i} - \frac{1}{n_i} < \frac{\left\lfloor \frac{1}{2} \left(\frac{d_i}{n_i} - \frac{2}{n_i-1} \right) n_i \right\rfloor}{n_i} \leq \frac{\frac{1}{2} \left(\frac{d_i}{n_i} - \frac{2}{n_i-1} \right) n_i}{n_i} \quad \text{para todo } i,$$

luego, del Teorema del encaje

$$\lim_{i \rightarrow \infty} \frac{\left\lfloor \frac{1}{2} \left(\frac{d_i}{n_i} - \frac{2}{n_i - 1} \right) n_i \right\rfloor}{n_i} = \frac{\delta}{2}.$$

y por la *Proposición 4.13*,

$$\lim_{i \rightarrow \infty} \frac{\log_q V_q \left(n_i, \left\lfloor \frac{d_i}{2} - \frac{n_i}{n_i - 1} \right\rfloor \right)}{n_i} = H_q \left(\frac{\delta}{2} \right),$$

de aquí que $1 - H_q(\delta/2)$ es una cota superior de $\{R : (\delta, R) \in U_q\}$. Por lo tanto, $\alpha_q(\delta) \leq 1 - H_q(\delta/2)$. $\square$

4.6 COTA ASINTÓTICA DE ELIAS

La última cota superior para la función de Manin que veremos es la cota asintótica que de Elias, la cual de hecho es mejor que todas las anteriores.

Lema 4.16. Sea $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que cada $\mathcal{C}_i$ es un código de longitud n_i , distancia mínima d_i y $d_i/n_i \rightarrow \delta$ cuando $i \rightarrow \infty$, con $\delta > 0$. Si x, r son reales positivos, $w_i = \lfloor xn_i \rfloor$ para todo i y $x^2 - 2rx + r\delta > 0$ entonces existe un entero positivo I tal que

$$w_i^2 - 2rn_iw_i + rn_id_i > 0 \text{ para todo } i > I.$$

Demostración. Por la *Proposición 4.1* existe un entero positivo N tal que $n_i > 1/x$ siempre que $i > N$, luego $w > xn_i - 1 > 0$, siempre que $i > N$, de aquí que

$$w_i^2 > x^2 n_i^2 - 2xn_i + 1 \text{ para todo } i > N,$$

así y dado que $d_i > d_i - 1$ para todo i , se sigue que

$$w_i^2 - 2rn_iw_i + rn_id_i > x^2 n_i^2 - 2xn_i + 1 - 2rxn_i^2 + 2rn_i + rn_i(d_i - 1) \text{ para todo } i > N,$$

al multiplicar por $1/n_i^2$ a ambos lados, obtenemos

$$\frac{w_i^2 - 2rn_iw_i + rn_id_i}{n_i^2} > x^2 - \frac{2x}{n_i} + \frac{1}{n_i^2} - 2rx + \frac{2r}{n_i} + r\frac{d_i}{n_i} - \frac{r}{n_i} \text{ para todo } i > N,$$

luego

$$\begin{aligned} \lim_{i \rightarrow \infty} \frac{w_i^2 - 2rn_iw_i + rn_id_i}{n_i^2} &\geq \lim_{i \rightarrow \infty} \left(x^2 - \frac{2x}{n_i} + \frac{1}{n_i^2} - 2rx + r\frac{d_i}{n_i} - \frac{r}{n_i} \right) \\ &= x^2 - 2rx + r\delta, \end{aligned}$$

y esta cantidad es positiva por hipótesis. Por lo tanto, existe un entero positivo I tal que $w_i^2 - 2rn_iw_i + rn_id_i > 0$ para todo $i > I$. En efecto, sea $A = \lim_{i \rightarrow \infty} (w_i^2 - 2rn_iw_i + rn_id_i)/n_i^2$ entonces

i. Si $A = \infty$ entonces dado $M > 0$ existe un entero positivo I tal que

$$\frac{w_i^2 - 2rn_iw_i + rn_id_i}{n_i^2} > M \text{ para todo } i > I,$$

así $w_i^2 - 2rn_iw_i + rn_id_i > 0$ para todo $i > I$.

ii. Si $A = L < \infty$, entonces existe un entero positivo I tal que

$$\left| \frac{w_i^2 - 2rn_iw_i + rn_id_i}{n_i^2} - L \right| < L \text{ para todo } i > I,$$

esto implica que $w_i^2 - 2rn_iw_i + rn_id_i > 0$ para todo $i > I$.

□

Teorema 4.17. (Cota asintótica de Elias) Sea $0 < \delta < r$ con $r = 1 - q^{-1}$. Entonces

$$\alpha_q(\delta) \leq 1 - H_q\left(r - \sqrt{r(r - \delta)}\right).$$

Demostración. Sea R tal que $(\delta, R) \in Uq$. Por la *Proposición 4.4*, existe una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si $\mathcal{C}_i$ es un $[n_i, k_i, d_i]$ código sobre $\mathbb{F}_q$ entonces

$$\frac{d_i}{n_i} \rightarrow \delta, \quad \frac{k_i}{n_i} \rightarrow R \quad \text{cuando } i \rightarrow \infty.$$

Como $r\delta > 0$ tenemos que $r - \sqrt{r(r - \delta)} > 0$. Sea $0 < x < r - \sqrt{r(r - \delta)}$ entonces $0 < \sqrt{r(r - \delta)} < r - x$. Elevando a ambos lados al cuadrado obtenemos $r(r - \delta) < x^2 - 2rx + r^2$, de aquí que $x^2 - 2rx + r\delta > 0$. Sea $w_i = \lfloor xn_i \rfloor$ para todo i , por el *Lema 4.16* existe un entero positivo I tal que

$$w_i^2 - 2rn_iw_i + rn_id_i > 0 \text{ para todo } i > I.$$

Como $x < r$ tenemos que $xn_i < rn_i$, así $w_i < rn_i$ para todo i y por la cota de Elias

$$q^{k_i} \leq A_q(n_i, d_i) \leq \left(\frac{rn_id_i}{w_i^2 - 2rn_iw_i + rn_id_i} \right) \left(\frac{q^{n_i}}{V_q(n_i, w_i)} \right) \text{ para todo } i > I,$$

tomando logaritmo en base q y multiplicando a ambos lados por $1/n_i$ obtenemos

$$\frac{k_i}{n_i} \leq \frac{\log_q \left(\frac{rn_id_i}{w_i^2 - 2rn_iw_i + rn_id_i} \right)}{n_i} + 1 - \frac{\log_q V_q(n_i, w_i)}{n_i} \text{ para todo } i > I,$$

por consiguiente

$$R \leq \lim_{i \rightarrow \infty} \left(\frac{\log_q \left(\frac{rn_id_i}{w_i^2 - 2rn_iw_i + rn_id_i} \right)}{n_i} + 1 - \frac{\log_q V_q(n_i, w_i)}{n_i} \right).$$

Observe que

$$\frac{xn_i - 1}{n_i} < \frac{w_i}{n_i} \leq \frac{xn_i}{n_i} \text{ para todo } i.$$

Luego, por la *Proposición 4.1* y el Teorema del encaje

$$\lim_{i \rightarrow \infty} \frac{w_i}{n_i} = x, \tag{4.13}$$

lo cual implica que

$$\lim_{i \rightarrow \infty} \frac{rn_id_i}{w_i^2 - 2rn_iw_i + rn_id_i} = \lim_{i \rightarrow \infty} \frac{\frac{rd_i}{n_i}}{\left(\frac{w_i}{n_i}\right)^2 - \frac{2rw_i}{n_i} + \frac{rd_i}{n_i}} = \frac{r\delta}{x^2 - 2rx + r\delta}.$$

Por la continuidad de la función logaritmo en base q , obtenemos

$$\lim_{i \rightarrow \infty} \log_q \left(\frac{rn_i d_i}{w_i^2 - 2rn_i w_i + rn_i d_i} \right) = \log_q \frac{r\delta}{x^2 - 2rx + r\delta}.$$

Por (4.13) y la *Proposición 4.13*

$$\lim_{i \rightarrow \infty} \frac{\log_q V_q(n_i, w_i)}{n_i} = H_q(x).$$

Así las cosas

$$R \leq 1 - H_q(x).$$

Sea $c = r - \sqrt{r(r - \delta)}$. Claramente, la función de Entropía de Hilbert es continua, luego

$$H_q(c) = \lim_{x \rightarrow c^-} H_q(x).$$

Por lo tanto,

$$R = \lim_{x \rightarrow c^-} R \leq \lim_{x \rightarrow c^-} (1 - H_q(x)) = 1 - H_q(c).$$

□

4.7 COTA ASINTÓTICA DE GILBERT-VARSHAMOV

En el caso asintótico, las cotas de Gilbert y Varshamov coinciden, esta cota es la única cota inferior para la función de Manin que veremos.

Teorema 4.18. (Cota asintótica de Gilbert-Varshamov) Sea $0 < \delta < 1 - q^{-1}$. Entonces

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Demostración. Sea R tal que $(\delta, R) \in U_q$. Por la *Proposición 4.4*, existe una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]$ código sobre $\mathbb{F}_q$ entonces

$$\frac{d_i}{n_i} \rightarrow \delta, \quad \frac{k_i}{n_i} \rightarrow R \quad \text{cuando } i \rightarrow \infty.$$

Si $0 < \varepsilon < 1$ entonces por el *Lema 4.3*, existe un entero positivo J tal que $d_i > \varepsilon$ siempre que $i > J$, por ende, $d_i \geq 1$ para todo $i > J$. Por la cota de Gilbert

$$B_q(n_i, d_i) \geq \frac{q^{n_i}}{V_q(n_i, d_i - 1)} \quad \text{para todo } i > J.$$

Observe que

$$V_q(n_i, d_i - 1) = \sum_{j=0}^{d_i-1} \binom{n_i}{j} (q-1)^j \leq \sum_{j=0}^{d_i} \binom{n_i}{j} (q-1)^j = V_q(n_i, d_i) \quad \text{para todo } i > J,$$

luego

$$B_q(n_i, d_i) \geq \frac{q^{n_i}}{V_q(n_i, d_i)} \quad \text{para todo } i > J,$$

tomando logaritmo en base q y multiplicando a ambos lados por $1/n_i$ obtenemos

$$\frac{\log_q B_q(n_i, d_i)}{n_i} \geq 1 - \frac{\log_q V_q(n_i, d_i)}{n_i} \quad \text{para todo } i > J. \quad (4.14)$$

Así que al tomar límites y aplicar la *Proposición 4.13* se obtiene

$$R' := \lim_{i \rightarrow \infty} \frac{\log_q B_q(n_i, d_i)}{n_i} \geq 1 - H_q(\delta). \quad (4.15)$$

Sea $\{\mathcal{C}'_i\}_i \subseteq C_q$ tal que $\mathcal{C}'_i$ es un $[n_i, \log_q B_q(n_i, d_i), d_i]_q$ código. Claramente, $\delta(\mathcal{C}'_i) \rightarrow \delta$ cuando $i \rightarrow \infty$. Como $R(\mathcal{C}'_i) \leq 1$ para todo i tenemos que $R' \leq 1$, así, por la *Proposición 4.4*, $(\delta, R') \in U_q$, esto implica que $\alpha_q(\delta) \geq R'$. De este resultado y la desigualdad (4.15) concluimos que $\alpha_q(\delta) \geq 1 - H_q(\delta)$. $\square$

Corolario 4.19. Sea $0 < \delta < 1 - q^{-1}$. Entonces $\alpha_q(\delta) > 0$.

Demostración. Por la cota asintótica de Gilbert-Varshamov tenemos que

$$\alpha_q(\delta) \geq 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta) \log_q(1-\delta),$$

el lado derecho de esta desigualdad es igual a

$$1 - \log_q \left(\frac{\delta^\delta (1-\delta)^{(1-\delta)}}{(q-1)^\delta} \right).$$

Note que por ser el logaritmo en base q una función creciente basta con probar que $q(q-1)^\delta > \delta^\delta (1-\delta)^{(1-\delta)}$ para concluir la prueba. Como $q-1 \geq 1$ y $\delta > 0$ tenemos que $(q-1)^\delta \geq 1$, al multiplicar a ambos lados de esta desigualdad por q y tener en cuenta que $q > 1$, obtenemos

$$q(q-1)^\delta > 1; \quad (4.16)$$

por otra parte, como $0 < \delta < 1$ y $0 < 1-\delta < 1$ tenemos que $\delta^\delta < 1$ y $(1-\delta)^{(1-\delta)} < 1$, luego $\delta^\delta (1-\delta)^{(1-\delta)} < 1$, de este resultado y la desigualdad (4.16) se sigue que $q(q-1)^\delta > \delta^\delta (1-\delta)^{(1-\delta)}$. $\square$

En la siguiente gráfica damos cuatro cotas superiores y una cota inferior para la función de Manin, para $q = 2$.

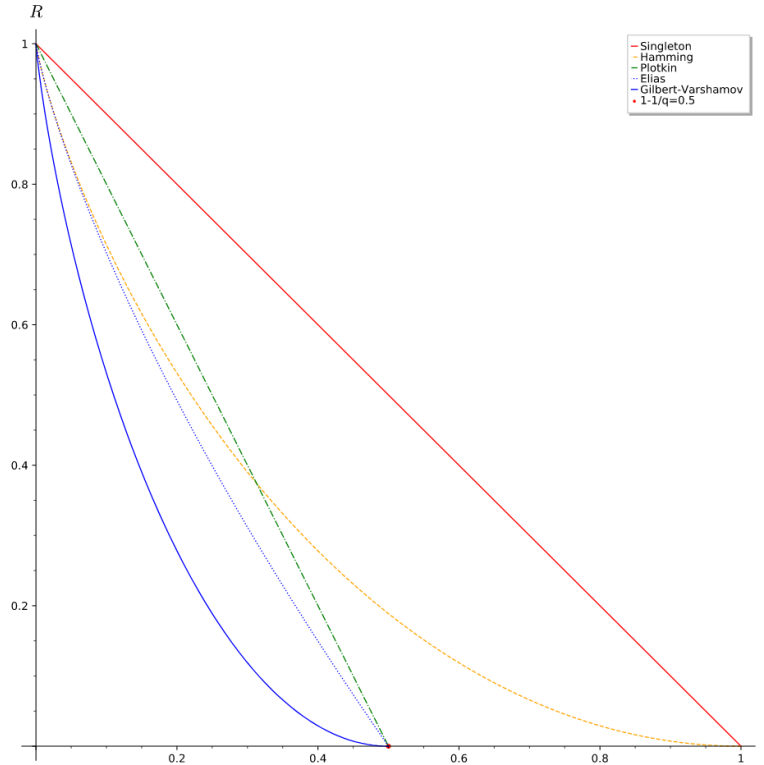


Figura 4.1: Cotas asintóticas con $q = 2$.

4.8 RESULTADOS SOBRE LA FUNCIÓN DE MANIN

En esta última sección presentaremos las propiedades de la función de Manin que establece [6] y que no hemos probado aún. A saber, que la función de Manin es continua en $[0, 1]$ y estrictamente decreciente en $[0, 1 - q^{-1}]$, y que el conjunto de puntos de acumulación de V_q es

$$U_q = \{(\delta, R) : 0 \leq \delta \leq 1 \text{ y } 0 \leq R \leq \alpha_q(\delta)\}.$$

Proposición 4.20. Sea $\delta_0 \in [0, 1]$. Entonces $(\delta_0, \alpha_q(\delta_0)) \in U_q$.

Demostración. Sea $r > 0$ luego, por la definición de supremo, existe R_0 tal que $(\delta_0, R_0) \in U_q$ y $\alpha_q(\delta_0) - r < R_0 \leq \alpha_q(\delta_0)$. Si $R_0 = \alpha_q(\delta_0)$ entonces $(\delta_0, \alpha_q(\delta_0)) \in U_q$; supongamos que $R_0 < \alpha_q(\delta_0)$, sea r' un entero positivo tal que

$$\left\{(\delta, R) : \sqrt{(\delta - \delta_0)^2 + (R - R_0)^2} < r'\right\} \subseteq \left\{(\delta, R) : \sqrt{(\delta - \delta_0)^2 + (R - \alpha_q(\delta_0))^2} < r\right\},$$

como $(\delta_0, R_0) \in U_q$ tenemos, por la definición de punto de acumulación, que existe $(a, b) \in V_q$ tal que $(a, b) \neq (\delta_0, R_0)$ y $\sqrt{(a - \delta_0)^2 + (b - R_0)^2} < r'$, luego $(a, b) \neq (\delta_0, \alpha_q(\delta_0))$ y

$$(a, b) \in \left\{(\delta, R) : \sqrt{(\delta - \delta_0)^2 + (R - \alpha_q(\delta_0))^2} < r\right\},$$

por lo tanto $(\delta_0, \alpha_q(\delta_0)) \in U_q$. □

Teorema 4.21. Sea $(\delta_0, R_0) \in U_q$ con $\delta_0 > 0$ y $R_0 > 0$. Entonces

$$\left\{(\delta, R) : 0 \leq \delta \leq \delta_0, R = \left(\frac{R_0}{\delta_0 - 1}\right)(\delta - 1)\right\} \cup \left\{(\delta, R) : \delta_0 \leq \delta \leq \frac{\delta_0}{1 - R_0}, R = \left(\frac{R_0 - 1}{\delta_0}\right)\delta + 1\right\} \subseteq U_q.$$

Demostración. Dado que $(\delta_0, R_0) \in U_q$ la *Proposición 4.4* garantiza la existencia de una sucesión $\{\mathcal{C}_i\}_i \subseteq C_q$ tal que si cada $\mathcal{C}_i$ es un $[n_i, k_i, d_i]_q$ código entonces

$$\frac{d_i}{n_i} \rightarrow \delta_0, \quad \frac{k_i}{n_i} \rightarrow R_0 \quad \text{cuando } i \rightarrow \infty.$$

Por el *Lema 4.8* tenemos que $0 < \delta_0 < 1$, $0 < R_0 < 1$ y $\delta_0 + R_0 < 1$, luego $\delta_0 < \delta_0/(1 - R_0) < 1$ y $R_0 < R_0/(1 - \delta_0) < 1$.

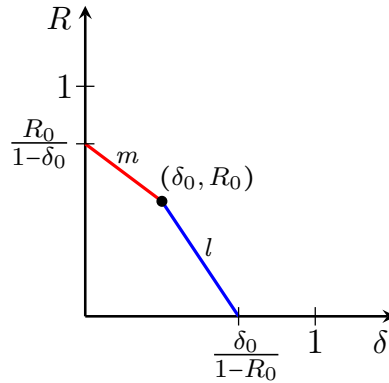


Figura 4.2: Puntos de acumulación de V_q a partir de (δ_0, R_0) .

En primer lugar, veamos que

$$l : \left\{ (\delta, R) : \delta_0 \leq \delta \leq \frac{\delta_0}{1 - R_0}, R = \left(\frac{R_0 - 1}{\delta_0} \right) \delta + 1 \right\} \subseteq U_q.$$

Sea $(\delta_1, R_1) \in l$, así

$$R_1 = \left(\frac{R_0 - 1}{\delta_0} \right) \delta_1 + 1. \quad (4.17)$$

Si $0 < \varepsilon < 1$ entonces, por el *Lema* 4.3, existe un entero positivo I tal que $k_i > \varepsilon$ siempre que $i > I$, por ende si $i > I$ entonces $k_i \geq 1$; para cada $i > I$ sea

$$l_i = \left\lfloor \frac{R_0 - R_1}{(1 - R_1)R_0} k_i \right\rfloor.$$

Observe que

$$0 < \frac{R_0 - R_1}{(1 - R_1)R_0} < 1, \quad (4.18)$$

en efecto, por (4.17) y por ser $\delta_0 < \delta_1$ y $R_0 < 1$ tenemos que

$$R_1 = \left(\frac{R_0 - 1}{\delta_0} \right) \delta_1 + 1 < \left(\frac{R_0 - 1}{\delta_0} \right) \delta_0 + 1 = R_0 < 1.$$

Al multiplicar por k_i en (4.18) obtenemos por la definición de la función parte entera que $0 \leq l_i < k_i$ para todo $i > I$. Note que si $k_i = 1$ entonces $l_i = 0$, por ende si $l_i \neq 0$ entonces $k_i > 1$ y por el *Corolario* 3.27 se sigue que existe un $[n_i - l_i, k_i - l_i, d_i]_q$ código. Así las cosas, sea $\{\mathcal{C}'_i\}_{i>I}$ tal que cada $\mathcal{C}'_i$ es un $[n_i - l_i, k_i - l_i, d_i]_q$ código, resta verificar que $\delta(\mathcal{C}'_i) \rightarrow \delta_1$ y $R(\mathcal{C}'_i) \rightarrow R_1$. Como

$$\frac{R_0 - R_1}{(1 - R_1)R_0} k_i - 1 < l_i \leq \frac{R_0 - R_1}{(1 - R_1)R_0} k_i \quad \text{para todo } i,$$

se sigue por el Teorema del encaje y la *Proposición* 4.1 que

$$\lim_{i \rightarrow \infty} \frac{l_i}{n_i} = \frac{R_0 - R_1}{1 - R_1}.$$

Así,

$$\lim_{i \rightarrow \infty} \frac{k_i - l_i}{n_i - l_i} = \lim_{i \rightarrow \infty} \frac{\frac{k_i}{n_i} - \frac{l_i}{n_i}}{1 - \frac{l_i}{n_i}} = \frac{R_0 - \frac{R_0 - R_1}{1 - R_1}}{1 - \frac{R_0 - R_1}{1 - R_1}} = \frac{R_1(1 - R_0)}{1 - R_0} = R_1,$$

además, por (4.17)

$$\lim_{i \rightarrow \infty} \frac{d_i}{n_i - l_i} = \lim_{i \rightarrow \infty} \frac{\frac{d_i}{n_i}}{1 - \frac{l_i}{n_i}} = \frac{\delta_0}{1 - \frac{R_0 - R_1}{1 - R_1}} = \frac{\delta_0(1 - R_1)}{1 - R_0} = \delta_1.$$

Ahora, veamos que

$$m : \left\{ (\delta, R) : 0 \leq \delta \leq \delta_0, R = \left(\frac{R_0}{\delta_0 - 1} \right) (\delta - 1) \right\} \subseteq U_q.$$

Sea $(\delta_1, R_1) \in m$, luego

$$R_1 = \left(\frac{R_0}{\delta_0 - 1} \right) (\delta_1 - 1). \quad (4.19)$$

Por el *Lema* 4.3 tenemos que existe un entero positivo J tal que $d_i \geq 1$ siempre que $i > J$; para cada $i > J$ sea

$$l_i = \left\lfloor \frac{\delta_0 - \delta_1}{(1 - \delta_1)\delta_0} d_i \right\rfloor,$$

un razonamiento análogo al anterior nos permite garantizar que $0 \leq l_i < d_i$ para todo $i > J$ y que

$$\lim_{i \rightarrow \infty} \frac{l_i}{n_i} = \frac{\delta_0 - \delta_1}{1 - \delta_1} \quad (4.20)$$

Si $d_i = 1$ es fácil ver que $l_i = 0$, por ende si $l_i \neq 0$ entonces $d_i > 1$ y por el *Corolario 2.67* se sigue que existe un $[n_i - l_i, k_i, d_i - l_i]_q$ código. Así las cosas, sea $\{\mathcal{C}'_i\}_{i>J}$ tal que cada $\mathcal{C}'_i$ es un $[n_i - l_i, k_i, d_i - l_i]_q$ código, resta probar que $\delta(\mathcal{C}'_i) \rightarrow \delta_1$ y $R(\mathcal{C}'_i) \rightarrow R_1$, por (4.20)

$$\lim_{i \rightarrow \infty} \frac{d_i - l_i}{n_i - l_i} = \lim_{i \rightarrow \infty} \frac{\frac{d_i}{n_i} - \frac{l_i}{n_i}}{1 - \frac{l_i}{n_i}} = \frac{\delta_0 - \frac{\delta_0 - \delta_1}{1 - \delta_1}}{1 - \frac{\delta_0 - \delta_1}{1 - \delta_1}} = \frac{\delta_1(1 - \delta_0)}{1 - \delta_0} = \delta_1,$$

además, por (4.19)

$$\lim_{i \rightarrow \infty} \frac{k_i}{n_i - l_i} = \lim_{i \rightarrow \infty} \frac{\frac{k_i}{n_i}}{1 - \frac{l_i}{n_i}} = \frac{R_0}{1 - \frac{\delta_0 - \delta_1}{1 - \delta_1}} = \frac{R_0(1 - \delta_1)}{1 - \delta_0} = R_1.$$

En resumen, si $(\delta_0, R_0) \in U_q$ con $\delta_0 > 0$ y $R_0 > 0$ entonces los puntos que pertenecen a los segmentos l y m de la *Figura 4.2* son puntos de acumulación de V_q . $\square$

Corolario 4.22. Sea $\delta_0 = 1 - q^{-1}$. Entonces $\alpha_q(\delta_0) = 0$.

Demostración. Si $\alpha_q(\delta_0) > 0$ tendríamos por el *Teorema 4.21* que

$$\left(\delta, \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \right) \in U_q \quad \text{para todo } \delta_0 < \delta < \frac{\delta_0}{1 - \alpha_q(\delta_0)}, \quad (4.21)$$

observe que $\delta(\alpha_q(\delta_0) - 1)/\delta_0 + 1 > 0$ para todo $\delta < \delta_0/(1 - \alpha_q(\delta_0))$, luego (4.21) contradice la cota asintótica de Plotkin para $\delta > \delta_0$, por lo tanto $\alpha_q(\delta_0) = 0$. $\square$

Corolario 4.23. La función de Manin es continua en $\delta = 1 - q^{-1}$.

Demostración. Sea $r = 1 - q^{-1}$. El *Corolario 4.19* y la cota asintótica de Plotkin garantizan que

$$0 < \alpha_q(\delta) \leq 1 - \frac{\delta}{r}, \quad \text{para todo } 0 < \delta < r$$

luego por el *Teorema del encaje*

$$\lim_{\delta \rightarrow r^-} \alpha_q(\delta) = 0; \quad (4.22)$$

por otra parte, por la cota asintótica de Plotkin tenemos que

$$\lim_{\delta \rightarrow r^+} \alpha_q(\delta) = 0. \quad (4.23)$$

Por (4.22), (4.23) y el *Corolario 4.22* concluimos que

$$\lim_{\delta \rightarrow r} \alpha_q(\delta) = \alpha_q(r).$$

$\square$

Teorema 4.24. Sea $0 < \delta_0 < 1 - q^{-1}$. Entonces α_q es continua en δ_0 .

Demostración. Por el Corolario 4.19 y el Lema 4.8 tenemos que $0 < \delta_0 < 1$, $0 < \alpha_q(\delta_0) < 1$ y $\delta_0 + \alpha_q(\delta_0) < 1$, de aquí que $\delta_0 < \delta_0/(1 - \alpha_q(\delta_0)) < 1$ y $\alpha_q(\delta_0) < \alpha_q(\delta_0)/(1 - \delta_0) < 1$. Consideremos las regiones

$$\begin{aligned} A &= A(\delta_0, \alpha_q(\delta_0)) = \left\{ (\delta, R) \in [0, 1]^2 : \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta - 1) \leq R \leq \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \right\}, \\ B &= B(\delta_0, \alpha_q(\delta_0)) = \left\{ (\delta, R) \in [0, 1]^2 : \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \leq R \leq \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta - 1) \right\}, \\ C &= C(\delta_0, \alpha_q(\delta_0)) = \left\{ (\delta, R) \in [0, 1]^2 : R < \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \text{ y } R < \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta - 1) \right\}, \\ D &= D(\delta_0, \alpha_q(\delta_0)) = \left\{ (\delta, R) \in [0, 1]^2 : R > \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \text{ y } R > \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta - 1) \right\}, \end{aligned}$$

y los segmentos

$$\begin{aligned} l &: \left\{ (\delta, R) : \delta_0 \leq \delta \leq \frac{\delta_0}{1 - \alpha_q(\delta_0)}, R = \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta + 1 \right\}, \\ m &: \left\{ (\delta, R) : 0 \leq \delta \leq \delta_0, R = \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta - 1) \right\}, \end{aligned}$$

representados en la Figura 4.3 con azul y rojo, respectivamente.

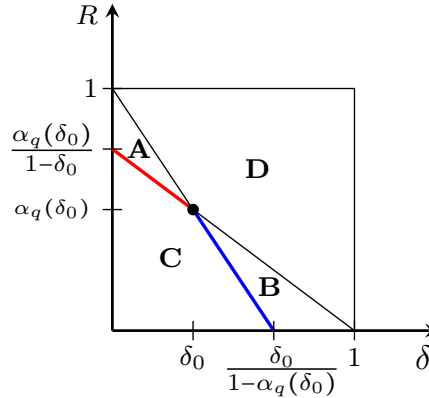


Figura 4.3: Regiones A, B, C y D, y segmentos l y m .

Por la Proposición 4.20 y el Teorema 4.21 tenemos que $l \subseteq U_q$ y $m \subseteq U_q$. Ahora, sea $\delta_1 \in [0, 1]$, si $(\delta_1, \alpha_q(\delta_1)) \in C(\delta_0, \alpha_q(\delta_0))$ tendríamos que existe R_1 tal que $\alpha_q(R_1) < R_1$ con (δ_1, R_1) en l o en m , de aquí que $(\delta_1, R_1) \in U_q$ pero esto contradice la definición de supremo; si $(\delta_1, \alpha_q(\delta_1)) \in D(\delta_0, \alpha_q(\delta_0))$ tendríamos que $\delta_1 > 0$, $\alpha_q(\delta_1) > 0$ y

$$\alpha_q(\delta_1) > \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0} \right) \delta_1 + 1 \quad \text{y} \quad \alpha_q(\delta_1) > \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta_1 - 1),$$

al despejar R_0 obtendríamos que $(\delta_0, \alpha_q(\delta_0)) \in C(\delta_1, \alpha_q(\delta_1))$ pero ya vimos que esto no puede suceder. En resumen,

$$(\delta_1, \alpha_q(\delta_1)) \in B(\delta_0, \alpha_q(\delta_0)), \text{ si } \delta_1 \geq \delta_0, \quad (4.24)$$

y

$$(\delta_1, \alpha_q(\delta_1)) \in A(\delta_0, \alpha_q(\delta_0)), \text{ si } \delta_1 \leq \delta_0.$$

Así las cosas, si f_{δ_0} y g_{δ_0} son las funciones dadas por

$$f_{\delta_0}(\delta) = \begin{cases} \frac{(\alpha_q(\delta_0))(\delta-1)}{\delta_0-1} & \text{si } 0 \leq \delta \leq \delta_0 \\ \frac{\delta(\alpha_q(\delta_0)-1)+\delta_0}{\delta_0} & \text{si } \delta_0 < \delta \leq \delta_0/(1-\alpha_q(\delta_0)) \end{cases}$$

y

$$g_{\delta_0}(\delta) = \begin{cases} \frac{\delta(\alpha_q(\delta_0)-1)+\delta_0}{\delta_0} & \text{si } 0 \leq \delta \leq \delta_0 \\ \frac{(\alpha_q(\delta_0))(\delta-1)}{\delta_0-1} & \text{si } \delta_0 < \delta \leq 1 \end{cases}$$

tenemos que

$$f_{\delta_0}(\delta) \leq \alpha_q(\delta) \leq g_{\delta_0}(\delta) \text{ para todo } \delta \in [0, 1].$$

Luego, por el Teorema del encaje

$$\lim_{\delta \rightarrow \delta_0} \alpha_q(\delta) = \alpha_q(\delta_0).$$

□

Corolario 4.25. La función de Manin es continua en $[0, 1]$.

Demostración. Sea $r = 1 - q^{-1}$. Por las cotas asintóticas de Plotkin y Gilbert-Varshamov tenemos que

$$1 - H_q(\delta) \leq \alpha_q(\delta) \leq 1 - \frac{\delta}{r} \quad \text{si } 0 < \delta < r,$$

por la Regla de L'hospital

$$\lim_{\delta \rightarrow 0^+} H_q(\delta) = \lim_{\delta \rightarrow 0^+} (\delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta)) = 0,$$

luego, por el Teorema 4.5 y el Teorema del encaje obtenemos que

$$\lim_{\delta \rightarrow 0^+} \alpha_q(\delta) = \alpha_q(0).$$

Este resultado junto a la cota asintótica de Plotkin, el Corolario 4.23 y el Teorema 4.24 garantizan que la función de Manin es continua en $[0, 1]$. □

Teorema 4.26. La función de Manin es estrictamente decreciente en $[0, 1 - q^{-1}]$.

Demostración. Sean $\delta_0 \in [0, 1 - q^{-1})$ y $\delta_1 \in [0, 1]$ tales que $\delta_0 < \delta_1$. Si $\delta_0 = 0$ entonces $\alpha_q(\delta_0) = 1$, como $0 < \delta_1$ se sigue, por la cota asintótica de Singleton, que $\alpha_q(\delta_1) < 1$, por lo tanto $\alpha_q(\delta_1) < \alpha_q(\delta_0)$; si $\delta_0 \in (0, 1 - q^{-1})$ entonces por la prueba del Teorema 4.24, específicamente por (4.24), resulta

$$\alpha_q(\delta_1) \leq \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta_1 - 1), \quad (4.25)$$

ahora, como la recta m que pasa por los puntos $(\delta_0, \alpha_q(\delta_0))$ y $(1, 0)$ es decreciente tenemos que

$$\left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta_1 - 1) < \left(\frac{\alpha_q(\delta_0)}{\delta_0 - 1} \right) (\delta_0 - 1) = \alpha_q(\delta_0),$$

por esto y (4.25) concluimos que $\alpha_q(\delta_1) < \alpha_q(\delta_0)$. En resumen, si $\delta_0 \in [0, 1 - q^{-1})$ y $\delta_1 \in [0, 1]$ son tales que $\delta_0 < \delta_1$ entonces $\alpha_q(\delta_1) < \alpha_q(\delta_0)$, en particular tenemos que si $\delta_0, \delta_1 \in [0, 1 - q^{-1}]$ y $\delta_0 < \delta_1$ entonces $\alpha_q(\delta_1) < \alpha_q(\delta_0)$. □

Lema 4.27. $(0, 0) \in U_q$.

Demostración. Por la prueba del *Teorema 4.5* tenemos que $\{(\delta, 0) : 0 < \delta < 1 - q^{-1}\} \subseteq U_q$, luego dado $r > 0$ existe δ_0 tal que $0 < \delta_0 < r$ y $(\delta_0, 0) \in U_q$, sea r' un entero positivo tal que

$$\left\{(\delta, R) : \sqrt{(\delta - \delta_0)^2 + R^2} < r'\right\} \subseteq \left\{(\delta, R) : \sqrt{\delta^2 + R^2} < r\right\},$$

como $(\delta_0, 0) \in U_q$ tenemos, por la definición de punto de acumulación, que existe $(a, b) \in V_q$ tal que $(a, b) \neq (\delta_0, 0)$ y $\sqrt{(a - \delta_0)^2 + b^2} < r'$, luego $(a, b) \neq (0, 0)$ y

$$(a, b) \in \left\{(\delta, R) : \sqrt{\delta^2 + R^2} < r\right\},$$

por lo tanto $(0, 0) \in U_q$. □

Teorema 4.28. $U_q = \{(\delta, R) : 0 \leq \delta \leq 1 \text{ y } 0 \leq R \leq \alpha_q(\delta)\}$.

Demostración. Se puede verificar fácilmente que

$$U_q \subseteq \{(\delta, R) : 0 \leq \delta \leq 1 \text{ y } 0 \leq R \leq \alpha_q(\delta)\}.$$

Por la cota asintótica de Plotkin tenemos que $\{(\delta_0, R_0) : 1 - q^{-1} \leq \delta_0 \leq 1, 0 \leq R_0 \leq \alpha_q(\delta_0)\} \subseteq U_q$. Resta verificar que $\{(0, R_0) : 0 \leq R_0 \leq \alpha_q(0)\} \subseteq U_q$ y $\{(\delta_0, R_0) : 0 < \delta_0 < 1 - q^{-1}, 0 \leq R_0 \leq \alpha_q(\delta_0)\} \subseteq U_q$. En primer lugar, veamos que $\{(\delta_0, R_0) : 0 < \delta_0 < 1 - q^{-1}, 0 \leq R_0 \leq \alpha_q(\delta_0)\} \subseteq U_q$. Si $R_0 = 0$ el resultado se obtiene por la prueba del *Teorema 4.5*; si $R_0 = \alpha_q(\delta_0)$ entonces por la *Proposición 4.20*, $(\delta_0, R_0) \in U_q$; supongamos que $0 < R_0 < \alpha_q(\delta_0)$, así por el *Corolario 4.8*, $\alpha_q(\delta_0) < 1$ y $\delta_0 + \alpha_q(\delta_0) < 1$, consideremos los segmentos

$$l : \left\{(\delta, R) : \delta_0 \leq \delta \leq \frac{\delta_0}{1 - \alpha_q(\delta_0)}, R = \left(\frac{\alpha_q(\delta_0) - 1}{\delta_0}\right)\delta + 1\right\},$$

$$m : \left\{(\delta, R) : \delta_0 \leq \delta \leq 1, R = \left(\frac{R_0}{\delta_0 - 1}\right)(\delta - 1)\right\},$$

representados en la *Figura 4.4* con azul y verde, respectivamente. Observe que l y m se intersectan en el punto

$$A = (A_1, A_2) = \left(\frac{\delta_0(1 - R_0 - \delta_0)}{(\alpha_q(\delta_0) - 1)(\delta_0 - 1) - R_0\delta_0}, \frac{(\alpha_q(\delta_0) - 1)(1 - R_0 - \delta_0)}{(\alpha_q(\delta_0) - 1)(\delta_0 - 1) - R_0\delta_0} + 1\right).$$

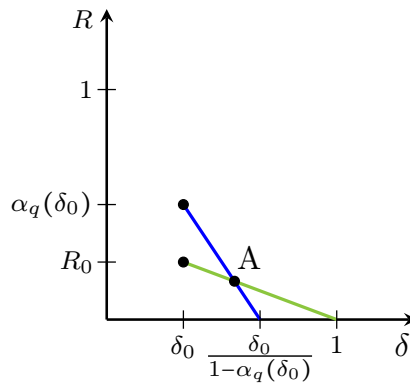


Figura 4.4: Segmentos l y m .

Como $A \in l$ se sigue, por el *Teorema 4.21*, que $A \in U_q$. Note que

$$\delta_0 < A_1 < \frac{\delta_0}{1 - \alpha_q(\delta_0)} \quad \text{y} \quad 0 < A_2 < R_0,$$

así, el *Teorema 4.21* garantiza que

$$s : \left\{ (\delta, R) : 0 \leq \delta \leq A_1, R = \left(\frac{A_2}{A_1 - 1} \right) (\delta - 1) \right\} \subseteq U_q,$$

este segmento se representa en la *Figura 4.5* con rojo. Como $A \in m$ tenemos que

$$A_2 = \frac{R_0}{\delta_0 - 1} (A_1 - 1),$$

al despejar R_0 de esta ecuación obtenemos

$$R_0 = \left(\frac{A_2}{A_1 - 1} \right) (\delta_0 - 1),$$

de aquí que $(\delta_0, R_0) \in s$, por lo tanto $(\delta_0, R_0) \in U_q$.

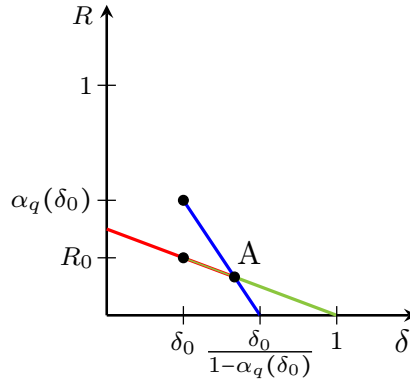


Figura 4.5: Segmentos l , m y s .

Ahora, veamos que $\{(0, R_0) : 0 \leq R_0 \leq \alpha_q(0)\} \subseteq U_q$. Si $R_0 = \alpha_q(0) = 1$ el resultado se tiene por la *Proposición 4.20*; si $R_0 = 0$ entonces por el *Lema 4.27* se sigue que $(0, R_0) \in U_q$; supongamos que $0 < R_0 < 1$, sea $\varepsilon > 0$ tal que $R_0 < 1 - \varepsilon$, como $\alpha_q(\delta) \rightarrow 1$ cuando $\delta \rightarrow 0^+$ tenemos que existe $M > 0$ tal que

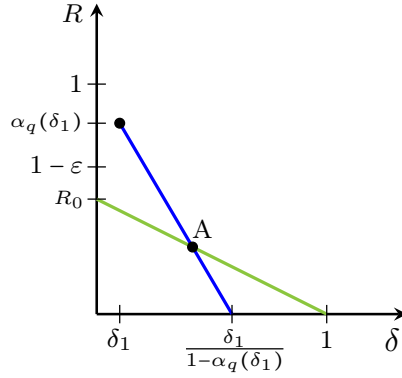
$$1 - \varepsilon < \alpha_q(\delta) \quad \text{siempre que} \quad 0 < \delta < M,$$

sea δ_1 tal que $0 < \delta_1 < M$, luego, el *Corolario 4.8*, garantiza que $\alpha_q(\delta_1) < 1$ y $\delta_1 + \alpha_q(\delta_1) < 1$, así $0 < R_0 < 1 - \varepsilon < \alpha_q(\delta_1) < 1$ y $0 < \delta_1 < \delta_1/(1 - \alpha_q(\delta_1)) < 1$, consideremos los segmentos

$$l : \{(\delta, R) : 0 \leq \delta \leq 1, R = R_0(1 - \delta)\},$$

$$m : \left\{ (\delta, R) : \delta_1 \leq \delta \leq \frac{\delta_1}{1 - \alpha_q(\delta_1)}, R = \left(\frac{\alpha_q(\delta_1) - 1}{\delta_1} \right) \delta + 1 \right\},$$

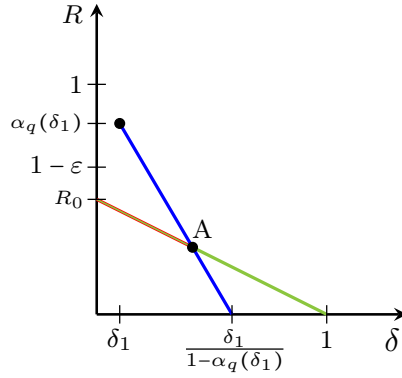
representados en la *Figura 4.6* con verde y azul, respectivamente.

Figura 4.6: Segmentos l y m .

Por el *Teorema 4.21* se sigue que $m \subseteq U_q$; por otra parte, l y m se intersectan ya que $\delta_1/(1 - \alpha_q(\delta_1)) < 1$, sea $A = (A_1, A_2)$ dicho punto de intersección, así $A \in U_q$, note que $0 < A_1 < 1$ y $0 < A_2 < 1$, luego, por el *Teorema 4.21*

$$s : \left\{ (\delta, R) : 0 \leq \delta \leq A_1, R = \left(\frac{A_2}{A_1 - 1} \right) (\delta - 1) \right\} \subseteq U_q,$$

este segmento se representa en la *Figura 4.7* con rojo.

Figura 4.7: Segmentos l , m y s .

Como $A \in l$ tenemos que $A_2 = R_0(1 - A_1)$, al despejar R_0 de esta ecuación obtenemos $R_0 = A_2/(1 - A_1)$, de aquí que $(0, R_0) \in s$, por lo tanto $(0, R_0) \in U_q$. $\square$

BIBLIOGRAFÍA

- [1] R. Hill. *A first course in coding theory*, pages 1–20. Oxford University Press Inc., 1986.
- [2] W. C. Huffman and V. Pless. *Fundamentals of error correcting codes*. Cambridge University Press, 2003.
- [3] G. Jeronimo, J. Sabia, and S. Tesauri. *Álgebra lineal*. Cursos de grado, Departamento de matemática, Universidad de Buenos Aires, 2008.
- [4] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*, pages 11–45. Cambridge University Press, first edition, 1986.
- [5] J. J. López and H. M. Ruiz. *La matemática de la teoría de códigos*. Trabajo de grado, Departamento de matemáticas y estadística, Universidad de Nariño, 2013.
- [6] Y. I. Manin. What is the maximum number of points on a curve over $\mathbb{F}_2$? *Journal of the Faculty of Science, University of Tokyo*, 28(3):715–720, 1981.
- [7] S. Roman. *Coding and information theory*, page 131. Springer-Verlag, 1992.
- [8] M. Tsfasman and S. Vlăduț. *Algebraic-geometric codes*, pages 67–70. Springer Netherlands, 1991.