Universidad de Valladolid

FACULTAD DE CIENCIAS
DEPARTAMENTO DE ÁLGEBRA, ANÁLISIS MATEMÁTICO,
GEOMETRÍA Y TOPOLOGÍA

TESIS DOCTORAL:

PESOS DE HAMMING DE CÓDIGOS CASTILLO

Tesis presentada por WILSON OLAYA LEÓN
para optar al grado de
Doctor por la Universidad de Valladolid

Dirigida por:
Carlos Munuera Gómez

Verano de 2014

A fuerza de observación, de lecturas y de conjeturas...

Con todo el amor que se merecen
Para Claudia, Juan Diego y Mariana.

Agradecimientos

Expreso mis más sinceros agradecimientos a todas las personas y entidades que hicieron posible esta etapa de mi carrera profesional.

A la Universidad Industrial de Santander (Bucaramanga-Colombia) y a la Fundación Carolina (Madrid-España) que financiaron mi estancia en la Universidad de Valladolid.

A Carlos Munuera Gómez por su valiosa labor como director de esta tesis. Por sus enseñanzas y su compromiso con mi formación. Y ante todo por su confianza y amistad.

A Luis Mª Abia Llera, coordinador del programa de doctorado en Matemáticas, por su continua colaboración, desde mi arribo a Valladolid y durante todos estos años.

A las personas de los departamentos de Álgebra, Análisis Matemático, Geometría y Topología (Facultad de Ciencias) y de Matemática Aplicada (Arquitectura), lugares en los que pase la mayor parte del tiempo dedicado a este trabajo.

A los Profesores Fernando Torres (Universidad de Campinas) y Cicero Carvalho (Universidad de Uberlandia) por sus informes académicos de esta tesis.

A mi familia, mi mujer Claudia y mis hijos Juan Diego y Mariana, por ser mi alegría en los momentos difíciles.

Introducción

Perspectiva histórica.

En la segunda mitad del siglo pasado hemos sido testigos de lo que podríamos llamar la gran revolución de la información digital. La principal causa de este suceso es la matematización de la teoría de la comunicación, ver [57]. En un proceso de transmisión de información un emisor envía un mensaje a un receptor a través de un canal. En este proceso el mensaje es convertido en una larga secuencia de símbolos (información digital) pertenecientes a un cuerpo finito $\mathbb{F}_q$ (alfabeto). Según las características del canal y nuestras necesidades, la información se codifica de tal manera que el proceso de comunicación sea lo más rápido, fiable, seguro o secreto posible, dando lugar a diferentes tipos de códigos: compresores, correctores de errores, criptográficos o esteganográficos.

En esta memoria consideramos los *códigos correctores de errores*, cuyo propósito es preservar la calidad de la información transmitida a través de un canal con ruido. La palabra "ruido" hace referencia a cualquier circunstancia que produce errores y por tanto distorsiona el mensaje original. Luego el objetivo de estos códigos es corregir la mayor cantidad posible de errores que puedan ocurrir durante la transmisión de la información.

Los códigos correctores de errores más estudiados y utilizados actualmente son los *códigos lineales*. Estos son subespacios k-dimensionales de $\mathbb{F}_q^n$. Ahora, si consideramos la distancia de Hamming sobre $\mathbb{F}_q^n$, es decir el número de componentes en que difieren dos vectores (palabras), entonces el principio utilizado para corregir errores es el de distancia mínima: recibida una palabra con errores se decodificará por la palabra del código más cercana según la métrica de Hamming. En este sentido, la capacidad correctora de un código esta determinada por su distancia mínima (o peso mínimo de Hamming). Una generalización de este concepto fue introducida independientemente por Tor Helleseth, Torleiv klove y J. Mykkeleveit en [29] y por Victor Wei en [63], motivada por sus

aplicaciones en criptografía. Para $r = 1, \ldots, k$, el *r-ésimo peso de Hamming* de un código lineal C de dimensión k, es el mínimo cardinal del soporte de un subcódigo r-dimensional de C. Así, d_1 es la distancia mínima de C.

Un cálculo completo de los parámetros de un código lineal C debería incluir los valores $n, k, d_1, d_2, \ldots, d_k$. En general calcular la distancia mínima de C es un problema difícil (más exactamente, es un problema NP-completo, ver [5]). Luego calcular todos los pesos de Hamming generalizados es aún más complicado. A menudo tenemos que conformarnos con obtener una estimación de estos valores basándonos en alguna cota inferior disponible. Muchas de estas cotas inferiores para la distancia mínima y, en general, para todos los pesos de Hamming generalizados, son diseñadas para una familia (o construcción) particular de códigos. En esta memoria consideramos las cotas de tipo orden, basadas en obtener estimaciones sobre subconjuntos parciales de palabras del código. De esta manera a menudo se obtienen mejores resultados que cuando se considera el conjunto total de palabras [1, 12, 30, 41].

Sean $\mathcal{X}$ una curva de género g sobre $\mathbb{F}_q$ y $\mathcal{P} = \{P_1, \ldots, P_n\}$ un conjunto de n distintos puntos racionales de $\mathcal{X}$. Sea G un divisor racional de grado no negativo y soporte disjunto al de $D = P_1 + \cdots + P_n$. El código *algebraico geométrico* (AG para acortar) asociado a la terna $(\mathcal{X}, D, G)$ esta definido como la imagen del espacio de Riemman-Roch $\mathcal{L}(G)$, de funciones racionales que tienen ceros y polos especificados por G, por la función evaluación $ev_{\mathcal{P}} : \mathcal{L}(G) \to \mathbb{F}_q^n, \quad ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$. Los códigos AG fueron introducidos por Valery Denisovich Goppa en los setenta, [22, 23] y adquirieron notoriedad debido a que en los ochenta, Michael Tsfasman, Serge Vladuts y Thomas Zink construyeron explícitamente familias de códigos AG cuyos parámetros sobrepasan la cota de Gilbert-Varshamov, una medida clásica que evalúa el comportamiento asintótico de una familia de códigos, ver [61].

En general, los parámetros de los códigos AG no son fáciles de calcular, ya que dependen de la información aritmética y geométrica de la curva sobre la cual se han construido. Si consideramos el divisor G obtenido como un múltiplo de un punto racional Q, entonces los correspondientes códigos AG son llamados *unipuntuales* y permiten un tratamiento teórico y práctico más simple. El espacio $\mathcal{L}(mQ)$, de funciones racionales con polos únicamente en Q de orden a lo sumo m, esta fuertemente relacionado con el semigrupo de Weierstrass de Q, $H(Q) = \{-v_Q(f) : f \in \mathcal{L}(\infty Q)\}$ donde v_Q es la valoración en Q.

Los *códigos Castillo* son códigos AG unipuntuales construidos a partir de una *curva Castillo*, es decir una curva que tiene un punto racional con semigrupo de Weierstrass simétrico y alcanza la cota superior de Lewittes para el número de puntos racionales.

Esta familia contiene algunos de los más importantes códigos AG estudiados hasta la fecha. Las curvas Castillo y los códigos Castillo fueron introducidos por Carlos Munuera, Alonso Sepúlveda y Fernando Torres en [47]. En este artículo también se muestra que estos códigos pueden ser estudiados de manera unificada sin importar la curva de la que proceden.

Organización de la memoria y resultados obtenidos.

La presente memoria esta dedicada a obtener una caracterización explícita sobre las estimaciones de la distancia mínima y los pesos de Hamming generalizados de los códigos Castillo. La exposición consta de cuatro capítulos. En el capítulo 1, *Preliminares*, establecemos el estado del arte de los temas de investigación a los que haremos referencia en los capítulos posteriores. Iniciando con la teoría básica de códigos lineales en donde pondremos énfasis en las propiedades de los pesos de Hamming generalizados y, en especial, en las cotas de tipo orden para la distancia mínima y los pesos de Hamming generalizados. Finalizaremos con la teoría de códigos AG, resaltando la construcción y propiedades fundamentales de la familia especial de códigos Castillo.

En el capítulo 2, consideramos los códigos de dominio ordenado, que generalizan a los códigos AG unipuntuales. Un dominio ordenado es un $\mathbb{F}_q$-álgebra R junto con una función peso v sobre R. Los códigos de dominio ordenado se definen como la imagen del subespacio vectorial $L(m)$, de los elementos en R con peso a lo sumo un entero m, por un morfismo de $\mathbb{F}_q$-álgebras, $\Phi : R \to \mathbb{F}_q^n$. Es decir, el código de dominio ordenado asociado a la pareja (Φ, m) es $C(\Phi, m) = \Phi(L(m))$. El espacio $L(m)$ esta relacionado con el semigrupo asociado a la función peso v. Por esta razón, estudiamos algunas propiedades sobre semigrupos numéricos, en particular sobre los generados por dos elementos y los telescópicos. Introducimos los conceptos de *oasis* y *desiertos* de un semigrupo numérico y cuando el semigrupo es generado por dos elementos consecutivos los caracterizamos explícitamente. Consideramos la cadena de códigos $(0) \subseteq C(\Phi, 0) \subseteq C(\Phi, 1) \subseteq \cdots$ y definimos el conjunto de dimensiones M formado por los enteros no negativos en los cuales la cadena aumenta su dimensión. Con estas herramientas obtenemos una versión de las cotas de orden para los códigos de dominio ordenado, que solo depende de M. Como casos especiales, estudiamos el conjunto de dimensiones y la cota de orden de los códigos AG unipuntuales y en particular de los códigos Castillo. Finalizamos con una técnica de mejora de los códigos de dominio ordenado.

En el capítulo 3, caracterizamos la cota de orden sobre la distancia mínima de los códigos Castillo. Calculamos explícitamente esta cota para los códigos Castillo que

tienen semigrupo de Weierstrass generado por dos elementos consecutivos. Como un caso especial de estos, se obtiene que ésta coincide con el verdadero valor de la distancia mínima de los códigos Hermitianos, dada por Kyeongcheol Yang y P. Vijay Kumar en [62]. Esta nueva caracterización de la distancia mínima de los códigos Hermitianos es más simple que las conocidas hasta el momento, ver [30, 62]. Estos resultados fueron publicados en [51]. En el caso general en que el semigrupo es generado por dos elementos cualesquiera obtenemos igualmente el cálculo completo de la cota de orden de todos estos códigos. También obtenemos resultados similares pero incompletos, para el caso de códigos Castillo con semigrupo telescópico. Finalmente calculamos explícitamente la cota de orden para todos los códigos de Suzuki. Estos resultados fueron publicados en [53].

El capítulo 4, trata sobre los pesos de Hamming generalizados de códigos Castillo. Se pueden distinguir dos partes. En la primera parte (Sección 4.1) caracterizamos la cota de orden solo para el segundo peso de Hamming de códigos Castillo. Calculamos explícitamente esta cota para un gran número de códigos Castillo con semigrupo de Weierstrass generado por dos elementos cualesquiera. Para semigrupos generados por dos elementos consecutivos la cota es calculada completamente. Como consecuencia obtenemos una nueva caracterización del verdadero valor del segundo peso de Hamming de códigos Hermitianos, calculados por Angela Barbero y Carlos Munuera en [2]. Estos resultados fueron publicados en [52]. En la segunda parte de este capítulo (Sección 4.2) introducimos los subconjuntos del conjunto M cuyos elementos se comportan *regular* y *fatal* para cada $i = 1, \ldots, n$. Estos conjuntos, junto con el subconjunto de elementos de M que se comportan *bien*, forman una partición de M. Como resultado principal de esta sección obtenemos un intervalo en el que los códigos Castillo son r-ésimos MDS. En consecuencia, obtenemos una nueva cota inferior d_w sobre la distancia mínima de códigos Castillo. En los ejemplos trabajados, esta cota es tan buena como la cota de orden, si bien no hemos podido encontrar relación entre ellas. Finalmente mostramos que el primer entero $w_i + 1$ para el cuál los códigos Hermitianos son $(w_i + 1)$-ésimo MDS, coincide con el verdadero valor del *toque* de los códigos Hermitianos (este es el primer elemento que satisface la igualdad en la cota singleton generalizada). Por tanto, obtenemos por primera vez el rango MDS de todos los códigos Hermitianos. Estos resultados se recogen en [54].

Índice general

Capítulo 1

Preliminares

En este capítulo presentamos un resumen de los temas de investigación a los que haremos referencia en esta tesis. Comenzando con la teoría básica de códigos lineales (Sección 1.1), pondremos el énfasis en los pesos de Hamming generalizados y, en especial, en las cotas de tipo orden para la distancia mínima. Finalizaremos con la teoría de códigos algebraico geométricos AG (Sección 1.2), resaltando los códigos unipuntuales y la familia especial de códigos Castillo.

1.1. Códigos lineales.

La teoría de códigos correctores de errores tiene su génesis en el año 1948 con la publicación del artículo *A Mathematical Theory of Communication* de Claude Shannon [57]. Inicialmente la teoría es esencialmente probabilística y los resultados obtenidos solamente demuestran la existencia de "buenos" códigos, sin mostrar cómo podrían ser construidos. La necesidad de construir estos códigos explícitamente hizo que años más tarde el álgebra y la teoría de números jugaran un importante papel en esta teoría, con los trabajos de Richard Hamming, Marcel Golay y otros.

El esquema general de un proceso de transmisión de información consiste en que un emisor envía un mensaje a un receptor a través de un canal. En este proceso el mensaje es convertido en una larga secuencia de símbolos (información digital) pertenecientes a un cuerpo finito $\mathbb{F}_q$ (alfabeto). Puesto que en el envío se pueden producir errores de muchos tipos (humanos, físicos, mecánicos, etc) que alteren la información, se conoce como *ruido* a cualquier agente que pueda corromper el mensaje. La finalidad de un código corrector de errores es preservar la calidad de la información que es transmitida a través de un canal con ruido. Su objetivo es corregir la mayor cantidad posible de errores que

puedan ocurrir durante dicha transmisión. La idea básica para conseguirlo es codificar los datos del mensaje agregando una cantidad extra de símbolos (redundancia) que permitan al receptor determinar si han ocurrido errores durante el proceso y corregir cuando sea posible. En consecuencia, el propósito de la teoría de códigos correctores consiste en crear códigos con alguna estructura matemática que permitan corregir el máximo número posible de errores, añadiendo la menor cantidad de redundancia (en otra palabras, diseñar códigos confiables y eficientes). Aunque en la práctica existen restricciones, se conocen como "buenos" códigos aquellos que mantienen un equilibrio entre estos dos aspectos.

La estrategia más frecuente, llamada codificación por bloques, consiste en dividir la información en bloques de k símbolos (símbolos de información) y la codificación los transforma en bloques de n símbolos (palabras), con $n \geq k$. Es decir, la *codificación* es una función $\text{cod} : \mathbb{F}_q^k \to \mathbb{F}_q^n$ y el código es la imagen de los bloques de información. De esta manera, al receptor llega una n-tupla y éste, conociendo la técnica con la que se ha codificado, puede verificar si ocurrieron cambios en la transmisión (detectar errores) y determinar con suficiente confianza cuál fue la n-tupla enviada (corregir errores). Este proceso contrario a la codificación se llama, como era de esperarse, *decodificación* y es una función $\text{dec} : \mathbb{F}_q^n \to C$, usualmente vista como un algoritmo. Esta decodificación se hace suponiendo que el error cometido es pequeño y se conoce como *decodificación de distancia mínima*, ver [34]. Matematizando aún más el proceso se puede exigir que las palabras del código formen un subespacio lineal de $\mathbb{F}_q^n$. Estos códigos (lineales) han jugado un papel importante en las telecomunicaciones y en la informática. Entre las aplicaciones de más importancia tenemos: la transmisión de datos desde el espacio (satélites de comunicaciones, sondas espaciales de la NASA), las cintas magnéticas para computadores, sistemas digitales de audio y video (CD y DVD), redes ADSL, telefonía móvil, entre otras. En la actualidad los códigos detectores-correctores de errores se usan en prácticamente todos los dispositivos de tratamiento de información. A continuación formalizaremos los conceptos que hemos sugerido en la exposición anterior.

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos.

Definición 1 Un *código lineal* C sobre $\mathbb{F}_q$, de *longitud* n y *dimensión* k, es un subespacio k-dimensional de $\mathbb{F}_q^n$.

Los elementos del código C son llamados *palabras*. El número $r = n - k$ es la *redundancia* de C. En lo que sigue la palabra código siempre hará referencia a un código lineal.

Una *matriz generadora* $\mathbf{G}$ de un código C es una $n \times k$ matriz cuyas filas forman una base de C. En consecuencia, una matriz generadora $\mathbf{G}$ es un codificador, ya que $C = \{\mathbf{uG} : \mathbf{u} \in \mathbb{F}_q^k\}$ y un mensaje $\mathbf{u} \in \mathbb{F}_q^k$ se codifica por $\mathbf{c} = \mathbf{uG} \in \mathbb{F}_q^n$.

Junto a n y k, el tercer parámetro fundamental de un código C es la *distancia mínima* d. Esta es la mínima de las distancias de Hamming entre los elementos de C.

Definición 2 La *distancia de Hamming* entre dos vectores $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ y $\mathbf{v} = (v_1, v_2, ..., v_n)$ en $\mathbb{F}_q^n$ es $d(\mathbf{u}, \mathbf{v}) = \#\{i : u_i \neq v_i\}$.

La distancia de Hamming es una métrica sobre $\mathbb{F}_q^n$. El *peso de Hamming* de $\mathbf{u} \in \mathbb{F}_q^n$ es $wt(\mathbf{u}) = d(\mathbf{u}, 0)$. Claramente, para un código C se verifica que

$$d = \text{mín}\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\} = \text{mín}\{wt(\mathbf{u}) : \mathbf{u} \in C, \mathbf{u} \neq 0\}.$$

Usualmente, de un código C de longitud n, dimensión k y distancia mínima d, se dice que es un código $[n, k, d]$.

Una *isometría* de $\mathbb{F}_q^n$ es una función lineal $l : \mathbb{F}_q^n \to \mathbb{F}_q^n$ que conserva la métrica de Hamming, es decir $d(\mathbf{u}, \mathbf{v}) = d(l(\mathbf{u}), l(\mathbf{v}))$. Luego una isometría es un isomorfismo.

Definición 3 Dos códigos C y C' sobre $\mathbb{F}_q$ son *isométricos* si existe una isometría l tal que $l(C) = C'$.

Códigos isométricos tienen los mismos parámetros $[n, k, d]$ y propiedades similares.

Sea $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathbb{F}_q^*)^n$. La función $\mathbf{x} : \mathbf{u} \mapsto \mathbf{x} * \mathbf{u} = (x_1 u_1, ..., x_n u_n)$ es una isometría de $\mathbb{F}_q^n$. Más aún, se verifica que toda isometría l puede escribirse como $l = \mathbf{x} \circ \sigma$, donde $\mathbf{x} \in (\mathbb{F}_q^*)^n$ y $\sigma \in \mathcal{S}_n$ (el grupo simétrico de orden n), ver [45].

Asociado a un código C se define su código dual, denotado por $C^\perp$.

Definición 4 El *código dual* $C^\perp$ de un código $C \subseteq \mathbb{F}_q^n$ se define como

$$C^\perp = \{\mathbf{u} \in \mathbb{F}_q^n : \mathbf{u} \cdot \mathbf{v} = 0 \text{ para todo } \mathbf{v} \in C\}, \tag{1.1}$$

donde $\mathbf{u} \cdot \mathbf{v} = \sum_{t=1}^n u_t v_t$ es el producto interno usual en $\mathbb{F}_q^n$.

Note que $C^\perp$ es un subespacio vectorial de $\mathbb{F}_q^n$, $(C^\perp)^\perp = C$ y $\dim C^\perp = n - \dim C$. Por tanto, si C es un código $[n, k]$ sobre $\mathbb{F}_q$ entonces $C^\perp$ es un código $[n, n-k]$. En general, a partir de los parámetros $[n, k, d]$ de un código C, no puede deducirse una relación entre las distancias mínimas de C y $C^\perp$.

Diremos que un código C es *primario* si no proviene de la Ecuación (1.1).

Una matriz generadora $\mathbf{H}$ de $C^{\perp}$ es también una *matriz de control de paridad* para el código C, pues verifica cuando un vector $\mathbf{u} \in \mathbb{F}_q^n$ esta en el código C, es decir $\mathbf{u} \in C$ si y sólo si $\mathbf{H}\mathbf{u}^T = 0$. Además, la matriz de control puede ser utilizada para calcular la distancia mínima del código C, ya que la distancia mínima de un código con matriz de control de paridad $\mathbf{H}$ coincide con el menor cardinal de un conjunto de columnas linealmente dependientes en $\mathbf{H}$, ver [44].

Recordemos que el objetivo principal de un código C es detectar y corregir los posibles errores producidos durante la transmisión de información a través de un canal con ruido. La idea para esto es hacer que las palabras de C estén tan "separadas" como sea posible, pues el principio utilizado para la corrección de errores es el de mínima distancia. Esto significa que recibida una palabra con errores, se decodificará por la palabra del código más cercana según la métrica de Hamming. Por tanto, el parámetro d es especialmente importante, pues determina la capacidad de corrección del código. Más exactamente, se sabe que un código C puede corregir al menos $r = \lfloor \frac{d-1}{2} \rfloor$ errores, pues las bolas con centro en una palabra y radio r son disjuntas. Por esta razón, $r = \lfloor \frac{d-1}{2} \rfloor$ se llama el *radio de decodificación* del código C.

En la práctica, se requiere la construcción de códigos que puedan corregir la mayor cantidad de errores manteniendo una buena cantidad de información a transmitir, esto último se logra disminuyendo la redundancia. En otras palabras, se necesitan códigos cuyos parámetros k y d sean grandes simultáneamente con respecto a su longitud n. Sin embargo, obtener las dos cosas sólo es posible dentro de ciertos límites, pues existen ciertas restricciones para estos parámetros. La más conocida es la cota singleton.

Proposición 5 (Cota singleton) *Si C es un código $[n, k, d]$, entonces*

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

Demostración. Consideremos la proyección $\pi : C \to \mathbb{F}_q^{n-d+1}$ obtenida al eliminar $d-1$ coordenadas fijas. Como cada palabra de C tiene al menos d coordenadas no nulas, entonces π es inyectiva. Por tanto, $\dim(\pi(C)) = k$ y $k \leq n - d + 1$. ■

Los códigos que cumplen la igualdad $k+d = n+1$ son óptimos en cuanto a capacidad correctora y se conocen como códigos de *máxima distancia separable* (MDS). El número $n + 1 - k - d$ es el *defecto singleton*. Así, códigos con defecto singleton 0 son MDS.

En general calcular la distancia mínima d de un código lineal C es un problema difícil (más exactamente, es un problema NP-completo, ver [5]). A menudo tenemos que conformarnos con obtener una estimación de d basada en alguna cota inferior disponible.

Muchas de estas cotas inferiores para la distancia mínima son diseñadas para una familia (o construcción) particular de códigos. Nosotros presentamos en la Sección 1.1.2 un par de cotas inferiores para la distancia mínima d que son de tipo orden.

La distancia mínima (peso mínimo de Hamming) de un código lineal puede verse como una propiedad de minimalidad de subcódigos de dimensión uno. En la siguiente sección presentamos la generalización de esta noción a dimensión superior. Este concepto fue introducido independientemente por Tor Helleseth, Torleiv klove y J. Mykkeleveit en [29] y por Victor Wei en [63], motivado por sus aplicaciones en criptografía.

1.1.1. Pesos de Hamming generalizados.

Sea C un código $[n, k]$ sobre $\mathbb{F}_q$. Definimos el *soporte* de C como

$$\text{sop}(C) = \{i : x_i \neq 0 \text{ para algún } x \in C\}.$$

Diremos que un código C de longitud n es *no degenerado* si $\text{sop}(C) = n$.

La definición siguiente generaliza la distancia mínima de un código lineal C.

Definición 6 Para $1 \leq r \leq k$, definimos el *r-ésimo peso de Hamming* de C como

$$d_r(C) = \text{mín}\{\#\text{sop}(C') : C' \text{ es un subcódigo lineal de } C \text{ y } \dim(C') = r\}.$$

Note que $d_1(C)$ es la distancia mínima de C. La secuencia $\{d_1, d_2, ..., d_k\}$ se conoce como la *jerarquía de pesos* de C. Sus tres propiedades fundamentales son las siguientes.

Proposición 7 *Si C es un código $[n, k]$, entonces*

(1) [Monotonía] Para todo $r = 1, 2, ..., k-1$, se tiene que $d_r(C) < d_{r+1}(C)$.

(2) [Cota singleton generalizada] Para todo $r = 1, 2, ..., k$, se tiene que

$$d_r(C) \leq n - k + r.$$

(3) [Dualidad] Si $C^\perp$ es el código dual de C, entonces

$$\{d_r(C^\perp) : 1 \leq r \leq n-k\} \cup \{n + 1 - d_r(C) : 1 \leq r \leq k\} = \{1, 2, ..., n\}.$$

Demostración. (1) Sea D un subcódigo de C tal que $\#\text{sop}(D) = d_{r+1}(C)$ y $\dim(D) = r+1$. Para $i \in \text{sop}(D)$ consideremos el espacio $D_i = \{x \in D : x_i = 0\}$. Así $\dim(D_i) = r$

y $d_r(C) \leq \#\text{sop}(D_i) \leq \#\text{sop}(D) - 1 = d_{r+1} - 1$. Luego $d_r(C) < d_{r+1}(C)$. (2) Como $d_k(C) \leq n$ y por (1) se tiene que $d_r(C) \leq n - k + r$. (3) Ver e.g. [63, Thm. 3]. ■

De la propiedad de dualidad se sigue que los conjuntos $\{d_r(C^\perp) : 1 \leq r \leq n-k\}$ y $\{n+1-d_r(C) : 1 \leq r \leq k\}$ son disjuntos y por tanto forman una partición de $I_n = \{1, 2, ..., n\}$. De las otras dos propiedades se deduce la propiedad siguiente.

Proposición 8 (Efecto dominó) *Sea C un código $[n, k]$. Si $d_{r'}(C) = n - k + r'$ para algún r', entonces $d_r(C) = n - k + r$ para todo r con $r' \leq r \leq k$.*

Definición 9 Un código C que satisface la igualdad en la cota singleton generalizada, para algún r, se dice que es un *código r-ésimo MDS*.

Por la propiedad efecto dominó se deduce que si C es r'-ésimo MDS, entonces C es r-ésimo MDS para todo $r' \leq r \leq k$.

Definición 10 El menor entero τ para el cual se da la igualdad en la cota singleton generalizada lo llamaremos el *toque* de C.

Si C es un código $[n, k]$ no degenerado, entonces el toque de C siempre existe y es por lo menos k, ya que $d_k(C) = n$. Si τ es el toque de C, entonces al intervalo discreto $[\tau, n]$ lo llamaremos el *rango MDS* de C.

1.1.2. Cotas de orden.

Una cota de orden se basa en obtener estimaciones sobre subconjuntos parciales de palabras del código. De esta manera algunas veces se obtienen mejores resultados que cuando se considera el conjunto total de palabras. El ingrediente principal es considerar el código dentro de una estructura ordenada fija.

Para nosotros un $\mathbb{F}_q$-*álgebra* será un anillo conmutativo R con unidad que contiene a $\mathbb{F}_q$ como subanillo. Entonces R es un espacio vectorial sobre $\mathbb{F}_q$. El ejemplo más interesante de $\mathbb{F}_q$-álgebras es el anillo de polinomios en m variables $\mathbb{F}_q[X_1, \ldots, X_m]$ y sus cocientes $\mathbb{F}_q[X_1, \ldots, X_m]/I$, donde I es un ideal. Otro importante ejemplo es $\mathbb{F}_q^n$. Puesto que $\mathbb{F}_q$ es naturalmente isomorfo a $\{(\lambda, \ldots, \lambda) | \lambda \in \mathbb{F}_q\}$, se tiene que $\mathbb{F}_q^n$ es también un álgebra con el producto componente a componente $*$,

$$(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n).$$

Note que $(\lambda, \ldots, \lambda) * (u_1, \ldots, u_n) = \lambda(u_1, \ldots, u_n)$ luego las estructuras de anillo y espacio vectorial sobre $\mathbb{F}_q^n$ son totalmente compatibles.

La cota de Andersen-Geil.

Sea $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ una base de $\mathbb{F}_q^n$. Consideremos los códigos $C_0 = (0)$, y para $k = 1, \ldots, n$, $\mathrm{C}_k = \langle \mathbf{b}_1, \ldots, \mathbf{b}_k \rangle$. Note que C_k es un código $[n, k]$. Asociada a la cadena de códigos $C_0 = (0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n$, definimos la *función de estratificación* $\rho_{\mathcal{B}} : \mathbb{F}_q^n \to \{0, \ldots, n\}$, $\rho_{\mathcal{B}}(\mathbf{v}) = \min\{i : \mathbf{v} \in C_i\}$.

Lema 11 *Sean $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{F}_q^n$. Entonces se verifica*

(1) $\rho_{\mathcal{B}}(\mathbf{v}_1 + \cdots + \mathbf{v}_m) \leq \max\{\rho_{\mathcal{B}}(\mathbf{v}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v}_m)\}$. *Si existe j tal que $\rho_{\mathcal{B}}(\mathbf{v}_i) < \rho_{\mathcal{B}}(\mathbf{v}_j)$ para todo $i \neq j$, entonces se tiene la igualdad.*

(2) Si $\mathbf{v} \neq \mathbf{0}$ entonces existen escalares $\lambda_1, \ldots, \lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \in \mathbb{F}_q$ con $\lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \neq 0$ tales que $\mathbf{v} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})}$.

(3) $\dim(\langle \mathbf{v}_1, \ldots, \mathbf{v}_m \rangle) \geq \#\{\rho_{\mathcal{B}}(\mathbf{v}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v}_m)\}$. *Recíprocamente, si $D \subseteq \mathbb{F}_q^n$ es un subespacio lineal de dimensión m, entonces existe una base $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ de D tal que $\#\{\rho_{\mathcal{B}}(\mathbf{u}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{u}_m)\} = m$.*

Demostración. (1) Se sigue de la estructura de espacio lineal. (2) se deduce de (1). (3) Supongamos que $\#\{\rho_{\mathcal{B}}(\mathbf{v}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v}_m)\} = t$ y $\rho_{\mathcal{B}}(\mathbf{v}_1) < \ldots < \rho_{\mathcal{B}}(\mathbf{v}_t)$. Si $\lambda_1 \mathbf{v}_1 + \cdots + \lambda_t \mathbf{v}_t = 0$ entonces $0 = \rho_{\mathcal{B}}(\mathbf{0}) = \rho_{\mathcal{B}}(\lambda_1 \mathbf{v}_1 + \cdots + \lambda_t \mathbf{v}_t) = \max\{\rho_{\mathcal{B}}(\mathbf{v}_i) : \lambda_i \neq 0\}$. Por (1) esto implica que $\lambda_1 = \cdots = \lambda_t = 0$. Para la recíproca, escribamos $D_i = D \cap C_i$. Para todo $i = 1, \ldots, n$, se tiene que $D_i = D_{i-1} \oplus (D \cap \langle \mathbf{b}_i \rangle)$, luego $\dim(D_{i-1}) \leq \dim(D_i) \leq \dim(D_{i-1}) + 1$ y la última desigualdad es una igualdad precisamente m veces. Si $D_i \neq D_{i-1}$, tomemos un vector $\mathbf{u}_i \in D_i \backslash D_{i-1}$. Entonces $\#\{\rho_{\mathcal{B}}(\mathbf{u}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{u}_m)\} = m$ y $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ es una base de D. ■

Consideremos en $\mathbb{N}^2$ el orden parcial $(r, s) \prec (i, j)$ si y sólo si $r \leq i$, $s \leq j$ y $(r, s) \neq (i, j)$. Un par de vectores no nulos $(\mathbf{u}, \mathbf{v})$ se dice que *se comporta bien* (con respecto a la base $\mathcal{B}$) si para cualquier par $(\mathbf{b}_r, \mathbf{b}_s)$ tal que $(r, s) \prec (\rho_{\mathcal{B}}(\mathbf{u}), \rho_{\mathcal{B}}(\mathbf{v}))$ se tiene que $\rho_{\mathcal{B}}(\mathbf{b}_r * \mathbf{b}_s) < \rho_{\mathcal{B}}(\mathbf{u} * \mathbf{v})$. Para $i = 1, \ldots, n$, definamos los conjuntos

$$\Lambda_i = \{\mathbf{b}_j \in \mathcal{B} : (\mathbf{b}_i, \mathbf{b}_j) \text{ se comporta bien}\}.$$

Lema 12 *Sea $\mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{v} \neq \mathbf{0}$. Si $\mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$, entonces $\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_j) = \rho_{\mathcal{B}}(\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})} * \mathbf{b}_j)$.*
Demostración. Por el Lema 11(2), $\mathbf{v} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})}$ con $\lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \neq 0$. Como $\mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$, $\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_j) = \rho_{\mathcal{B}}\left(\sum_{i=1}^{\rho_{\mathcal{B}}(\mathbf{v})} \lambda_i \mathbf{b}_i * \mathbf{b}_j\right) = \rho_{\mathcal{B}}(\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})} * \mathbf{b}_j)$. La última igualdad se tiene por la propiedad de buen comportamiento. ■

Proposición 13 *Sea* $\mathbf{v} \in \mathbb{F}_q^n$. *Si* $\mathbf{v} \neq \mathbf{0}$ *entonces* $wt(\mathbf{v}) \geq \#\Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$.
Demostración. Consideremos el espacio vectorial $V(\mathbf{v}) = \{\mathbf{u} \in \mathbb{F}_q^n : \text{sop}(\mathbf{u}) \subseteq \text{sop}(\mathbf{v})\}$ $= \{\mathbf{u} * \mathbf{v} : \mathbf{u} \in \mathbb{F}_q^n\}$. Entonces $wt(\mathbf{v}) = \dim(V(\mathbf{v})) \geq \dim(\langle \mathbf{v} * \mathbf{b}_1, \ldots, \mathbf{v} * \mathbf{b}_n \rangle) \geq$ $\#\{\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_n)\} \geq \#\{\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_j) : \mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}\} = \#\{\rho_{\mathcal{B}}(\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})} * \mathbf{b}_j) :$ $\mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}\} = \#\Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$. ■

De la Proposición 13 se obtiene la *cota de Andersen-Geil* (o *cota de orden*) para la distancia mínima del código primario C_k con respecto a la base $\mathcal{B}$.

Teorema 14 *Para* $k = 1, \ldots, n$, *la distancia mínima de* C_k *satisface*

$$d(C_k) \geq \text{mín}\{\#\Lambda_r : r = 1, \ldots, k\}.$$

Note que los conjuntos Λ_r dependen de la base $\mathcal{B}$. Así la cota también depende de la base $\mathcal{B}$. Esta cota puede ser aplicada a un código lineal arbitrario C, si consideramos su inclusión en una cadena de códigos $C_1 \subset \cdots \subset C_{k-1} \subset C \subset C_{k+1} \subset \cdots \subset C_n = \mathbb{F}_q^n$. Además los mejores resultados son obtenidos cuando todos los códigos en la cadena se han obtenidos de la misma construcción.

También como consecuencia de la Proposición 13 se deduce una cota similar para la distancia mínima de los códigos $C_I = \langle \{\mathbf{b}_i : i \in I\} \rangle$ donde I es un subconjunto arbitrario de $\{1, \ldots, n\}$ (conservando el orden de la base y la función ρ).

Teorema 15 *Para* $I \subseteq \{1, \ldots, n\}$, $I \neq \varnothing$, *la distancia mínima de* $C_I = \langle \{\mathbf{b}_i : i \in I\} \rangle$ *satisface* $d(C_I) \geq \text{mín}\{\#\Lambda_i : i \in I\}$.

Los resultados anteriores también establecen propiedades sobre la jerarquía de pesos.

Lema 16 *Sea* $D \subseteq \mathbb{F}_q^n$ *un subespacio lineal de dimensión* r *y sea* $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ *una base de* D, *entonces* $\#sop(D) \geq \#\bigcup_{i=1,\ldots,r} \Lambda_{\rho_{\mathcal{B}}(\mathbf{v}_i)}$.
Demostración. Consideremos el espacio $V(D) = \{\mathbf{u} \in \mathbb{F}_q^n : \text{sop}(\mathbf{u}) \subseteq \text{sop}(D)\}$. Como $\#\text{sop}(D) = \dim(V(D))$ y $\text{sop}(D) = \text{sop}(\mathbf{v}_1) \cup \cdots \cup \text{sop}(\mathbf{v}_r)$, entonces se tiene que $V(D) = V(\mathbf{v}_1) + \cdots + V(\mathbf{v}_r)$. Ahora, como en la prueba de la Proposición 13, para cada $i = 1, \ldots, r$ se verifica que $\dim(V(\mathbf{v}_i)) \geq \Lambda_{\rho_{\mathcal{B}}(\mathbf{v}_i)}$. ■

Teorema 17 *Para cada* $r = 1, \ldots, k$, *el* r*-ésimo peso de Hamming de* C_k *satisface*

$$d_r(C_k) \geq \min_{1 \leq j_1 < \cdots < j_r \leq k} \#\Lambda_{j_1,\ldots,j_r},$$

donde $\Lambda_{j_1,\ldots,j_r} = \Lambda_{j_1} \cup \cdots \cup \Lambda_{j_r}$.

Demostración. De acuerdo al Lema 11(3), todo subespacio lineal D de C_k tiene una base $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ tal que $1 \leq \rho_{\mathcal{B}}(\mathbf{v}_1) < \cdots < \rho_{\mathcal{B}}(\mathbf{v}_r) \leq k$. Recíprocamente, dados vectores $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ que satisfacen la anterior condición, se tiene que $D = \langle \mathbf{v}_1, \ldots, \mathbf{v}_r \rangle$ es un subespacio vectorial de C_k de dimensión r. Por tanto, el resultado es consecuencia del Lema 16. ■

La cota dada en el Teorema 14 fue introducida por Henning Andersen y Olav Geil en [1]. En este artículo se tratan los códigos lineales descritos por medio de matrices generadoras. También se trata el caso de códigos de dominio ordenado y códigos de variedad afín, que mencionaremos más adelante.

La cota de Feng-Rao.

Utilizando ideas similares a las expuestas anteriormente podemos dar una cota para la distancia mínima de los códigos duales.

Sea $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ una base de $\mathbb{F}_q^n$ y considere la cadena de códigos duales

$$\mathrm{C}_n^{\perp} = (0) \subset \mathrm{C}_{n-1}^{\perp} \subset \cdots \subset \mathrm{C}_0^{\perp} = \mathbb{F}_q^n.$$

Dado un vector $\mathbf{u} \in \mathbb{F}_q^n$, definimos los *síndromes* de $\mathbf{u}$

$$s_1 = s_1(\mathbf{u}) = \mathbf{b}_1 \cdot \mathbf{u}, \ldots, s_n = s_n(\mathbf{u}) = \mathbf{b}_n \cdot \mathbf{u}$$

o equivalentemente, $\mathbf{B}\mathbf{u}^T = \mathbf{s}^T$, donde $\mathbf{s} = (s_1, \ldots, s_n)$ y $\mathbf{B}$ es la matriz cuyas filas son los vectores $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Luego $\mathbf{u} \in C_r^{\perp} \setminus C_{r+1}^{\perp}$ si y sólo si $s_1 = \cdots = s_r = 0$ y $s_{r+1} \neq 0$.

Consideremos también los *síndromes dos-dimensionales*

$$s_{ij} = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{u}, \ 1 \leq i, j \leq n.$$

Sea $\mathbf{S}$ la matriz $\mathbf{S} = (s_{ij})$, $1 \leq i, j \leq n$. Note que esta matriz puede escribirse también como $\mathbf{S} = \mathbf{B}\mathbf{D}(\mathbf{u})\mathbf{B}^T$, donde $\mathbf{D}(\mathbf{u})$ es la matriz diagonal con $\mathbf{u}$ sobre la diagonal. Como $\mathbf{B}$ tiene rango máximo, se sigue que $\mathrm{rank}(\mathbf{S}) = \mathrm{rank}(\mathbf{D}(\mathbf{u})) = wt(\mathbf{u})$.

Lema 18 *Sea* $\mathbf{u} \in C_r^{\perp}$.

(1) $s_{ij} = 0$ *para todo* (i, j) *tal que* $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) \leq r$.

(2) Si $\mathbf{u} \notin C_{r+1}^{\perp}$ *entonces* $s_{ij} \neq 0$ *para todo* (i, j) *tal que* $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r + 1$.

Demostración. Como $\mathbf{u} \in C_r^{\perp}$ se tiene que $s_1 = \cdots = s_r = 0$. (1) Si $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) \leq r$ entonces, por el Lema 11(2), $\mathbf{b}_i * \mathbf{b}_j = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_r \mathbf{b}_r$ y $s_{ij} = \lambda_1 s_1 + \cdots + \lambda_r s_r = 0$.

(2) Si $\mathbf{u} \notin C_{r+1}^{\perp}$ entonces $s_{r+1} \neq 0$. Cuando $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r+1$, se tiene que $\mathbf{b}_i * \mathbf{b}_j = \lambda_1\mathbf{b}_1 + \cdots + \lambda_r\mathbf{b}_r + \lambda_{r+1}\mathbf{b}_{r+1}$ con $\lambda_{r+1} \neq 0$. Entonces $s_{ij} = \lambda_1 s_1 + \cdots + \lambda_r s_r + \lambda_{r+1}s_{r+1} = \lambda_{r+1}s_{r+1} \neq 0$. ■

Para $r = 0, \ldots, n-1$, definamos los conjuntos

$$N_r = \{(i,j) : (\mathbf{b}_i, \mathbf{b}_j) \text{ se comporta bien y } \rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r+1\}.$$

Sea $N_r = \{(i_1, j_1), \ldots, (i_t, j_t)\}$. La propiedad de buen comportamiento implica que todos los i en este conjunto son distintos. Escribamos $i_1 < i_2 < \ldots < i_t$. Por simetría, $j_t = i_1, \ldots, j_1 = i_t$, luego $j_t < \ldots < j_1$. Sea $\mathbf{S}_r$ la submatriz de $\mathbf{S}$

$$\mathbf{S}_r = \begin{bmatrix} s_{i_1,j_t} & \cdots & s_{i_1,j_1} \\ \vdots & & \vdots \\ s_{i_t,j_t} & \cdots & s_{i_t,j_1} \end{bmatrix}.$$

Lema 19 *Si $\mathbf{u} \in C_r^{\perp} \setminus C_{r+1}^{\perp}$ entonces $\mathbf{S}_r$ tiene rango máximo.*
Demostración. Sea (l,m) una posición en la anti-diagonal de $\mathbf{S}_r$. Así, $l = i_h, m = j_h$ para algún h y por el Lema 18(2), $s_{lm} \neq 0$. Si (l,m) está sobre la anti-diagonal, entonces $l = i_h, m < j_h$, luego $\rho_{\mathcal{B}}(\mathbf{b}_l * \mathbf{b}_m) < \rho_{\mathcal{B}}(\mathbf{b}_{i_h} * \mathbf{b}_{j_h}) = r+1$. Así, por el Lema 18(1), $s_{lm} = 0$. Luego $\det(\mathbf{S}_r) \neq 0$. ■

Corolario 20 *Si $\mathbf{u} \in C_r^{\perp} \setminus C_{r+1}^{\perp}$ se tiene que $wt(\mathbf{u}) \geq \#N_r$.*
Demostración. $wt(\mathbf{u}) = rank(\mathbf{S}) \geq rank(\mathbf{S}_r) = \#N_r$. ■

La *cota de Feng-Rao* (o *cota de orden dual*) para la distancia mínima de $C_k^{\perp}$ con respecto a la base $\mathcal{B}$ se deduce del corolario anterior y establece lo siguiente.

Teorema 21 *Para $k = 0, 1, \ldots, n-1$, la distancia mínima de $C_k^{\perp}$ satisface*

$$d(C_k^{\perp}) \geq \text{mín}\{\#N_r : r = k, \ldots, n-1\}.$$

Como en el caso de códigos primarios, esta cota depende del cambio de la base $\mathcal{B}$. La cota dada en el Teorema 21 fue introducida por Gui-Liang Feng y Thammavarapu R.N. Rao en [12] para el caso de códigos algebraico geométricos unipuntuales duales. Al mismo tiempo, Ryutaroh Matsumoto y Shinji Miura independientemente desarrollaron muchas de estas mismas ideas. En [41] formularon la cota de Feng-Rao para cualquier código lineal definido por su matriz de control de paridad. Una generalización de la cota de Feng-Rao a códigos de dominio ordenado y códigos de evaluación fue presentada por

Tom Høholdt, Jacobus van Lint y Ruud Pellikaan en [30]. El propósito fue simplificar la teoría de códigos algebraico geométricos y formular la cota de orden dual sobre la distancia mínima en este lenguaje.

1.1.3. Códigos de evaluación.

Una forma tradicional de obtener subespacios vectoriales de $\mathbb{F}_q^n$ es a través de una función lineal entre espacios vectoriales sobre $\mathbb{F}_q^n$. Es decir, si R es un $\mathbb{F}_q$-álgebra y $\Phi : R \to \mathbb{F}_q^n$ es un morfismo de $\mathbb{F}_q$-álgebras, entonces para todo subespacio vectorial $L \subseteq R$ se tiene un código lineal $C(L) = \Phi(L)$ y su código dual $C(L)^\perp$.

Si $\{f_1, f_2, \dots\}$ es una base de R, entonces obtenemos una cadena de códigos lineales, $C_i = \langle \Phi(f_1), \dots, \Phi(f_i) \rangle$, $i = 1, 2, \dots$. Cuando Φ es sobreyectiva, entonces existe un i tal que $C_i = \mathbb{F}_q^n$, y las cotas de orden de la sección 1.1.2 pueden ser aplicadas para obtener una estimación de la distancia mínima de estos códigos.

El caso más interesante de la anterior construcción se da cuando R es un conjunto de funciones que pueden ser evaluadas en puntos $P_1, \dots, P_n$ pertenecientes a un objeto geométrico $\mathcal{X}$. Sea $\mathcal{P} = \{P_1, \dots, P_n\}$ y consideremos $\Phi = \mathrm{ev}_\mathcal{P} : R \to \mathbb{F}_q^n$ definido por $ev_\mathcal{P}(f) = (f(P_1), \dots, f(P_n))$. Estos códigos son llamados *códigos de evaluación.*

Ejemplo 22 (Códigos de Reed-Muller) *Consideremos $R = \mathbb{F}_q[X_1, \dots, X_m]$ y sea $\mathcal{P}$ el conjunto de los $n = q^m$ puntos $P_1, \dots, P_n$ en $\mathbb{F}_q^m$. La función evaluación $ev_\mathcal{P} : \mathbb{F}_q[X_1, \dots, X_m] \to \mathbb{F}_q^n$, $ev_\mathcal{P}(f) = (f(P_1), \dots, f(P_n))$, es lineal y verifica que $ev_\mathcal{P}(fg) = ev_\mathcal{P}(f) * ev_\mathcal{P}(g)$, luego es un morfismo de $\mathbb{F}_q$-álgebras. Para ver la sobreyectividad, sea $P = (a_1, \dots, a_m) \in \mathbb{F}_q^m$, y consideremos el polinomio $f_P = \prod_{i=1}^m \prod_{\alpha \in \mathbb{F}_q, \alpha \neq a_i} (X_i - \alpha)$ entonces $f_P(P) \neq 0$ y $f_P(Q) = 0$ para todo $Q \neq P$. Así, $\{ev_\mathcal{P}(f_P) : P \in \mathbb{F}_q^m\}$ genera $\mathbb{F}_q^n$. Consideremos la base $\{f_1, f_2, \dots\}$ de $\mathbb{F}_q[X_1, \dots, X_m]$ que consiste en todos los monomios ordenados de acuerdo a un orden graduado (por ejemplo, el orden lexicográfico graduado: primero compare grados y si fuera necesario use orden lexicográfico para desempatar). En consecuencia, obtenemos una cadena creciente de códigos $C_1 \subset C_2 \subset \dots$, donde $C_i = ev_\mathcal{P}(\langle f_1, \dots, f_i \rangle)$.*

Entre estos códigos, de particular interés resultan los de la forma

$$\mathcal{RM}(r, m) = ev_\mathcal{P}(\mathbb{F}_q[X_1, \dots, X_m]_{(r)}),$$

donde $\mathbb{F}_q[X_1, \dots, X_m]_{(r)}$ representa el espacio lineal de todos los polinomios de grado a lo sumo r. Estos son llamados códigos de Reed-Muller. *La misma construcción puede hacerse considerando polinomios homogéneos y evaluando estos en puntos del espacio proyectivo. En este caso se obtienen los llamados códigos de* Reed-Muller proyectivos.

Los códigos de Reed-Muller son importantes tanto del punto de vista teórico como práctico y se sabe mucho acerca de ellos. Por ejemplo, en 1972 se usó un código de Reed-Muller en la misión espacial Mariner 9 para transmitir fotos en blanco y negro del planeta Marte. El caso $m = 1$ es particularmente simple e interesante, por lo que merece una atención especial.

Ejemplo 23 (Códigos de Reed-Solomon) *Sean $R = \mathbb{F}_q[X]$ y $\{1, X, X^2, \dots\}$ una base de R. Sea $\mathcal{P}$ el conjunto de puntos en la recta afín $\mathbb{F}_q$. Los códigos de evaluación $\mathcal{RS}(r) = ev_{\mathcal{P}}(\langle 1, X, \dots, X^r\rangle)$ son llamados códigos de* Reed-Solomon. *Sus parámetros son fáciles de obtener: ya que un polinomio de grado r tiene a lo sumo r raíces, para $r < n$ el código $ev_{\mathcal{P}}(\langle 1, X, \dots, X^r\rangle)$ tiene longitud $n = q$, dimensión $k = r+1$ y distancia mínima $d = n-r$ (es decir, es un código MDS). Estos códigos son ampliamente utilizados (reproductores de CD y DVD, códigos de barras, etc.).*

En los anteriores dos ejemplos, note que para todo $f \in \mathbb{F}_q[X_1, \dots, X_m]$ se tiene que $ev_{\mathcal{P}}(f^q) = ev_{\mathcal{P}}(f)$, luego podemos obtener los mismos códigos desde el álgebra de cocientes $\mathbb{F}_q[X_1, \dots, X_m]/\langle X_1^q - X_1, \dots, X_m^q - X_m\rangle$. En general, podemos tomar un ideal $I \subset \mathbb{F}_q[X_1, \dots, X_m]$ y considerar $I_q = I + \langle X_1^q - X_1, \dots, X_m^q - X_m\rangle$. Sea $\mathcal{P} = \{P_1, ..., P_n\}$ el conjunto de todos los puntos racionales en la variedad $V = V(I_q)$. Por tanto, la función evaluación $ev_{\mathcal{P}} : R_q = \mathbb{F}_q[X_1, \dots, X_m]/I_q \to \mathbb{F}_q^n$ es un isomorfismo de espacios vectoriales. Para cualquier subespacio $L \subseteq R_q$ obtenemos el llamado código de *variedad afín* $C(I, L) = ev_{\mathcal{P}}(L)$. Se sabe que todo código lineal puede ser obtenido de esta forma, incluyendo los códigos algebraico geométricos que veremos a continuación. Los códigos de variedad afín fueron introducidos por Fitzgerald y Robert Lax en [13].

1.2. Códigos algebraico geométricos.

Los códigos algebraico geométricos (AG) fueron introducidos por Valery Denisovich Goppa en los setenta, [22, 23], como una generalización de otra familia de códigos inventada por él mismo, que se conocen como códigos clásicos de Goppa. El punto clave en las construcción de Goppa radica en que se puede obtener información acerca de los parámetros de un código (longitud, dimensión y distancia mínima) en términos de información aritmética y geométrica de la curva sobre la cual se ha construido (número de puntos racionales, género,...).

Los códigos AG se vuelven famosos debido a que en los ochenta, Michael Tsfasman, Serge Vladuts y Thomas Zink demuestran que existen infinitas familias de estos códigos que sobrepasan la cota de Gilbert-Varshamov, [61]. En consecuencia, se obtiene un

camino para dar solución al problema fundamental de la teoría de códigos que fue considerado por Shannon en términos probabilísticos, como hemos dicho, pero sin dar ninguna idea de como construir tales familias.

El interés suscitado por estos códigos ha fomentado el estudio de las herramientas teóricas que los soportan, principalmente geometría algebraica sobre cuerpos finitos.

Curvas algebraicas.

Recordaremos algunos conceptos básicos que utilizaremos para la construcción de códigos AG. Una exposición amplia de estos temas se puede encontrar en [14, 30, 60].

Una *curva algebraica* $\mathcal{X}$ sobre $\mathbb{F}_q$ es una variedad algebraica irreducible de dimensión uno sobre $\mathbb{F}_q$. El conjunto de puntos racionales sobre $\mathcal{X}$ es denotado por $\mathcal{X}(\mathbb{F}_q)$. Puesto que códigos AG son códigos de evaluación de funciones racionales de $\mathcal{X}$ en (algunos) puntos de $\mathcal{X}(\mathbb{F}_q)$, sólo nos interesan las curvas con $\mathcal{X}(\mathbb{F}_q) \neq \emptyset$. Sea $\mathbb{F}_q(\mathcal{X})$ el cuerpo de funciones racionales de $\mathcal{X}$. Entre todas las curvas que tienen $\mathbb{F}_q(\mathcal{X})$ como un cuerpo de funciones, hay (salvo isomorfismo) una única curva proyectiva no singular. En general, se usa ésta para la construcción de códigos AG. Así, en lo que sigue, la palabra *curva* se refiere a curva algebraica, proyectiva, absolutamente irreducible, no singular (aunque casi siempre utilicemos modelos singulares planos de tales curvas para los cálculos).

Los puntos sobre $\mathcal{X}$ corresponden a anillos de valoración en el cuerpo de funciones. Dada una función $f \neq 0$, el *orden* de f en el punto P de $\mathcal{X}$ es el entero $v_P(f)$, donde v_P es la valoración discreta correspondiente al anillo de valoraciones de P. Si $v_P(f) < 0$ entonces P es un *polo* y si $v_P(f) > 0$ entonces P es un *cero* de f. El divisor de f es $\mathrm{div}(f) = \sum_{P \in \mathcal{X}} v_P(f) P$.

Dado un divisor racional G de $\mathcal{X}$, consideramos el espacio vectorial de funciones que tienen ceros y polos especificados por G,

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : \mathrm{div}(f) + G \geq 0\} \cup \{0\}.$$

La dimensión del espacio $\mathcal{L}(G)$ es denotada por $\ell(G)$. El teorema de Riemann-Roch establece que existe una constante g (el *género* de $\mathcal{X}$) tal que $\ell(G) = \deg(G) + 1 - g + \ell(W - G)$, donde W es un divisor canónico. Como divisores canónicos tienen grado $2g - 2$, se sigue que $\ell(G) = \deg(G) + 1 - g$ cuando $\deg(G) > 2g - 2$.

Dos divisores G y G' son *linealmente equivalentes*, denotado por $G \sim G'$, si existe una función racional ϕ con $\mathrm{div}(\phi) = G - G'$. En este caso $\mathcal{L}(G)$ y $\mathcal{L}(G')$ son isomorfos vía la función $f \mapsto \phi f$.

La gonalidad de la curva $\mathcal{X}$ sobre $\mathbb{F}_q$ es el menor grado γ de un morfismo no constante

de $\mathcal{X}$ a la línea proyectiva. Equivalentemente, γ es el menor grado de un divisor racional G tal que $\ell(G) > 1$. Más aún, generalizando esta noción obtenemos la secuencia de gonalidades de $\mathcal{X}$, $GS(\mathcal{X}) = \{\gamma_i : i = 1, 2, \dots\}$ donde $\gamma_i = \text{mín}\{\deg(G) : \ell(G) \geq i\}$.

En la proposición siguiente se establecen algunas de las propiedades fundamentales de la secuencia de gonalidades.

Proposición 24 *Sea $\mathcal{X}$ una curva de género g, entonces la secuencia de gonalidades $GS(\mathcal{X})$ satisface lo siguiente:*

(1) $\gamma_1 = 0$, γ_2 es la gonalidad usual y la secuencia $(\gamma_i)_{i\geq 1}$ es estrictamente creciente.

(2) si $i \leq g$, entonces $2i - 2 \leq \gamma_i \leq i + g - 1$.

(3) $\gamma_g = 2g - 2$ y si $i > g$, entonces $\gamma_i = i + g - 1$.

(4) [Simetría] sea m un entero positivo con $0 \leq m \leq 2g - 1$. Entonces $m \in GS(\mathcal{X})$ si y sólo si $2g - 1 - m \notin GS(\mathcal{X})$.

Demostración. (1) Se tiene de la definición. La desigualdad de la derecha de (2) y (3) se siguen del teorema de Riemann-Roch, mientras que la desigualdad de la izquierda de (2) se sigue del teorema de Clifford. (4) Por (3) se tiene que $2g-1 \notin GS(\mathcal{X})$ y existen g gonalidades en el intervalo $[0, 2g-1]$. Por tanto, demostraremos que $2g-1-\gamma_i \neq \gamma_j$ para cualesquiera $i, j = 1, \dots, g$. Sea A un divisor racional tal que $\deg(A) = \gamma_i$ y $\ell(A) \geq i$. Sea W un divisor canónico sobre $\mathcal{X}$. Por el teorema de Riemann-Roch, $\ell(W - A) \geq i + g - \gamma_i - 1$. Si $j \leq i + g - \gamma_i - 1$, entonces $\gamma_j \leq \deg(W - A) = 2g - 2 - \gamma_i$ y por tanto, $2g - 1 - \gamma_i \neq \gamma_j$. Si $j \geq i + g - \gamma_i - 1$, argumentaremos por reducción al absurdo. Supongamos que $2g - 1 - \gamma_i = \gamma_j$. Sea B un divisor racional tal que $\deg(B) = \gamma_j$ y $\ell(B) \geq j$. Como antes, se tiene que $\ell(W-B) \geq j+g-\gamma_j-1$ así $\ell(W-B) \geq j+\gamma_i-g \geq i$. Esto es imposible ya que $\deg(W - B) = 2g - 2 - \gamma_j = \gamma_i - 1$. ■

Construcción de códigos AG.

Sean $\mathcal{X}$ una curva de género g sobre $\mathbb{F}_q$ y $\mathcal{P} = \{P_1, \dots, P_n\}$ un conjunto de n distintos puntos racionales de $\mathcal{X}$. Sea G un divisor racional de grado no negativo y soporte disjunto a $D = P_1 + \cdots + P_n$. El código *algebraico geométrico* $C(\mathcal{X}, D, G)$ es el código de evaluación dado por

$$ev_{\mathcal{P}} : \mathcal{L}(G) \to \mathbb{F}_q^n \qquad ev_{\mathcal{P}}(f) = (f(P_1), \dots, f(P_n)).$$

La función $ev_{\mathcal{P}}$ es lineal y tiene núcleo $\mathcal{L}(G - D)$. La dimensión de este núcleo, $a = \ell(G-D)$, es llamada la *abundancia* de $C(\mathcal{X}, D, G)$. En particular, si $\deg(G) < n$ entonces

$a = 0$ y por tanto $C(\mathcal{X}, D, G) \cong \mathcal{L}(G)$. Los parámetros de estos códigos se establecen en el siguiente resultado.

Teorema 25 *El código $C(\mathcal{X}, D, G)$ tiene dimensión $k = \ell(G) - \ell(G - D)$ y distancia mínima $d \geq n - \deg(G) + \gamma_{a+1}$. En particular, cuando $2g - 2 < \deg(G) < n$, entonces $k = \deg(G) + 1 - g$ y $d \geq n - \deg(G)$.*

Demostración. Las afirmaciones sobre la dimensión se siguen de la definición de $C(\mathcal{X}, D, G)$ y el teorema de Riemann-Roch. Para la cota de la distancia mínima, sea $\mathbf{c}$ una palabra de peso $d > 0$. Sea $D' \leq D$ el divisor obtenido como la suma de los puntos en $\mathcal{P}$ correspondientes a las $n - d$ coordenadas nulas de $\mathbf{c}$. Entonces existe una función $f \in \mathcal{L}(G - D') \setminus \mathcal{L}(G - D)$ tal que $\mathbf{c} = ev_{\mathcal{P}}(f)$. Así, $\ell(G - D') \geq \ell(G - D) + 1 = a + 1$ y por la definición de las gonalidades, $\gamma_{a+1} \leq \deg(G - D') = \deg(G) - (n - d)$. ■

La cota más débil $d \geq d_G(C(\mathcal{X}, D, G)) = n - \deg(G)$ se llama la *cota de Goppa* sobre la distancia mínima. Note que la cota de Goppa es similar a la cota sobre la distancia mínima de los códigos de Reed-Solomon vista en el Ejemplo 23. La cota para d dada en el Teorema 25, $d \geq n - \deg(G) + \gamma_{a+1}$, es llamada la *cota de Goppa mejorada* y fue introducida por Carlos Munuera en [42].

Corolario 26 *Sea $C(\mathcal{X}, D, G)$ el código $[n, k, d]$ con abundancia $a \geq 0$. Entonces*

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

Demostración. Por el Teorema 25, $k + d \geq n + \ell(G) - \deg(G) - a + \gamma_{a+1}$. Ahora, por el teorema de Riemann-Roch, $\ell(G) \geq \deg(G) + 1 - g$ y por la Proposición 24(2), $\gamma_{a+1} \geq 2a$. Por tanto, se tiene la desigualdad de la izquierda. La desigualdad de la derecha es la cota singleton, ver Proposición 5. ■

El defecto singleton de $C(\mathcal{X}, D, G)$ es menor que $g - a$, es decir $n + 1 - k - d \leq g - a$.

Proposición 27 *$d(C(\mathcal{X}, D, G)) = d_G(C(\mathcal{X}, D, G)) = n - \deg(G)$ si y sólo si existe un divisor D', $0 \leq D' \leq D$, tal que $G \sim D'$.*

Demostración. Como en la prueba del Teorema 25, $d = n - \deg(G)$ si y sólo si existe un divisor $D', 0 \leq D' \leq D$ tal que $\ell(G - D') > 0$. Como G y D' tienen el mismo grado, esto ocurre si y sólo si $G \sim D'$. ■

Ejemplo 28 *Consideremos $\mathcal{X} = \mathbb{P}^1$ la recta proyectiva sobre $\mathbb{F}_q$. Sea Q el punto en infinito y $\mathcal{P}$ el conjunto de $n = q$ puntos afines. Entonces $C(\mathbb{P}^1, D, mQ)$, $1 \leq m \leq q$, es*

precisamente el código de Reed-Solomon de dimensión $k = m + 1$. Como $g = 0$, este es un código MDS.

Así, los códigos AG pueden también ser vistos como una generalización de los códigos de Reed-Solomon: En lugar de la línea proyectiva $\mathbb{P}^1$, consideramos una curva arbitraria $\mathcal{X}$ sobre $\mathbb{F}_q$. Recuerde que los códigos de Reed-Solomon tienen excelentes parámetros k y d, pero también longitud pequeña (piense en el caso binario, $q = 2$).

De acuerdo a la cota de Hasse-Weil, cf. [60], el número de puntos racionales de una curva $\mathcal{X}$ verifica

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

Así, códigos más largos pueden obtenerse usando curvas de género grande, aunque esto incrementa el defecto singleton. Del Corolario 26, los *parámetros asintóticos* verifican

$$\frac{k}{n} + \frac{d}{n} \geq 1 - \frac{g}{n},$$

donde $\frac{k}{n}$ es la *tasa de transmisión de información* y $\frac{d}{n}$ es la *distancia mínima relativa*. Estos valores representan respectivamente la velocidad y el coste de transmisión, y la capacidad correctora con respecto a la longitud. Ambos parámetros están entre 0 y 1, y son mejores cuanto más cercanos a 1 se encuentren. Por tanto, una forma de obtener buenos códigos AG sobre curvas de género alto es hacer n grande con respecto a g. Esta estrategia requiere curvas con muchos puntos racionales respecto a su género.

Ejemplo 29 (Códigos sobre la cuártica de Klein) *La curva $\mathcal{X}$ definida sobre $\mathbb{F}_8$ por la ecuación proyectiva $X^3Y + Y^3Z + Z^3X = 0$ se llama la curva* cuártica de Klein. *Esta es una curva no singular plana, luego su género es 3 por la formula de Plücker. Un cálculo directo demuestra que $\mathcal{X}$ tiene 24 puntos racionales, que es el máximo número permitido por la cota de Serre que mejora la cota de Hasse-Weil,*

$$|\#\mathcal{X}(\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Consideremos los puntos $Q_0 = (1:0:0), Q_1 = (0:1:0), Q_2 = (0:0:1) \in \mathcal{X}(\mathbb{F}_8)$ y el divisor $G = m(Q_0 + Q_1 + Q_2)$, para $m = 2, \ldots, 6$. Sea $\mathcal{P}$ el conjunto con los 21 puntos racionales restantes (diferentes de Q_1, Q_2, Q_3) y sea D la suma de todos estos puntos. El código AG, $C(\mathcal{X}, D, G)$, fue primero estudiado en [24]. De acuerdo al Teorema 25 éste tiene dimensión $k = 3m - 2$ y distancia mínima $d \geq 21 - 3m$. Note que para otros valores de m los parámetros de los códigos obtenidos son más difíciles de estimar. Para $m = 3, 4$, no se conocen códigos que mejoren estos parámetros, ver [40].

En los siguientes dos resultados se establecen las propiedades de isometría y dualidad de códigos AG. Demostraremos que el dual de un código AG es de nuevo un código AG.

Proposición 30 (Isometría) *Sean $\sigma \in \mathcal{S}_n$ y $D_\sigma = P_{\sigma(1)} + \cdots + P_{\sigma(n)}$. Supongamos que G y G' son dos divisores racionales ambos con soporte disjunto de $\mathcal{P}$. Si $G \sim G'$ entonces los códigos $C(\mathcal{X}, D, G)$ y $C(\mathcal{X}, D_\sigma, G')$ son isométricos.*
Demostración. Como $G \sim G'$, existe una función racional ϕ tal que $G - G' = \mathrm{div}(\phi)$ y por tanto $\mathcal{L}(G) = \{\phi f : f \in \mathcal{L}(G')\}$. Luego, $C(\mathcal{X}, D, G) = ev_{\mathcal{P}}(\phi) * C(\mathcal{X}, D, G') = ev_{\mathcal{P}}(\phi) * \sigma^{-1}(C(\mathcal{X}, D_\sigma, G'))$. ■

Teorema 31 (Dualidad) *Existe una forma diferencial ω con polos simples y residuo 1 en todo punto $P_i \in \mathcal{P}$. Si W es el divisor de ω, entonces*

$$C(\mathcal{X}, D, G)^\perp = C(\mathcal{X}, D, D + W - G).$$

Demostración. La existencia de tal forma ω es garantizada por la independencia de valoraciones, ver [60]. La función $\mathcal{L}(D+W-G) \to \Omega(G-D)$, $\phi \mapsto \phi\omega$ es un isomorfismo bien definido de espacios vectoriales. Además, $\phi(P_i) = \phi(P_i)\mathrm{res}_{P_i}(\omega) = \mathrm{res}_{P_i}(\phi\omega)$, donde $\mathrm{res}_P(\eta)$ denota el residuo en P de la forma diferencial η. Sea $\mathbf{u} \in C(\mathcal{X}, D, G)$, $\mathbf{v} \in C(\mathcal{X}, D, D + W - G)$ y escribamos $\mathbf{u} = ev_{\mathcal{P}}(f), \mathbf{v} = ev_{\mathcal{P}}(\phi)$. Entonces

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} f(P_i)\phi(P_i) = \sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\phi\omega) = \sum_{i=1}^{n} \mathrm{res}_{P_i}(f\phi\omega).$$

Ya que $\mathrm{div}(f) \geq -G$ y $\mathrm{div}(\phi\omega) \geq G - D$, se tiene que $\mathrm{div}(f\phi\omega) \geq -D$, así $f\phi\omega$ no tiene polos fuera de $\mathrm{sop}(D)$. Entonces $\sum_{i=1}^{n} \mathrm{res}_{P_i}(f\phi\omega) = \sum_{P \in \mathcal{X}} \mathrm{res}_P(f\phi\omega) = 0$ donde la parte derecha de la igualdad se sigue del teorema del residuo ([60], Corollary IV.3.3). Por tanto, como $\dim(C(\mathcal{X}, D, G)) + \dim(C(\mathcal{X}, D, D + W - G)) = n$, obtenemos el resultado. ■

Ahora estudiaremos la jerarquía de pesos de un código AG. Usando la secuencia de gonalidades de $\mathcal{X}$ se obtiene una cota inferior para el r-ésimo peso de Hamming.

Proposición 32 *Sea $C = C(\mathcal{X}, D, G)$ un código AG de abundancia $a \geq 0$. Entonces*

$$d_r(C) = \mathrm{mín}\{n - \deg(D') : 0 \leq D' \leq D, \ell(G - D') \geq r + a\}.$$

Demostración. Sea $d_r(C) = m$. Existe un subcódigo $C' \subseteq C$ tal que $\dim(C') = r$ y $\mathrm{sop}(C') = m$. Supongamos que $C' = \langle ev_{\mathcal{P}}(f_1), \ldots, ev_{\mathcal{P}}(f_r)\rangle$. Por tanto, $f_1, \ldots, f_r$ son

funciones independientes que se anulan en $n-m$ puntos distintos, digamos $P_{m+1}, \ldots, P_n$ (reordenando si fuera necesario). Entonces $f_1, \ldots, f_r \in \mathcal{L}(G - \sum_{i=m+1}^{n} P_i) \setminus \mathcal{L}(G - D)$ y $\ell(G - \sum_{i=m+1}^{n} P_i) \geq r + a$. Recíprocamente, supongamos que existen $n - m$ puntos distintos $P_{m+1}, \ldots, P_n$, tales que $\ell(G - \sum_{i=m+1}^{n} P_i) \geq r + a$. Sea $\{\phi_1, \ldots, \phi_a\}$ una base de $\mathcal{L}(G - D)$ y completemos a una base $\{\phi_1, \ldots, \phi_a, f_1, f_2, \ldots\}$ de $\mathcal{L}(G - \sum_{i=m+1}^{n} P_i)$. Sea $C' = \langle ev_{\mathcal{P}}(f_1), \ldots, ev_{\mathcal{P}}(f_r) \rangle$. Así, $\mathrm{sop}(C') \leq m$ y $\dim(C') = r$, luego $d_r(C) \leq m$. ■

Corolario 33 *Sea $C = C(\mathcal{X}, D, G)$ un código AG de dimensión k y abundancia $a \geq 0$. Entonces para todo $r = 1, \ldots, k$ se verifica:*

(1) $d_r(C) \geq n - \deg(G) + \gamma_{r+a}$.

(2) si $r + a > g$, *entonces* $d_r(C) = n - k + r$.

(3) si $r + a = g$, *entonces* $d_r(C) = n - k + r$ *o* $d_r(C) = n - k + r - 1$.

Demostración. (1) Sea $D' \leq D$ un divisor efectivo tal que $d_r(C) = n - \deg(D')$. Entonces $\ell(G - D') \geq r + a$ y por tanto, $\deg(G) + d_r(C) - n \geq \gamma_{r+a}$. (2) Por la Proposición 24, $\gamma_{r+a} = r + a + g - 1$. Así, $n - k + r \leq n - \deg(G) + \gamma_{r+a}$ y la igualdad se sigue de la cota singleton generalizada. (3) Similar a (2). ■

La cota inferior para los pesos de Hamming generalizados del código $C(\mathcal{X}, D, G)$ dada en el Corolario 33(1) se conoce como la *cota gonalidad* y fue introducida por Carlos Munuera en [42]. Note que el item (2) del mismo corolario muestra que el código $C(\mathcal{X}, D, G)$ es $(g - a + 1)$-ésimo MDS.

1.2.1. Códigos unipuntuales y semigrupos de Weierstrass.

Si G es un múltiplo de un punto racional Q de $\mathcal{X}$ y $\mathcal{P}$ es el conjunto de puntos racionales de $\mathcal{X}$ diferentes de Q entonces el código $C(m) = C(\mathcal{X}, D, mQ)$ es llamado *unipuntual*. Estos códigos son los códigos AG mas estudiados porque, en general, son más fáciles de tratar que los otros.

El espacio $\mathcal{L}(mQ)$ es el conjunto de funciones racionales con polos únicamente en Q de orden a lo sumo m. Consideremos el $\mathbb{F}_q$-álgebra

$$\mathcal{L}(\infty Q) = \bigcup_{m=0}^{\infty} \mathcal{L}(mQ).$$

Entonces la función evaluación $ev_{\mathcal{P}} : \mathcal{L}(\infty Q) \to \mathbb{F}_q^n$ es un morfismo de $\mathbb{F}_q$-álgebras. Como la dimensión de $C(n+2g-1)$ es $k = \ell((n+2g-1)Q) - \ell((n+2g-1)Q - D) = n$, se tiene

que $C(n+2g-1) = \mathbb{F}_q^n$ y por tanto $ev_{\mathcal{P}}$ es sobreyectiva. Para describir explícitamente estos códigos $C(m)$, es preciso determinar los espacios de funciones racionales $\mathcal{L}(mQ)$ y $\mathcal{L}(\infty Q)$. El semigrupo de Weierstrass resulta útil para esta tarea.

Definimos $H = H(Q) = \{-v_Q(f) : f \in \mathcal{L}(\infty Q) \setminus \{0\}\}$, donde v_Q es la valoración en Q. Note que $H \subseteq \mathbb{N}_0$. Un entero en H se llama *número polar* (o *polo*) de Q, mientras que un entero en $\mathbb{N}_0 \setminus H$ se llama *número laguna* (o *laguna*) de Q. Denotaremos por $\mathrm{Gaps}(H)$ el conjunto de lagunas de H. Es claro que

$$m \in \mathrm{Gaps}(H) \Leftrightarrow \mathcal{L}(mQ) = \mathcal{L}((m-1)Q). \tag{1.2}$$

El lema siguiente muestra que H es un semigrupo numérico. Este se conoce como el *semigrupo de Weierstrass* de Q.

Lema 34 *El conjunto H satisface:*

(1) $0 \in H$.

(2) si $h, h' \in H$ *entonces* $h + h' \in H$.

(3) $g = \#(\mathbb{N}_0 \setminus H)$.

Demostración. (1) Si $f \in \mathbb{F}_q^*$, entonces $-v_Q(f) = 0$. (2) Sean $f, f' \in \mathcal{L}(\infty Q)$ tal que $h = -v_Q(f)$ y $h' = -v_Q(f')$. Entonces $ff' \in \mathcal{L}(\infty Q)$ y $-v_Q(ff') = h + h'$. (3) Como consecuencia del teorema de Riemann-Roch se tiene que $h \in H$ para todo $h \geq 2g$. Ahora como $\ell(0) = 1$ y $\ell((2g-1)Q) = g$ se tiene que exactamente g enteros satisfacen que $\mathcal{L}(mQ) = \mathcal{L}((m-1)Q)$. Luego, por la Ecuación (1.2) se tiene la afirmación. ■

El menor entero c tal que $a \in H$ para todo $a \geq c$ se llama el *conductor* de H. Claramente $c \leq 2g$. Cuando $c = 2g$ el semigrupo es llamado *simétrico* y satisface que $l \in \mathrm{Gaps}(H)$ si y sólo si $2g-1-l \in H$. Si $H = \{0 = h_1 < h_2 < \dots\}$, el primer elemento no nulo de H, h_2, es llamado la *multiplicidad* de H.

Ejemplo 35 (Curva Hermitiana) *La* curva Hermitiana *es la curva $\mathcal{H}$ definida sobre el cuerpo $\mathbb{F}_{q^2}$ por la ecuación afín*

$$y^q + y = x^{q+1}.$$

$\mathcal{H}$ es una curva plana no singular, luego su género es $g = q(q-1)/2$. Tiene exactamente un punto en infinito $Q = (0:1:0)$, que es el polo común de x y y. La función $\beta \mapsto \beta^q + \beta$ es la función traza de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ y por tanto es $\mathbb{F}_q$-lineal y sobreyectiva. Sea $\alpha \in \mathbb{F}_{q^2}$.

Como $\alpha^{q+1} \in \mathbb{F}_q$, *se tiene que el polinomio* $T^q + T = \alpha^{q+1}$ *tiene* q *diferentes raíces* β *en* $\mathbb{F}_{q^2}$. *Entonces la línea* $x = \alpha$ *intersecta* $\mathcal{H}$ *en* q *diferentes puntos afines, que son racionales sobre* $\mathbb{F}_{q^2}$. *En términos de divisores*

$$\operatorname{div}(x-\alpha) = \sum_{\beta \in \mathbb{F}_{q^2}, \beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - qQ$$

donde $P_{\alpha,\beta} = (\alpha : \beta : 1)$. *Cuando* $\beta^q + \beta \neq 0$, *un razonamiento similar prueba que*

$$\operatorname{div}(y-\beta) = \sum_{\alpha \in \mathbb{F}_{q^2}, \alpha^{q+1}=\beta^q+\beta} P_{\alpha,\beta} - (q+1)Q.$$

En particular, como se tienen q^2 *cambios para* α, *se deduce que* $\mathcal{H}$ *tiene* q^3 *puntos racionales afines, es decir* q^3+1 *puntos racionales en total. Entonces* $\mathcal{H}$ *tiene el máximo número posible de puntos racionales de acuerdo a su género, ya que alcanza la cota superior de Hasse-Weil. Ésta es una* curva maximal.

Calculemos el semigrupo de Weierstrass $H(Q)$. *Conocidos los divisores* $\operatorname{div}(x-\alpha)$ *y* $\operatorname{div}(y-\beta)$, *se tiene que* q *y* $q+1$ *son números polares, luego* $\langle q, q+1\rangle \subseteq H(Q)$. *Por otro lado, el semigrupo* $\langle q, q+1\rangle$ *tiene género* $g = q(q-1)/2 = g(\mathcal{H})$. *Entonces se tiene que* $H(Q) = \langle q, q+1\rangle$. *Por tanto, este semigrupo es simétrico, ver Proposición 61.*

Ejemplo 36 (Códigos Hermitianos) *Esta es la familia de códigos más estudiada entre todos los códigos AG. Considere la curva Hermitiana* $\mathcal{H}$ *sobre* $\mathbb{F}_{q^2}$. *Sean* Q *el punto en infinito y* $\mathcal{P}$ *el conjunto de los* $n = q^3$ *puntos afines sobre* $\mathcal{H}$. *Los* Códigos Hermitianos *son códigos unipuntuales* $C(m) = ev_{\mathcal{P}}(\mathcal{L}(mQ))$ *para* $m = 0, 1, 2, \ldots$. *Supongamos que el semigrupo de Weierstrass de* Q *es* $H(Q) = \{h_1 = 0, h_2 = q, h_3 = q+1, \ldots\}$ *enumerado en forma creciente. Si* $m \in H(Q)$ *entonces* m *puede ser escrito como una combinación lineal* $m = \lambda q + \mu(q+1)$, *donde* λ *y* μ *son enteros no negativos y* $\mu < q$. *Entonces* $-v_Q(x^\lambda y^\mu) = m$. *Por tanto, una base de* $\mathcal{L}(\infty Q)$ *es* $\{x^\lambda y^\mu : 0 \leq \lambda, 0 \leq \mu < q\}$ *y una base de* $\mathcal{L}(mQ)$ *es* $\{x^\lambda y^\mu : 0 \leq \lambda, 0 \leq \mu < q, \lambda q + \mu(q+1) \leq m\}$.

Los códigos Hermitianos fueron primero estudiados por Henning Stichtenoth, [59], y después por muchos autores. Su distancia mínima fue calculada por Kyeongcheol Yang y P. Vijay Kumar en [62] y toda su jerarquía de pesos por Angela Barbero y Carlos Munuera en [2].

El mismo argumento que en el Ejemplo 36 demuestra que para una curva arbitraria $\mathcal{X}$ el anillo $\mathcal{L}(\infty Q)$ es un $\mathbb{F}_q$-álgebra finitamente generada. Consideremos un conjunto de generadores $\{a_1, \ldots, a_r\}$ de $H(Q)$ y funciones $\psi_1, \ldots, \psi_r$ tal que $v(\psi_i) = a_i$ para

$i = 1, \ldots, r$. Entonces todo elemento en $H(Q)$ es combinación lineal de $a_1, \ldots, a_r$ con coeficientes enteros no negativos, luego $\mathcal{L}(\infty Q) = \mathbb{F}_q[\psi_1, \ldots, \psi_r]$.

Sea $H = \{0 = h_1 < h_2 < \ldots\}$ el semigrupo de Weierstrass de Q. Para cada $h_i \in H$ sea $f_i \in \mathcal{L}(\infty Q)$ tal que $h_i = -v_Q(f_i)$, entonces por las propiedades de la valoración v_Q, se tiene que $\{f_1, f_2, \ldots\}$ es una base de $\mathcal{L}(\infty Q)$. En consecuencia, utilizando la cadena de códigos $(\mathbf{0}) \subseteq C(0) \subseteq C(1) \subseteq C(2) \subseteq \cdots \subseteq C(n + 2g - 1) = \mathbb{F}_q^n$ y borrando los códigos repetidos podemos utilizar las cotas de orden de la Sección 1.1.2 para obtener la estimación de la distancia mínima de $C(m)$ y su dual. Esto lo detallaremos en la Sección 2.4.1.

En cuanto a la dualidad de los códigos unipuntuales, note que en general el dual de un código unipuntual no es un código unipuntual. De acuerdo a la Proposición 31 se tiene que $C(m)^\perp = C(\mathcal{X}, D,\ D + W - mQ)$, donde W es el divisor de una forma diferencial ω con polos simples y residuo 1 en todos los puntos $P_i \in \mathcal{P}$. Sin embargo, en el caso en que $W = \operatorname{div}(\omega) = (n + 2g - 2)Q - D$ es claro que el dual del código unipuntual $C(m)$ es de nuevo un código unipuntual, como lo establece la proposición siguiente.

Proposición 37 (Dualidad unipuntual) *Si existe una forma diferencial ω con polos simples y residuo 1 en todos los puntos $P_i \in \mathcal{P}$, tal que* $\operatorname{div}(\omega) = (n + 2g - 2)Q - D$ *entonces* $C(m)^\perp = C(n + 2g - 2 - m)$.

Ejemplo 38 (Códigos duales Hermitianos) *Consideremos la curva Hermitiana $\mathcal{H}$ sobre $\mathbb{F}_{q^2}$. La función $f = \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha)$ tiene divisor* $\operatorname{div}(f) = D - q^3 Q$, *donde D es la suma de los $n = q^3$ puntos racionales afines sobre $\mathcal{H}$. Entonces* $\operatorname{div}(f) = D - nQ$. *Además,* $\operatorname{div}(df/f) = (n + 2g - 2)Q - D$, *ver [59]. Luego* $C(m)^\perp = C(n + 2g - 2 - m)$.

1.2.2. Códigos Castillo.

Como señalamos antes, curvas con muchos puntos racionales con respecto a su género proporcionan códigos AG con buenos parámetros. Esta observación ha conllevado, en los últimos años, a una intensa investigación orientada a determinar buenas cotas sobre el número de puntos racionales de una curva y a encontrar curvas con muchos puntos. Para nuestros propósitos en esta sección es importante una de dichas cotas, debida a Joseph Lewittes [33]. Esta cota tiene la particularidad de ser apropiada para construcción de códigos unipuntuales. Pues vincula el número de puntos racionales sobre la curva al semigrupo de Weierstrass de uno de ellos y como hemos visto en la sección anterior, las propiedades de este semigrupo influyen fuertemente en los parámetros de los códigos unipuntuales obtenidos.

La cota de Lewittes para el número de puntos racionales de una curva.

Sea $\mathcal{X}$ una curva sobre $\mathbb{F}_q$ y supongamos que $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$. Consideremos los códigos unipuntuales $C(m) = C(\mathcal{X}, D, mQ)$ donde $D = P_1 + \cdots + P_n$.

Teorema 39 (Cota de Lewittes-Geil-Matsumoto) *Sea $\mathcal{X}$ una curva sobre $\mathbb{F}_q$, Q un punto racional y H el semigrupo de Weierstrass de Q. Entonces*

$$\#\mathcal{X}(\mathbb{F}_q) \leq \#(H \setminus (qH^* + H)) + 1 \leq qh_2 + 1$$

donde h_2 es la multiplicidad de H.

Demostración. Sea $f \in \mathcal{L}(h_2 Q)$ una función racional tal que $h_2 = -v_Q(f)$. Entonces $f^q \in \mathcal{L}(qh_2 Q)$ y $ev(f^q) = ev(f)$. Como ev es inyectiva para $m = qh_2 < n = \#\mathcal{X}(\mathbb{F}_q) - 1$ y como $f^q \neq f$, se tiene que $qh_2 \geq n$. Para la otra desigualdad, observe que $h \in H$ si y sólo si $\ell(hQ) = \ell((h-1)Q) + 1$. Así, $\dim(C(h)) \leq \dim(C(h-1)) + 1$. Como ev es sobreyectiva, ya que $\dim(C(n + 2g - 1)) = n$. Una cota superior sobre el número de $h \in H$ para los cuales $\dim(C(h)) = \dim(C(h-1)) + 1$ será también una cota para el número n. Veamos que si $h \in qH^* + H$ entonces $\dim(C(h)) = \dim(C(h-1))$. Sea $h = q\alpha + \beta$ con $\alpha, \beta \in H, \alpha \neq 0$. Para $f, g \in \mathcal{L}(\infty Q)$ con $-v_Q(f) = \alpha$ y $-v_Q(g) = \beta$ se tiene que $f^q g \in \mathcal{L}(hQ) \setminus \mathcal{L}((h-1)Q)$ y $fg \in \mathcal{L}((h-1)Q)$. Ahora, como $ev(f^q g) = ev(fg)$, entonces $\dim(C(h)) = \dim(C(h-1))$. Esto concluye la prueba del teorema. ■

La cota $\#\mathcal{X}(\mathbb{F}_q) \leq \#(H \setminus (qH^* + H)) + 1$ fue establecida por Olav Geil y Ryutaroh Matsumoto [19], mejorando el resultado previo $\#\mathcal{X}(\mathbb{F}_q) \leq qh_2 + 1$ obtenido por Joseph Lewittes [33].

Curvas Castillo.

Definición 40 Una curva $\mathcal{X}$ sobre $\mathbb{F}_q$ es llamada *curva Castillo* si existe un punto racional $Q \in \mathcal{X}(\mathbb{F}_q)$ tal que: (i) el semigrupo de Weierstrass de Q, $H(Q)$ es simétrico; y (ii) el número de puntos racionales sobre $\mathcal{X}$ alcanza la cota de Lewittes $\#\mathcal{X}(\mathbb{F}_q) = qh_2 + 1$, donde h_2 es la multiplicidad de $H(Q)$.

Ejemplo 41 *Algunas de las curvas citadas anteriormente son Castillo. (1) Una curva racional es una curva Castillo. (2) La curva Hermitiana $\mathcal{H}$ sobre $\mathbb{F}_{q^2}$ es una curva Castillo. Sea Q el punto en infinito. El semigrupo de Weierstrass $H = \langle q, q+1 \rangle$ es simétrico de multiplicidad $h_2 = q$ y $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^3 + 1$.*

Muchas de las curvas interesantes para propósitos de teoría de códigos son Castillo. Veamos otros ejemplos.

Ejemplo 42 *Sean $\mathcal{X}$ una curva hiperelíptica y Q un punto racional hiperelíptico. $\mathcal{X}$ es una curva Castillo si y sólo si Q es el único punto racional hiperelíptico sobre $\mathcal{X}$ y se alcanza la igualdad en la cota hiperelíptica $\#\{$puntos racionales no hiperelípticos$\}$ $+2\#\{$puntos racionales hiperelípticos$\} \leq 2q+2$.*

Ejemplo 43 (Curva Norma-Traza) *La* curva Norma-Traza *es la curva $\mathcal{X}$ sobre $\mathbb{F}_{q^r}$ definida por la ecuación afín*

$$x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$$

o equivalentemente por $N_{\mathbb{F}_{q^r}|\mathbb{F}_q}(x) = T_{\mathbb{F}_{q^r}|\mathbb{F}_q}(y)$, donde N y T son respectivamente las funciones norma y traza de $\mathbb{F}_{q^r}$ sobre $\mathbb{F}_q$. Esta curva tiene $2^{2r-1}+1$ puntos racionales y el semigrupo de Weierstrass del único polo Q de x es generado por q^{r-1} y $(q^r-1)/(q-1)$, luego es simétrico. Por tanto, esta es una curva Castillo. Los códigos AG sobre esta curva han sido estudiados por Olav Geil, ver [17] para más detalles.

Ejemplo 44 (Curva Hermitiana generalizada) *Para $r \geq 2$, la* curva Hermitiana generalizada *es la curva $\mathcal{X}_r$ sobre $\mathbb{F}_{q^r}$ definida por la ecuación afín*

$$y^{q^{r-1}} + \ldots + y^q + y = x^{1+q} + \ldots + x^{q^{r-2}+q^{r-1}}$$

o equivalentemente por $s_{r,1}(y, y^q, \ldots, y^{q^{r-1}}) = s_{r,2}(x, x^q, \ldots, x^{q^{r-1}})$, donde $s_{r,1}$ y $s_{r,2}$ son respectivamente el primer y el segundo polinomio simétrico en r variables. Note que $\mathcal{X}_2$ es la curva Hermitiana. $\mathcal{X}_r$ tiene $q^{2r-1}+1$ puntos racionales. Sea Q el único polo de x. Entonces $H(Q) = \langle q^{r-1}, q^{r-1}+q^{r-2}, q^r+1\rangle$. Este semigrupo es telescópico por tanto simétrico. En consecuencia, $\mathcal{X}_r$ es una curva Castillo. Estas curvas fueron introducidas por Arnaldo Garcia y Henning Stichtenoth en [16]. Los códigos AG basados en esta curva fueron estudiados por Stanislav Bulygin en [6] (caso binario) y por Carlos Munuera, Alonso Sepúlveda y Fernando Torres en [49] (caso general).

Ejemplo 45 (Curva de Suzuki) *La* curva de Suzuki *$\mathcal{S}$ se caracteriza por ser la única curva sobre $\mathbb{F}_q$, con $q = 2q_0^2$, y $q_0 = 2^r \geq 2$, de género $g = q_0(q-1)$ que tiene q^2+1 puntos $\mathbb{F}_q$-racionales, ver [15]. Un modelo plano singular de $\mathcal{S}$ es dado por la ecuación*

$$y^q - y = x^{q_0}(x^q - x).$$

Luego, sólo hay un punto Q sobre $x = \infty$ que es $\mathbb{F}_q$-racional. Se sabe que el semigrupo de Weierstrass de Q es $H = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$ (ver [27, 38]). Así, H es un semigrupo telescópico (ver [30]) y por tanto simétrico. Es decir, $\mathcal{S}$ es una curva Castillo.

Los códigos AG sobre la curva de Suzuki fueron introducidos por Johan P. Hansen y Henning Stichtenoth en [27]. La distancia mínima de estos códigos es conocida en muchos casos, pero no siempre.

La proposición siguiente establece algunas propiedades de las curvas Castillo.

Proposición 46 *Sea $\mathcal{X}$ una curva Castillo con respecto al punto $Q \in \mathcal{X}(\mathbb{F}_q)$. Sean $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ y $D = P_1 + \cdots + P_n$.*

(1) Sea $f \in \mathcal{L}(\infty Q)$ tal que $-v_Q(f) = h_2$. Entonces, para todo $a \in \mathbb{F}_q$, se tiene que $\operatorname{div}(f-a) = D_a - h_2 Q$ con $0 \leq D_a \leq D$.

(2) $D \sim nQ$.

Demostración. (1) El morfismo $f : \mathcal{X} \to \mathbb{P}^1$ tiene grado h_2 luego $\#f^{-1}(a) \leq h_2$ para todo $a \in \mathbb{F}_q$. Como $\#\mathcal{X}(\mathbb{F}_q) = qh_2$ se tiene que $\#f^{-1}(a) = h_2$. Entonces existen exactamente h_2 puntos $P \in \mathcal{X}(\mathbb{F}_q)$ tal que $f(P) = a$. (2) Consideremos los códigos unipuntuales $C(\mathcal{X}, D, mQ)$ y la función $\phi = f^q - f$. Por tanto, $-v_Q(\phi) = qh_2 = n$ y $\phi(P_i) = 0$ para todo P_i. Entonces $\phi \in \mathcal{L}(nQ - D)$ luego $D \sim nQ$. ■

Corolario 47 *Sea $\mathcal{X}$ una curva Castillo de género g con respecto al punto $Q \in \mathcal{X}(\mathbb{F}_q)$. Sean $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ y $D = P_1 + \cdots + P_n$. Entonces $(n+2g-2)Q - D$ es un divisor canónico.*

Demostración. $(n+2g-2)Q - D \sim (2g-2)Q$. Como H es simétrico, este es un divisor canónico. ■

Observación 48 *Sea ϕ la función definida en la prueba de la Proposición 46. Se sabe (ver [48]) que la forma diferencial $\omega = d\phi/\phi$ tiene polos simples y residuo 1 en todos los puntos P_i. Así ω puede ser la forma diferencial requerida por la Proposición 31.*

Recuerde que por γ_r denotamos la r-ésima gonalidad de $\mathcal{X}$ sobre $\mathbb{F}_q$.

Proposición 49 *Sea $\mathcal{X}$ una curva Castillo con respecto al punto $Q \in \mathcal{X}(\mathbb{F}_q)$. Sea $H = \{h_1 = 0 < h_2 < \ldots\}$ el semigrupo de Weierstrass de Q. Si la multiplicidad de H satisface $h_2 \leq q+1$, entonces*

(1) $\gamma_i \leq h_i$ para todo $i = 1, 2, \ldots$.

(2) $\gamma_2 = h_2$.

(3) $\gamma_i = h_i$ para $i \geq g - \gamma_2 + 2$.

Demostración. (1) Se sigue de la definición de gonalidad. (2) Hay un morfismo no constante de grado γ_2 de $\mathcal{X}$ a la línea proyectiva. Entonces $qh_2+1 = \#\mathcal{X}(\mathbb{F}_q) \leq \gamma_2(q+1)$, así $(qh_2+1)/(q+1) = h_2-(h_2-1)/(q+1) \leq \gamma \leq h_2$. Por nuestra hipótesis $h_2 \leq q+1$, se tiene que $(h_2-1)/(q+1) < 1$ y se da la igualdad. (3) La afirmación sobre las gonalidades de orden superior se sigue del hecho que ambos, el semigrupo H y el conjunto de gonalidades $GS(\mathcal{X}) = (\gamma_i)_{i\geq 1}$ verifican la misma propiedad de simetría: para todo entero t, se tiene que $t \in H$ (resp. $t \in GS(\mathcal{X})$) si y sólo si $2g-1-t \notin H$ (resp. $2g-1-t \notin GS(\mathcal{X})$). ■

Códigos Castillo.

Sea $\mathcal{X}$ una curva Castillo con respecto al punto $Q \in \mathcal{X}(\mathbb{F}_q)$. Supongamos que $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$ y sea $D = P_1 + \cdots + P_n$. Un *código Castillo* es un código unipuntual $C(m) = C(\mathcal{X}, D, mQ)$. Sea $H = H(Q) = \{0 = h_1 < h_2 < \ldots\}$ el semigrupo de Weierstrass de Q.

Definamos la función $\iota = \iota_Q : \mathbb{Z} \to \mathbb{N}_0$ por $\iota(m) = \begin{cases} \text{máx}\{i : h_i \leq m\} & \text{si } m \geq 0 \\ 0 & \text{si } m < 0 \end{cases}$.

Proposición 50 *El código Castillo $C(m)$ tienen dimensión $k = \iota(m) - \iota(m-n)$ y abundancia $a = \iota(m-n)$.*

Demostración. Note que $\iota(m) = \ell(mQ)$. Para $m \geq n$, por la Proposición 46(2), la abundancia de $C(m)$ es $\ell(mQ-D) = \ell(mQ-nQ) = \iota(m-n)$. ■

El siguiente resultado establece algunas propiedades sobre la distancia mínima de los códigos Castillo.

Proposición 51 *Sea $C(m)$ un código Castillo. Entonces*

(1) para $1 \leq m < n$, la distancia mínima de $C(m)$ alcanza la cota de Goppa si y sólo si la distancia mínima de $C(n-m)$ también la alcanza.

(2) para $1 \leq r \leq q-1$, $d(C(rh_2)) = n - rh_2$.

(3) para $n - h_2 \leq m \leq n$, $d(C(m)) = h_2$.

Demostración. (1) Como vimos en la Proposición 27, $d(C(m))$ alcanza la igualdad en la cota de Goppa si y sólo si existe $D', 0 \leq D' \leq D$ tal que $mQ \sim D'$. Sea $D'' = D - D'$. Entonces $mQ \sim D - D'' \sim nQ - D''$, luego $(n-m)Q \sim D''$ y $d(C(n-m))$ también alcanza la igualdad en la cota de Goppa. (2) Se sigue de las Proposiciones 27 y 46(1). (3) $h_2 = d(C(n-h_2)) \geq d(C(m)) \geq d(C(n)) \geq h_2$. La primera igualdad por el item

(2) de esta proposición y la última desigualdad por la cota de Goppa mejorada, pues $\gamma_2 = h_2$. ■

Finalmente establecemos la propiedad de dualidad de los códigos Castillo.

Proposición 52 (Isometría dual) *Sea $C(m)$ un código Castillo. Entonces existe un $\mathbf{x} \in (\mathbb{F}_q^*)^n$ tal que*

$$C(m)^\perp = \mathbf{x} * C(n + 2g - 2 - m).$$

Demostración. Es consecuencia de las Proposiciones 30, 37 y el Corolario 47. ■

Los códigos que verifican la relación de dualidad de la anterior proposición se llaman códigos *dual isométricos*. Por tanto, los códigos Castillo son dual isométricos.

Sea $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ una base de $\mathbb{F}_q^n$. Sea $C_k = \langle \mathbf{b}_1, \ldots, \mathbf{b}_k \rangle$, $k = 1, \ldots, n$. Un vector $\mathbf{x} \in (\mathbb{F}_q^*)^n$ que provee la isometría dual puede ser explícitamente obtenido desde las relaciones de dualidad $(\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{x} = 0$, $i + j \leq n$.

Las curvas Castillo y los códigos Castillo fueron introducidos por Carlos Munuera, Alonso Sepúlveda y Fernando Torres en [47] y generalizados por ellos mismos en [48].

Capítulo 2

Códigos de dominio ordenado y cotas de orden

En este capítulo consideraremos los códigos de evaluación obtenidos de un morfismo lineal de un $\mathbb{F}_q$-álgebra R sobre $\mathbb{F}_q^n$. Recordemos que para utilizar las cotas de orden, vistas en la Sección 1.1.2, es necesario construir una cadena de códigos lineales obtenidos a partir de una base ordenada fija. Por tanto, necesitamos introducir una estructura de orden en R, este orden será establecido por las funciones peso sobre R, lo cual convierte a R en un dominio ordenado (Sección 2.1). En la Sección 2.2 estudiamos semigrupos numéricos, ya que el semigrupo asociado a la función peso nos permitirá establecer la cadena de códigos requerida. En la Sección 2.3, definimos los códigos provenientes de un dominio ordenado y el conjunto de dimensiones para establecer las cotas de orden para estos códigos (Sección 2.4). Estas cotas no dependen de la base sino del conjunto de dimensiones. Como casos especiales, estudiaremos las cotas de orden de los códigos unipuntuales (Subsección 2.4.1) y, en particular, de la familia de códigos Castillo (Subsección 2.4.2); finalizaremos con una técnica de mejora de los códigos de dominio ordenado (Subsección 2.4.3).

2.1. Funciones peso y dominios ordenados.

Las funciones peso y los dominios ordenados fueron introducidos en [30]. El propósito allí fue simplificar la teoría de códigos algebraico geométricos y formular la cota de orden dual sobre la distancia mínima en este lenguaje.

Sea $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Diremos que una función $v : R \to \mathbb{N}_0 \cup \{-\infty\}$ es una *función peso* sobre R si v verifica las propiedades siguientes. Para todos $f, g \in R$,

(W.1) $v(f) = -\infty$ si y sólo si $f = 0$;

(W.2) $v(1) = 0$;

(W.3) $v(f + g) \leq \text{máx}\{v(f), v(g)\}$;

(W.4) $v(fg) = v(f) + v(g)$;

(W.5) si $v(f) = v(g)$ entonces existe un elemento $\lambda \in \mathbb{F}_q^*$ tal que $v(f - \lambda g) < v(f)$.

Ejemplo 53 *Consideremos el álgebra $R = \mathbb{F}_q[X]$ de polinomios en una variable. Para $f \in R$ definimos $v(f) = grado(f)$. Entonces v es una función peso sobre R.*

Las propiedades siguientes son consecuencia de las propiedades (W.1) a (W.5).

Proposición 54 *Sea v una función peso sobre R. Entonces*

(a) $v(f) = 0$ si y sólo si $f \in \mathbb{F}_q^*$.

(b) si $v(f) > v(g)$ entonces $v(f + g) = v(f)$.

(c) R es un dominio de integridad.

Demostración. (a) Para todo $\lambda \in \mathbb{F}_q^*$ se tiene que $v(\lambda\lambda^{-1}) = v(\lambda) + v(\lambda^{-1}) = v(1) = 0$ es decir $v(\lambda) = 0$. Recíprocamente, si $v(f) = 0$ entonces, por (W.2) y (W.5), existe $\lambda \in \mathbb{F}_q^*$ tal que $v(f - \lambda) = -\infty$ y $f = \lambda \in \mathbb{F}_q$. (b) $v(f) > v(g)$ entonces $v(f) = v(-g + (f + g)) \leq \text{máx}\{v(g), v(f + g)\} = v(f + g) \leq v(f)$, luego $v(f + g) = v(f)$. (c) Si $fg = 0$ con $g \neq 0$ entonces $v(1) \leq v(g)$. Así $v(f) \leq v(fg) = -\infty$ lo cual implica que $v(f) = -\infty$ y por tanto $f = 0$. ■

Note que los elementos de R se pueden ordenar según el valor de la función peso. Así, el orden de $f \in R$ es $v(f)$. De acuerdo a la Proposición 54(c), un $\mathbb{F}_q$-álgebra R con una función peso v sobre R se llama un *dominio ordenado*.

Consideremos el conjunto

$$H(v) = \{v(f) : f \in R^*\} = \{h_1 < h_2 < \dots\}$$

que consiste en todos los enteros que aparecen como el orden de un elemento no nulo. Para cada $h_i \in H(v)$ sea $f_i \in R$ tal que $v(f_i) = h_i$ y consideremos el conjunto ordenado $\mathcal{F} = \{f_1, f_2, \dots\}$.

Proposición 55 *Sea R un dominio ordenado con función peso v. Consideremos los conjuntos $\mathcal{F} = \{f_1, f_2, \dots\}$ y $H(v)$ como antes. Entonces*

(1) $\mathcal{F}$ *es una base de* R *sobre* $\mathbb{F}_q$.

(2) si $f = \sum_j \lambda_j f_j$, *entonces* $v(f) = \max\{v(f_j) : \lambda_j \neq 0\}$.

(3) $H(v)$ *es un semigrupo numérico.*

Demostración. (1) Aplicando iterativamente la propiedad (W.5) se tiene que $\mathcal{F}$ es una base de R. (2) Se tiene de la Proposición 54(b). (3) Se deduce de las propiedades (W.2) y (W.4). ■

Ejemplo 56 *Sean* $\mathcal{X}$ *una curva sobre* $\mathbb{F}_q$ *y* Q *un punto racional de* $\mathcal{X}$. *Consideremos el* $\mathbb{F}_q$*-álgebra* $\mathcal{L}(\infty Q) = \bigcup_{m=0}^{\infty} \mathcal{L}(mQ)$ *donde* $\mathcal{L}(mQ)$ *es el conjunto de funciones racionales con polos únicamente en* Q *de orden a lo sumo* m. *Por las propiedades de valoración discreta, la función* $v = -v_Q$, *donde* v_Q *es la valoración en* Q, *es una función peso sobre* $\mathcal{L}(\infty Q)$. *Por tanto,* $\mathcal{L}(\infty Q)$ *es un dominio ordenado y el semigrupo* $H(v)$ *es, en este caso, el semigrupo de Weierstrass de* Q, $H(v) = H(Q) = \{-v_Q(f) : f \in \mathcal{L}(\infty Q) \setminus \{0\}\}$.

En la siguiente sección estudiaremos los semigrupos numéricos, pues como veremos más adelante, el semigrupo asociado a la función peso nos resultará útil para determinar los parámetros de los códigos provenientes de dominios ordenados.

2.2. Semigrupos numéricos.

Recordaremos algunos conceptos sobre semigrupos que utilizaremos continuamente en este trabajo. Una referencia general sobre semigrupos numéricos es [56].

Un *semigrupo numérico* es un conjunto $S \subseteq \mathbb{N}_0$ tal que: (i) $0 \in S$ y (ii) si $a, b \in S$ entonces $a + b \in S$. Un entero en S es un *número polar* (o *polo*) de S, mientras que un entero en $\mathbb{N}_0 \setminus S$ es una *laguna* de S. Denotamos por $\mathrm{Gaps}(S)$ el conjunto de lagunas de S. El número $g = \#\mathrm{Gaps}(S)$ es el *género* de S. Note que un semigrupo S tiene género finito si y sólo si el máximo común divisor de sus elementos no nulos es 1. Nosotros sólo consideraremos semigrupos de género finito.

El menor entero c tal que $a \in S$ para todo $a \geq c$ es el *conductor* de S.

Lema 57 *El conductor* c *de un semigrupo de género* g *satisface que* $c \leq 2g$.
Demostración. Como $c - 1$ es una laguna, dado un par $(a, b) \in \mathbb{N}_0^2$ con $a + b = c - 1$, al menos uno de estos dos números es también una laguna. Como hay c tales pares y g lagunas, obtenemos la desigualdad. ■

El semigrupo S es *simétrico* cuando $c = 2g$. Note que para semigrupos simétricos, dado un par $(a, b) \in \mathbb{N}_0^2$ con $a + b = c - 1$, exactamente uno de estos dos números es una laguna y el otro es un polo. Recíprocamente, esta condición garantiza que $c = 2g$.

El siguiente hecho se utilizará frecuentemente en este capítulo.

Lema 58 *Sea S un semigrupo de género g. Si $a \in S$ entonces*

$$\#(S \setminus (a + S)) = a.$$

Demostración. Sean c el conductor de S y m un entero. Si $m \geq a + c$ entonces $m \in S$ y $m \in a + S$. Consideremos $S \setminus (a + S) = U \setminus V$, donde $U = \{m \in S : m < a + c\}$ y $V = \{a + m : m \in S, a + m < a + c\} \subseteq U$. Ahora, como $\#U = a + c - g$ y $\#V = \#\{m \in S : m < c\} = c - g$. Entonces $\#(S \setminus (a + S)) = \#U - \#V = a$. ■

De acuerdo al Lema 57, el intervalo discreto $[0, 2g - 1]$ contiene g polos y g lagunas. Si escribimos a $S = \{\rho_1 = 0 < \rho_2 < \dots\}$ enumerando en forma creciente sus elementos, entonces $2g = \rho_{g+1}$, luego $\rho_{g+i} = 2g + i - 1$ para todo $i = 1, 2, \dots$. Así $\rho_i \leq i + g - 1$ y la igualdad se tiene cuando $i > g$. El primer elemento no nulo de S, ρ_2, es la *multiplicidad* de S.

En algunos casos podemos identificar explícitamente cuál es la secuencia de las lagunas y de los polos de S, por esta razón introducimos las definiciones siguientes.

Definición 59 (Oasis y desiertos) *Los oasis (resp. desiertos) de S son los conjuntos finitos maximales de polos consecutivos (resp. lagunas consecutivas) de S.*

Note que si ρ_2 es la multiplicidad del semigrupo S, entonces $\{1, 2, \dots, \rho_2 - 1\}$ y $\{\rho_1 = 0\}$ son respectivamente el primer desierto y el primer oasis de S. Análogamente, si S es simétrico, entonces $\{l_g = 2g - 1\}$ y $\{2g - 2, \dots, 2g - \rho_2\}$ son respectivamente el último desierto y el último oasis de S.

Un *conjunto de generadores* de S es un conjunto $A = \{a_1, \dots, a_r\} \subset S$ tal que cualquier $a \in S$ se puede escribir como una combinación lineal $a = \lambda_1 a_1 + \cdots + \lambda_r a_r$ con coeficientes enteros no negativos. En este caso denotaremos $S = \langle a_1, \dots, a_r \rangle$. Todo semigrupo admite un conjunto finito de generadores. Por ejemplo, el conjunto de Apéry

$$A(S) = \{a \in S^* : a - \rho_2 \notin S^*\}.$$

Para finalizar esta sección estudiaremos algunos casos especiales de semigrupos numéricos que mencionaremos constantemente en lo que sigue.

Semigrupos generados por dos elementos.

Sean $a, b \in \mathbb{N}$ con $a < b$ y $\mathrm{mcd}(a, b) = 1$. Consideremos el semigrupo generado por a y b, denotado por $S = \langle a, b \rangle$. Note que, en general para cada semigrupo S de género finito existen $a, b \in S$ tal que $\mathrm{mcd}(a, b) = 1$ y $\langle a, b \rangle \subseteq S$.

Lema 60 (Representación normal) *Sean $a, b \in \mathbb{N}$ con $a < b$ y $\mathrm{mcd}(a, b) = 1$. Si $S = \langle a, b \rangle$, entonces*

(1) para cada $m \in S$ existe una única representación

$$m = \lambda a + \mu b \quad con \quad 0 \leq \mu < a \quad y \quad \lambda \geq 0.$$

(2) para cada $l \in Gaps(S)$ existe una única representación

$$l = \lambda a + \mu b \quad con \quad 0 \leq \mu < a \quad y \quad \lambda < 0.$$

Demostración. Por el teorema de Bézout, todo entero m puede escribirse como $m = \lambda a + \mu b$. Sumando y restando ab a ambos sumandos si fuera necesario, podemos obtener una representación única de este tipo con $0 \leq \mu < a$. Entonces m es un polo cuando $\lambda \geq 0$ y una laguna cuando $\lambda < 0$. ■

En consecuencia, la mayor laguna es $-a+(a-1)b$. La proposición siguiente establece la propiedad de simetría del semigrupo $S = \langle a, b \rangle$.

Proposición 61 *Si $a, b \in \mathbb{N}$, $a < b$ y $\mathrm{mcd}(a, b) = 1$, entonces $S = \langle a, b \rangle$ es simétrico.*
Demostración. Por el Lema 60, la mayor laguna es $-a + (a - 1)b$. Supongamos que $-a + (a - 1)b = (\lambda_1 a + \mu_1 b) + (\lambda_2 a + \mu_2 b)$ con $\lambda_1, \lambda_2 < 0$, $0 \leq \mu_1, \mu_2 < a$. Entonces $(-\lambda_1 - \lambda_2 - 1)a = (\mu_1 + \mu_2 - a + 1)b$. Como $-\lambda_1 - \lambda_2 - 1 > 0$ se tiene que a divide a $\mu_1 + \mu_2 - a + 1 < a$, una contradicción. Entonces el semigrupo es simétrico. ■

En consecuencia, $S = \langle a, b \rangle$ tiene género $g = (a - 1)(b - 1)/2$.

Ejemplo 62 *El semigrupo S generado por 4 y 7 tiene género 9. Un cálculo directo muestra que $Gaps(S) = \{1, 2, 3, 5, 6, 9, 10, 13, 17\}$. S es el semigrupo de Weierstrass del único polo de x sobre la curva Norma-Traza $x^7 = y^4 + y^2 + y$ sobre $\mathbb{F}_8$.*

Semigrupos generados por dos elementos consecutivos.

Consideremos el semigrupo $S = \langle a, a+1 \rangle$. Éste, entre otros, es el caso del semigrupo de Weierstrass del punto infinito de la curva Hermitiana, ver el Ejemplo 35.

Note que, en este caso, existen $a-1$ oasis y $a-1$ desiertos de S. Denotaremos por M_t los oasis y por L_t los desiertos de S. Más aún, se tiene una caracterización sencilla de estos conjuntos:

(i) Para $t = 0, 1, ..., a-2$, $M_t = \{ta, ta+1, ..., ta+t\}$ es un oasis de S. Además, si $m_i \in M_t$, entonces $m_i = ta - \frac{t(t+1)}{2} - 1 + i$.

(ii) Para $t = 1, 2, ..., a-1$, $L_t = \{(t-1)a+t, (t-1)a+t+1, ..., ta-1\}$ es un desierto de S. Además, si $l_i \in L_t$, entonces $l_i = i + \frac{t(t+1)}{2} - 1$.

Ahora si utilizamos la representación normal de los polos y de las lagunas de S dada en el Lema 60, podemos identificar cada laguna $l \in \text{Gaps}(H)$ por $l \simeq (\lambda, \mu)$ si tiene representación normal $l = \lambda a + \mu(a+1)$ donde $0 \leq \mu < a$ y $\lambda < 0$. De manera análoga, identificaremos cada polo $m \in H$ por $m \simeq (\lambda, \mu)$ si tiene representación normal $m = \lambda a + \mu(a+1)$ donde $0 \leq \mu < a$ y $\lambda \geq 0$.

Proposición 63 *Sea* $S = \langle a, a+1 \rangle$.

(1) Si $m_i \in M_t$, *entonces* $m_i \simeq \left(\frac{(t+1)(t+2)}{2} - i, i - \frac{t(t+1)}{2} - 1 \right)$.

(2) Si $l_i \in L_t$, *entonces* $l_i \simeq \left((t-1)a - \frac{t(t-1)}{2} - i, i + \frac{t(t-1)}{2} - (a-1)(t-1) \right)$.

Demostración. Note que si $m_i \simeq (x, y) \in M_t$, entonces $x + y = t$. Análogamente, si $l_i \simeq (x, y) \in L_t$, entonces $x + y = t - 1$. (1) Como $m_i = ta - \frac{t(t+1)}{2} - 1 + i = (x+y)a + y$ entonces $y = i - \frac{t(t+1)}{2} - 1$ y $x = \frac{(t+1)(t+2)}{2} - i$. (2) Como $l_i = i + \frac{t(t+1)}{2} - 1 = (x+y)a + y$, entonces $y = i + \frac{t(t-1)}{2} - (a-1)(t-1)$ y $x = (t-1)a - \frac{t(t-1)}{2} - i$. ■

En resumen, podemos caracterizar los elementos de cada oasis (resp. desierto) de S como sigue:

1. Los elementos del t-ésimo oasis M_t son

$$\begin{aligned} ta = m_{\frac{t(t+1)}{2}+1} &\simeq (t, 0) \\ ta+1 = m_{\frac{t(t+1)}{2}+2} &\simeq (t-1, 1) \\ &\vdots \\ ta+t = m_{\frac{t(t+1)}{2}+(t+1)} &\simeq (0, t). \end{aligned}$$

2. Los elementos del t-ésimo desierto L_t son

$$\begin{aligned}(t-1)a+t=l_{(t-1)a-\frac{t(t-1)}{2}+1} &\simeq (-1,t)\\ (t-1)a+t+1=l_{(t-1)a-\frac{t(t-1)}{2}+2} &\simeq (-2,t+1)\\ &\vdots\\ ta-1=l_{ta-\frac{t(t+1)}{2}} &\simeq (-(a-t),a-1).\end{aligned}$$

Ejemplo 64 *Considere el semigrupo S generado por 5 y 6. Los desiertos y oasis de S son respectivamente $L_1=\{1,2,3,4\}$, $L_2=\{7,8,9\}$, $L_3=\{13,14\}$, $L_4=\{19\}$ y $M_0=\{0\}$, $M_1=\{5,6\}$, $M_2=\{10,11,12\}$, $M_3=\{15,16,17,18\}$.*

Semigrupos Telescópicos.

Los semigrupos telescópicos están generados por un conjunto ordenado de números naturales que satisfacen ciertas propiedades. Estos fueron introducidos por Christoph Kirfel y Ruud Pellikaan en [32].

Definición 65 El semigrupo $S_k=\langle a_1,\ldots,a_k\rangle$, donde el orden de los elementos es fijo, es un semigrupo *telescópico* si sus generadores ordenados satisfacen:

(i) $\mathrm{mcd}(a_1,\ldots,a_k)=1$;

(ii) para $i=2,\ldots,k$ se verifica que $a_i/\delta_i\in S_{i-1}=\langle a_1/\delta_{i-1},\ldots,a_{i-1}/\delta_{i-1}\rangle$ donde $\delta_i=\mathrm{mcd}(a_1,\ldots,a_i)$.

Note que semigrupos generados por dos elementos son semigrupos telescópicos. Más aún, si S_k es telescópico, entonces para $i=2,\ldots,k$ el semigrupo $S_i=\langle a_1/\delta_i,\ldots,a_i/\delta_i\rangle$ también es telescópico.

La siguiente proposición establece algunas propiedades de estos semigrupos, para su demostración ver [30, 32].

Proposición 66 *Sea $S_k=\langle a_1,\ldots,a_k\rangle$ un semigrupo telescópico. Entonces*

(1) [Representación normal] Para cada $m\in S$ existen una única representación

$$m=\sum_{i=1}^{k}\lambda_i a_i \quad \textit{tal que} \quad 0\leq\lambda_i<\delta_{i-1}/\delta_i \quad \textit{para} \quad i=2,\ldots,k.$$

(2) [Simetría] El conductor y el género de S_k satisfacen:

$$c(S_k) = \delta_{k-1}(c(S_{k-1}) - 1) + (\delta_{k-1} - 1)a_k = \sum_{i=1}^{k}(\delta_{i-1}/\delta_i - 1)a_i,$$

$$g(S_k) = \delta_{k-1}g(S_{k-1}) + (\delta_{k-1} - 1)(a_k - 1)/2 = c(S_k)/2.$$

Ejemplo 67 *El semigrupo $S = \langle 8, 12, 10, 13\rangle$ es telescópico y tiene género 14. Note que el orden de los generadores no puede ser el dado por el orden usual de los enteros, ya que en ese caso para $i = 3$ no se satisface la condición (ii) en la Definición 65. Por otra parte, S es el semigrupo de Weierstrass del punto infinito de la curva de Suzuki dada por la ecuación afín $y^8 - y = x^{10} - x^3$.*

2.3. Códigos de dominio ordenado y conjunto de dimensiones.

Sea R un dominio ordenado sobre $\mathbb{F}_q$ con función peso v. Consideremos el semigrupo asociado a v, $H = H(v) = \{h_1, h_2, \dots\}$. Si $\delta = \text{mcd}\{a : a \in H(v)^*\} = 1$ entonces el peso v es llamado *normal*. En otro caso, definimos la normalización de v como el peso $v' = v/\delta$. Para nosotros todas las funciones peso serán normales.

Para cada $h_i \in H$ sea $f_i \in R$ tal que $v(f_i) = h_i$. Por la Proposición 55, el conjunto ordenado $\mathcal{F} = \{f_1, f_2, \dots\}$ es una base de R como espacio vectorial sobre $\mathbb{F}_q$.

Ahora, para $m = -1, 0, 1, \dots$, consideramos los subespacios lineales

$$L(m) = \{f \in R : v(f) \leq m\}.$$

Note que $L(-1) = (\mathbf{0})$, $L(0) = \mathbb{F}_q$ y $\{f_i : h_i \leq m\}$ es una base de $L(m)$. Entonces $L(m-1) \subseteq L(m)$ con igualdad si m es una laguna de H. Como v es normal, H tiene un número finito de lagunas, g. Así la igualdad ocurre precisamente g veces. Si m es un polo, entonces $\dim(L(m)) = \dim(L(m-1)) + 1$.

Sea $\Phi : R \to \mathbb{F}_q^n$ un morfismo sobreyectivo de $\mathbb{F}_q$-álgebras (por ejemplo, una función evaluación). Los códigos lineales $C(\Phi, m) = \Phi(L(m))$ son llamados *códigos de dominio ordenado*. En consecuencia, obtenemos una cadena de códigos lineales

$$(\mathbf{0}) \subseteq C(\Phi, 0) \subseteq C(\Phi, 1) \subseteq \dots. \tag{2.1}$$

Como Φ es sobreyectiva, la cadena contiene exactamente $n + 1$ códigos distintos.

Definición 68 El *conjunto de dimensiones* de la cadena (2.1) es definido como

$$M = M(\Phi, v) = \{m \in \mathbb{N}_0 : C(\Phi, m-1) \neq C(\Phi, m)\}.$$

Note que M esta conformado por n números enteros y $M \subseteq H(v)$. Escribamos $M = \{m_1 = 0, m_2, \ldots, m_n\}$. El nombre conjunto de "dimensiones" de M esta justificado por el siguiente hecho.

Proposición 69 *Si m es un entero no negativo, entonces*

$$\dim(C(\Phi, m)) = \text{máx}\{i : m_i \leq m\}.$$

En consecuencia, $\dim(C(\Phi, m_k)) = k$.
Demostración. Si $k = \text{máx}\{i : m_i \leq m\}$ entonces $C(\Phi, m) = C(\Phi, m_k)$. ■

Lema 70 *Sean $m \in H$ y $f \in R$ tal que $v(f) = m$. Entonces $m \in M$ si y sólo si $\Phi(f) \notin C(\Phi, m-1)$.*
Demostración. Se sigue del hecho que $L(m) = L(m-1) + \langle f \rangle$ y por tanto $C(\Phi, m) = C(\Phi, m-1) + \langle \Phi(f) \rangle$. ■

El ideal (f), generado por f, es un subespacio lineal de R. Así, podemos considerar el anillo de cocientes $R/(f)$ como un espacio vectorial sobre $\mathbb{F}_q$. Las propiedades de la función peso v nos permiten dar estimaciones de los parámetros de $C(\Phi, m)$ como veremos a continuación.

Lema 71 *Sea R un dominio ordenado con función peso v. Si $f \in R^*$, un elemento no nulo, entonces* $\dim(R/(f)) = v(f)$.
Demostración. La función peso v envía el ideal (f) en el conjunto $v(f) + H$. Sean $f_1, f_2, \ldots \in R$ tales que $v(f_i) = h_i$ y $f_i \in (f)$ cuando $h_i \in v(f) + H$. Entonces $\{f_1, f_2, \ldots\}$ es una base de R y $\{f_i + (f) : h_i \notin v(f) + H\}$ es una base de $R/(f)$. Así, por el Lema 58, $\dim(R/(f)) = \#(H \setminus (v(f) + H)) = v(f)$. ■

Lema 72 *Sea $m \in H$. Si $m < n$ entonces $L(m) \cap \ker(\Phi) = (0)$.*
Demostración. Sea $f \in \ker(\Phi), f \neq 0$. Entonces $(f) \subseteq \ker(\Phi)$ y se tiene una aplicación bien definida, lineal y sobreyectiva, $\Phi : R/(f) \to \mathbb{F}_q^n$. Luego $\dim(R/(f)) \geq n$ y por el Lema 71, $v(f) \geq n$. Así $f \notin L(m)$. ■

Proposición 73 *Sea $m < n$ un entero no negativo. Entonces*

(1) $m \in M$ si y sólo si $m \in H$.

(2) El código $C(\Phi, m)$ tiene dimensión $k = \dim(L(m)) = \text{máx}\{i : h_i \leq m\}$ y distancia mínima $d \geq n - m$. Si el semigrupo H tiene género g y $2g \leq m < n$, entonces $k = m + 1 - g$.

Demostración. Note que si $m < n$ entonces, por el Lema 72, la función $\Phi : L(m) \to \mathbb{F}_q^n$ es inyectiva. Luego $m \in M$ si y sólo si $L(m-1) \neq L(m)$ esto es, si y sólo si $m \in H$. Así, $k = \dim(L(m)) = \text{máx}\{i : h_i \leq m\}$. Como H tiene g lagunas y su conductor verifica $c \leq 2g$, entonces cuando $m \geq 2g$ se tiene que $m = h_{m+1-g}$ y por tanto $k = m + 1 - g$. Para la afirmación acerca de la distancia mínima d. Sea $\mathbf{c} = \Phi(f)$, $f \in L(m)$, una palabra de $C(\Phi, m)$ con $wt(\mathbf{c}) = d$. Sea $I = \{1, \ldots, n\} \setminus \text{sop}(\mathbf{c})$ el conjunto de las coordenadas nulas de $\mathbf{c}$ y $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$ la proyección sobre las coordenadas de I. La función $\pi \circ \Phi : R \to \mathbb{F}_q^{n-d}$ es un morfismo sobreyectivo de álgebras. Como $f \in L(m) \cap \ker(\pi \circ \Phi)$, por el Lema 72, $m \geq n - d$ es decir $d \geq n - m$. ■

La desigualdad $d(C(\Phi, m)) \geq n - m$ es la *cota de Goppa* sobre la distancia mínima del código de dominio ordenado $C(\Phi, m)$. Note que esta generaliza la cota definida después del Teorema 25.

2.4. Cotas de orden para códigos de dominio ordenado.

Además de la cota de Goppa, podemos aplicar a $C(\Phi, m)$ y su dual $C(\Phi, m)^\perp$ las cotas de orden dadas en la Sección 1.1.2. Consideremos la secuencia de códigos

$$(\mathbf{0}) \subset C(\Phi, m_1) \subset \cdots \subset C(\Phi, m_n)$$

obtenida de la cadena de la Ecuación (2.1) después de borrar los códigos repetidos, es decir $M = \{m_1, \ldots, m_n\}$ es el conjunto de dimensiones de la cadena. Puesto que $\dim(C(\Phi, m_k)) = k$, la función de estratificación $\rho_{\mathcal{B}}$ definida en la Sección 1.1.2 puede escribirse como

$$\rho(\mathbf{v}) = \text{mín}\{\dim(C(\Phi, m)) : \mathbf{v} \in C(\Phi, m)\}.$$

Lema 74 *Sea $f \in R^*$, un elemento no nulo.*

(1) $\rho(\Phi(f)) \leq \dim C(\Phi, v(f))$ con igualdad si $v(f) \in M$.

(2) Si $v(f) \notin M$ entonces $v(fh) \notin M$ para todo $h \in R^*$.

Demostración. (1) La primera afirmación se tiene ya que $f \in L(v(f))$ y por tanto $\Phi(f) \in C(\Phi, v(f))$. Si $v(f) \in M$ entonces $\Phi(f) \in C(\Phi, v(f)) \setminus C(\Phi, (v(f) - 1))$ y

$\rho(\Phi(f)) = \dim C(\Phi, v(f))$. (2) Si $v(f) \notin M$ entonces $\Phi(f) \in C(\Phi, v(f)-1)$ luego existen $\psi \in L(v(f)-1)$ tal que $\Phi(f) = \Phi(\psi)$. Si $v(fh) \in M$ entonces $\dim C(\Phi, v(fh)) = \rho(\Phi(fh)) = \rho(\Phi(\psi h)) \leq \dim C(\Phi, v(\psi h))$. Como $v(fh) > v(\psi h)$ obtenemos la igualdad $C(\Phi, v(fh)) = C(\Phi, v(\psi h))$, contradiciendo la suposición $v(fh) \in M$. ■

Sea $\bar{H} = H \setminus M$. Por el Lema 74(2), $\bar{H} + H \subseteq \bar{H}$, es decir $M \subseteq H \setminus (\bar{H} + H)$.

Corolario 75 $M \subseteq H \setminus (qH^* + H)$.
Demostración. Sean $m \in H^*$ y $f \in R$ tal que $v(f) = m$. Así, $v(f^q) = qv(f) > v(f)$. Como Φ es un morfismo, se tiene que $\Phi(f^q) = \Phi(f) * \cdots * \Phi(f)$(q veces) $= \Phi(f)$. Luego $qm \notin M$. Esto demuestra que $qH^* \subseteq \bar{H}$, así $qH^* + H \subseteq \bar{H} + H$ y $M \subseteq H \setminus (\bar{H} + H) \subseteq H \setminus (qH^* + H)$. ■

Para $i = 1, \ldots, n$, sea $\phi_i \in R$ tal que $v(\phi_i) = m_i$. Por tanto, el conjunto $\mathcal{B} = \{\Phi(\phi_1), \ldots, \Phi(\phi_n)\}$ es una base de $\mathbb{F}_q^n$ y la secuencia de códigos (C_k) esta dada por

$$C_k = \langle \Phi(\phi_1), \ldots, \Phi(\phi_k) \rangle = C(\Phi, m_k),\ k = 1, \ldots, n.$$

Proposición 76 *Sean $h_r, h_s \in H$. Si $h_r + h_s = m_k \in M$ entonces $h_r, h_s \in M$. Más aún, si $h_r = m_i, h_s = m_j$, entonces $\rho(\Phi(\phi_i) * \Phi(\phi_j)) = k$ y la pareja $(\Phi(\phi_i), \Phi(\phi_j))$ se comporta bien.*
Demostración. Si $h_r + h_s \in M$, entonces, por el Lema 74(2), $h_r, h_s \in M$. Sean $h_r = m_i$ y $h_s = m_j$. En consecuencia, $\rho(\Phi(\phi_i) * \Phi(\phi_j)) = \rho(\Phi(\phi_i\phi_j)) = \dim C(\Phi, v(\phi_i\phi_j)) = \dim C(\Phi, m_i + m_j) = k$. Si $(a, b) \prec (i, j)$ entonces $v(\phi_a\phi_b) < v(\phi_i\phi_j)$ y por tanto $\rho(\Phi(\phi_a) * \Phi(\phi_b)) = \rho(\Phi(\phi_a\phi_b)) < \dim C(\Phi, m_i + m_j) = \rho(\Phi(\phi_i) * \Phi(\phi_j))$. ■

De la Proposición 76 se deduce una nueva versión de las cotas de orden para la distancia mínima de $C(\Phi, m)$ y $C(\Phi, m)^\perp$ como sigue. Para $r = 1, \ldots, n$, $s = 0, \ldots, n-1$, consideremos los conjuntos

$$\Lambda_r^* = \{(r, j) : m_r + m_j \in M\} \ \text{ y } \ N_s^* = \{(i, j) : m_i + m_j = m_{s+1}\}. \tag{2.2}$$

Definimos

$$d_{ORD}(k) = \min\{\#\Lambda_r^* : r = 1, \ldots, k\} \ \text{ y } \ d_{ORD}^\perp(k) = \min\{\#N_s^* : s = k, \ldots, n-1\}.$$

Mediante la aplicación de las cotas de los Teoremas 14 y 21 con respecto a la base $\{\Phi(\phi_1), \ldots, \Phi(\phi_n)\}$, obtenemos el siguiente resultado.

Teorema 77 *Para un entero no negativo m, se tiene que*

$$d(C(\Phi,m)) \geq d_{ORD}(\dim(C(\Phi,m))) \quad y \quad d(C(\Phi,m)^{\perp}) \geq d^{\perp}_{ORD}(\dim(C(\Phi,m))).$$

Las desigualdades dadas en el Teorema 77 son las cotas de *orden* (o *Feng-Rao*) para la distancia mínima del código primario $C(\Phi,m)$ y su dual $C(\Phi,m)^{\perp}$, respectivamente. No dependen de la base $\mathcal{B}$ sino del conjunto de dimensiones M.

Para la jerarquía de pesos del código $C(\Phi,m)$ se deduce el siguiente resultado.

Teorema 78 (Jerarquía de pesos) *Sea m un entero no negativo. Para cada $r = 1,\ldots,k = \dim C(\Phi,m)$, el r-ésimo peso de Hamming de $C(\Phi,m)$ satisface*

$$d_r(C(\Phi,m)) \geq d^*_r(k) = \min_{1\leq j_1<\cdots<j_r\leq k} \#\Lambda^*_{j_1,\ldots,j_r},$$

donde $\Lambda^*_{j_1,\ldots,j_r} = \Lambda^*_{j_1} \cup \cdots \cup \Lambda^*_{j_r}$.
Demostración. Es consecuencia del Teorema 17 y el hecho que $\#\Lambda_j \geq \#\Lambda^*_j$. ■

2.4.1. Cota de orden para códigos unipuntuales primarios.

Sean $\mathcal{X}$ una curva de género g sobre $\mathbb{F}_q$, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ el conjunto de puntos racionales sobre $\mathcal{X}$ y $\mathcal{P} = \{P_1,\ldots,P_n\}$. Del Ejemplo 56, se tiene que los códigos unipuntuales son códigos de dominio ordenado, donde $R = \mathcal{L}(\infty Q)$ y $v = -v_Q$. En esta sección utilizaremos la misma notación de la Sección 1.2.1. Para simplificar la exposición supondremos, de ahora en adelante, que $n > 2g$. Consideremos la cadena de códigos unipuntuales

$$(\mathbf{0}) \subseteq C(0) \subseteq \cdots \subseteq C(n+2g-1) = \mathbb{F}_q^n.$$

Sea $M = \{m_1,\ldots,m_n\}$ el conjunto de dimensiones de esta cadena. Recordemos que $M = \{m \in \mathbb{N}_0 : C(m) \neq C(m-1)\}$. Sean $H = H(Q) = \{h_1 = 0 < h_2 < \ldots\}$ el semigrupo de Weierstrass de Q y $\mathrm{Gaps}(H) = \{l_1,\ldots,l_g\}$ el conjunto de lagunas de H. El siguiente resultado caracteriza el conjunto M para códigos unipuntuales.

Proposición 79 $M = \{m \in H : \ell(mQ-D) = \ell((m-1)Q-D)\}$.
Demostración. Si $m \in M$ entonces $\ell(mQ) \neq \ell((m-1)Q)$ y $m \in H$. El núcleo de la función evaluación restringida a $\mathcal{L}(mQ)$ es $\mathcal{L}(mQ-D)$, así cuando $m < n$ esta evaluación es inyectiva y por tanto $m \in M$ si y sólo si $m \in H$. Cuando $m \geq n$ entonces $m-1, m \in H$ lo cual implica $\ell(mQ) = \ell((m-1)Q)+1$. Por tanto, $C(m) \neq C(m-1)$ si y sólo si ambos núcleos son iguales. ■

En consecuencia, para todo entero no negativo $m < n$ se tiene que $m \in M$ si y sólo si $m \in H$. Entonces, una vez H es conocido, el problema de calcular el conjunto de dimensiones M se reduce a determinar sus últimos g elementos. Ya que $C(n+2g-1) = \mathbb{F}_q^n$ deducimos que g elementos del conjunto $\{n, \ldots, n+2g-1\}$ están en M mientras que los otros g elementos no están.

Lema 80 *Sea $m \geq n$. Si $m \notin M$ entonces $m + h \notin M$ para todo $h \in H$.*
Demostración. Es consecuencia del comentario después del Lema 74. ■

Proposición 81 *Si $D \sim nQ$, entonces $M \cap \{n, \ldots, n+2g-1\} = \{n + l_1, \ldots, n + l_g\}$.*
Demostración. Si $D \sim nQ$ entonces $n \notin M$ y por el Lema 80 $n + h_1, \ldots, n + h_g \notin M$. La afirmación se sigue por razones de cardinalidad. ■

Ejemplo 82 (Códigos Hermitianos) *Por el Ejemplo 38, $D \sim nQ$. En consecuencia, la Proposición 81 establece el conjunto de dimensiones M para los códigos Hermitianos. Utilizando los resultados de la Sección 2.2 se tiene que*

$$M \cap \{n, \ldots, n+2g-1\} = \{n + (t-1)q + \lambda : 1 \leq t \leq a-1 \ y \ t \leq \lambda \leq a-1\}.$$

Del Teorema 77, la cota de orden sobre la distancia mínima de códigos unipuntuales primarios es:

$$d(C(m)) \geq d_{ORD}(\dim(C(m))).$$

Esta cota mejora la cota de Goppa, $d(C(m)) \geq d_G(C(m)) = n - m$, como probaremos en el siguiente resultado. Sea N el menor elemento en el conjunto $\bar{H} = H \setminus M$. Por la Proposición 73(1), $N \geq n$. De otra parte, los conjuntos Λ_i^* pueden reescribirse como $\Lambda_i^* = \{m_j \in M : m_i + m_j \in M\}$ o, ya que $\bar{H} + H \subseteq \bar{H}$ como se señalo en el comentario después del Lema 74, como $\Lambda_i^* = \{m \in M : m - m_i \in H\} = (m_i + H) \cap M$.

Proposición 83 *Para todo $i = 1, \ldots, n$ se tiene que $d_{ORD}(\dim(C(m_i))) \geq d_G(C(m_i))$. Si $m_i < N - l_g$ entonces se tiene la igualdad.*
Demostración. Para la primera afirmación es suficiente demostrar que $\#(M \setminus \Lambda_i^*) \leq m_i$ para todo i. Ya que $\Lambda_i^* = (m_i + H) \cap M$, se tiene que $M \setminus \Lambda_i^* \subseteq H \setminus (m_i + H)$ y esto se deduce del hecho de que $\#(H \setminus (m_i + H)) = m_i$, establecido en el Lema 58. Si $m_i + l_g < N$, entonces todos los elementos en $H \setminus (m_i + H)$ son menores que N y por tanto $M \setminus \Lambda_i^* = H \setminus (m_i + H)$. ■

Ejemplo 84 (Códigos de Suzuki) *Sea $\mathcal{S}$ la curva de Suzuki dada por la ecuación afín $y^8 - y = x^{10} - x^3$ sobre $\mathbb{F}_8$, ver Ejemplo 45. $\mathcal{S}$ tiene género $g = 14$ y 64 puntos*

racionales afines más un punto Q en infinito. Consideremos los códigos $C(m)$, donde D es la suma de los 64 puntos racionales de $\mathcal{S}$ diferentes de Q. El semigrupo de Weierstrass de Q es $H = \langle 8, 10, 12, 13\rangle = \{0, 8, 10, 12, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26, 28, \rightarrow\}$. Así $qH^* + H = \{64, 72, 74, 76, 77, 80, 82, 84, 85, 86, 87, 88, 89, 90, 92, \rightarrow\}$. Por el Corolario 75, $M \subseteq \{0, 8, 10, \ldots$ (igual que H) $\ldots, 63, 65, 66, 67, 68, 69, 70, 71, 73, 75, 78, 79, 81, 83, 91\}$. Como ambos conjuntos tienen cardinal $n = 64$ concluimos que son iguales. Un cálculo directo nos da la secuencia $(\#\Lambda_i^*,\ 1 \leq i \leq 64)$: (64, 56, 54, 52, 51, 48, 46, 44, 43, 42, 41, 40, 39, 38, 36, 35, 34, 33, 32, 31, 30, 29, 28, 28, 26, 25, 24, 23, 22, 21, 20, 21, 18, 19, 16, 17, 16, 13, 12, 14, 10, 13, 8, 12, 10, 9, 8, 8, 6, 8, 7, 4, 5, 4, 4, 4, 5, 4, 3, 2, 2, 2, 2, 1). Encontramos 14 códigos no abundantes $(m < 64)$ que mejoran la cota de Goppa (más todos los códigos abundantes). En concreto los correspondientes a los valores $m_i \in \{37, 45, 47, 49, 50, 53, 55, 57, 58, 59, 60, 61, 62, 63\}$. Más aún, obtenemos códigos $[64, 37, \geq 16], [64, 58, \geq 4], [64, 62, \geq 2]$ y $[64, 63, \geq 2]$ que alcanzan los mejores parámetros conocidos, ver [40].

Cuando el dual de un código unipuntual es de nuevo un código unipuntual, ver la Proposición 37, podemos usar las dos cotas de orden para estimar la distancia mínima de estos códigos, esto es la cota de orden primaria, $d_{ORD}(\dim C(m))$ y la cota de orden dual, $d^{\perp}_{ORD}(\dim C(n + 2g - 2 - m))$. Ambas cotas dan el mismo resultado, como lo establece el siguiente resultado, para su demostración ver e.g. [21].

Proposición 85 *Si existe una forma diferencial ω con polos simples y residuo 1 en todos los puntos $P_i \in \mathcal{P}$, tal que* $\operatorname{div}(\omega) = (n + 2g - 2)Q - D$, *entonces*

$$d_{ORD}(\dim C(m)) = d^{\perp}_{ORD}(\dim C(n + 2g - 2 - m)).$$

A continuación, estudiaremos la cota de orden para la familia especial de códigos unipuntuales sobre curvas Castillo.

2.4.2. Cota de orden para códigos Castillo.

Utilizaremos la misma notación que la Sección 1.2.2. Como consecuencia de las Proposiciones 46(2) y 81 obtenemos directamente el conjunto de dimensiones M.

$$M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H). \tag{2.3}$$

En consecuencia, $M = \{m_1, \ldots, m_n\}$ con $m_i = h_i$ cuando $i \leq n-g$ y $m_i = n+l_{i+g-n}$ cuando $i > n - g$. Más aún, el siguiente resultado establece una propiedad de simetría para el conjunto de dimensiones M, esto es, $m \in M$ si y sólo si $n + 2g - 1 - m \in M$.

Lema 86 (Simetría) *Para códigos Castillo,* $M = \{m \in H : n + 2g - 1 - m \in H\}$. *En consecuencia, para* $i = 1, \ldots, n$ *se tiene que* $m_{n-i+1} = n + 2g - 1 - m_i$.
Demostración. Por el teorema de Riemann-Roch, $\ell(mQ - D) = m - n + 1 - g + \ell((n + 2g - 2 - m)Q)$, luego $\ell(mQ) = \ell((m-1)Q)$ si y sólo si $\ell((n + 2g - 2 - m)Q) = \ell((n+2g-1-m)Q)$, esto es, si y sólo si $n+2g-1-m \in H$. Para la segunda afirmación note que $m_1 = 0$, $m_n = n + 2g - 1$ y $2g - 1 - m_i \in \text{Gaps}(H)$ para $i = 1, \ldots, g$. Por tanto, $m_{n+1-i} = n + 2g - 1 - m_i$. ■

El siguiente resultado establece una caracterización más simple de la propiedad de isometría dual, ver la Proposición 52.

Proposición 87 (Isometría dual) *Para códigos Castillo, existe* $\mathbf{x} \in (\mathbb{F}_q^*)^n$ *tal que para todo* $k = 1, \ldots, n$ *se verifica*

$$C(m_k)^\perp = \mathbf{x} * C(m_{n-k}).$$

Demostración. Por el Lema 86, $m_{n-k+1} > n+2g-2-m_k \geq n+2g-1-m_{k+1} = m_{n-k}$. Ahora, como M es el conjunto de dimensiones, $C(n + 2g - 2 - m) = C(m_{n-k})$. ■

Recuerde que códigos isométricos tienen la misma distancia mínima. Por tanto, para códigos Castillo podemos utilizar ambas cotas, la cota de orden primaria o la cota de orden dual para obtener estimaciones para la distancia mínima. Probaremos que ambas cotas dan el mismo resultado.

Proposición 88 *Sea* $C(m_k)$ *un código Castillo, con* $m_k \in M$. *Entonces para cada* $r = 1, \ldots, n$ *se tiene que* $\#N^*_{n-r} = \#\Lambda^*_r$. *En consecuencia,* $d_{ORD}(k) = d^\perp_{ORD}(n - k)$.
Demostración. Del Lema 86 se sigue que $m_{n+1-r} = n+2g-1-m_r$. En consecuencia, $\#N^*_{n-r} = \#\{(i,j) : m_i + m_j = m_{n-r+1}\} = \#\{(i,j) : m_r + m_j = m_{n-i+1}\} = \#\Lambda^*_r$. ■

Para Finalizar este capítulo, establecemos una técnica de mejora de los códigos de dominio ordenado.

2.4.3. Códigos de dominio ordenado mejorados.

Al elegir adecuadamente los elementos del dominio ordenado, a ser evaluados por el morfismo Φ, en algunos casos podemos cambiar ligeramente los códigos de dominio ordenado mejorando sus parámetros. Sea δ un entero, $0 < \delta \leq n$. Utilizaremos la misma notación que en las secciones anteriores. Para $i = 1, \ldots, n$, sea $\phi_i \in R$ tal que

$v(\phi_i) = m_i$, definimos el *código de dominio ordenado mejorado*

$$\overline{C}(\delta) = \langle \{\Phi(\phi_i) : \#\Lambda_i^* \geq \delta\} \rangle.$$

Por la Proposición 13, la distancia mínima de $\overline{C}(\delta)$ es al menos δ. Diremos que la secuencia (Λ_i^*) es *monótona* para δ si para cada i, j tal que $\#\Lambda_i^* \geq \delta$ y $\#\Lambda_j^* < \delta$ se tiene que $i < j$. Si (Λ_i^*) es monótona para δ entonces $\overline{C}(\delta)$ es un código de dominio ordenado habitual, así que sólo hay mejora de códigos de dominio ordenado para aquellos δ en los cuales la secuencia no es monótona.

Note que, en este caso, los códigos $\overline{C}(\delta)$ dependen del cambio de $\phi_1, \ldots, \phi_n$. De hecho, si $\#\Lambda_i^* = \delta$ y $\#\Lambda_j^* < \delta$ para algún $j < i$, entonces $v(\phi_i + \phi_j) = v(\phi_i)$ pero en general $\Phi(\phi_j) \notin \overline{C}(\delta)$, luego $\Phi(\phi_i + \phi_j) \notin \overline{C}(\delta)$. Por tanto, se tiene una colección de códigos mejorados con distancia designada δ, que dependen del conjunto $\{\phi_1, \ldots, \phi_n\}$.

Ejemplo 89 (Códigos de Suzuki mejorados) *Consideremos la curva de Suzuki $\mathcal{S}$ sobre $\mathbb{F}_8$ del Ejemplo 84. En ese ejemplo calculamos la secuencia $(\#\Lambda_i^*)$. Esta secuencia es monótona excepto para $\delta = 5, 7, 8, 9, 10, 12, 13, 14, 17, 19, 21$.*

Sea $k_\delta = \dim(\overline{C}(\delta))$ la dimensión del código mejorado $\overline{C}(\delta)$ y sea $m_{k_\delta} \in M$ el elemento en el conjunto de dimensiones M tal que $k_\delta = \dim(C(m_{k_\delta}))$. La siguiente tabla contiene la dimensión k_δ de los códigos de Suzuki mejorados, recuerde que la distancia mínima es al menos δ. También hemos incluido la cota de orden del código de Suzuki habitual $C(m_{k_\delta})$ con igual dimensión, para analizar la mejora de los códigos de Suzuki.

δ	21	19	17	14	13	12	10	9	8	7	5
k_δ	31	33	35	38	40	42	44	45	49	50	53
m_{k_δ}	44	46	48	51	53	55	57	58	62	63	67
$d_{ORD}(k_\delta)$	20	18	16	13	12	10	8	8	6	6	4

Por la Proposición 51(3), la verdadera distancia mínima de $C(57)$ y $C(58)$ es 8 (esto es, $d(C(57)) = d(C(58)) = 8$). Ahora, note que los códigos de Suzuki mejorados $\overline{C}(10)$ y $\overline{C}(9)$ tienen sus mismas dimensiones respectivamente y su distancia mínima es mayor. Por otro lado, el código de Suzuki $C(52)$ tiene dimensión 39 y distancia mínima al menos 12 (es decir, $d_{ORD}(39) = 12$), mientras que el código de Suzuki mejorado $\overline{C}(12)$ tiene la misma estimación para la distancia mínima pero dimensión 42.

Capítulo 3

Distancia mínima de códigos Castillo

En este capítulo damos una caracterización de la cota de orden para la distancia mínima de los códigos Castillo primarios (Sección 3.1). En la Sección 3.2 calculamos explícitamente esta cota para los códigos Castillo que tienen semigrupo de Weierstrass generado por dos elementos consecutivos. Como caso especial de estos, obtenemos una nueva caracterización de la verdadera distancia mínima de los códigos Hermitianos que es más simple que las conocidas hasta el momento (Subsección 3.2.1). Estos resultados fueron publicados en [51]. En la Sección 3.3 consideramos el caso general cuando el semigrupo es generado por dos elementos cualesquiera y calculamos la cota de orden para todos estos códigos. También obtenemos resultados similares, pero incompletos, para el caso de códigos Castillo con semigrupo telescópico (Sección 3.4). Para finalizar, completamos el cálculo explícito de la cota de orden para todos los códigos de Suzuki (Sección 3.5). Estos resultados fueron publicados en [53].

3.1. Caracterizando la cota de orden para códigos Castillo.

Sea $\mathcal{X}$ una curva Castillo con respecto al punto racional Q, de género g sobre $\mathbb{F}_q$. Sean $H = \{h_1 = 0, h_2, \dots\}$ el semigrupo de Weierstrass de Q, $\text{Gaps}(H) = \{l_1, \dots, l_g\}$ el conjunto de lagunas de H y $M = \{m_1, \dots, m_n\}$ el conjunto de dimensiones.

Nuestro propósito en esta sección es presentar una caracterización de la cota de orden para la distancia mínima de los códigos Castillo primarios $C_i = C(m_i)$, es decir $d_{ORD}(i)$. Como veremos esta caracterización solo depende de los valores del semigrupo de Weierstrass. Para simplificar la exposición, si no se tendrían que considerar muchos casos, en lo que sigue supondremos que $n > 2c - m_2$, donde c es el conductor y m_2 la multiplicidad del semigrupo H.

Proposición 90 *Si $m_i \leq n-c$, entonces $\#\Lambda_i^* = n - m_i$. Por tanto, $d_{ORD}(i) = n - m_i$.*
Demostración. Como $m_i + c \leq n$ entonces el conductor del conjunto $m_i + H$ es a lo sumo n. De la Ecuación (2.3) se sigue que $M = H \setminus (n + \mathbb{N}_0)) \cup \{n + \text{Gaps}(H)\}$, así

$$\begin{aligned} \Lambda_i^* = (m_i + H) \cap M &= (m_i + H) \cap [(H \setminus (n + \mathbb{N}_0)) \cup \{n + \text{Gaps}(H)\}] \\ &= [(m_i + H) \cap (H \setminus (n + \mathbb{N}_0))] \cup \{n + \text{Gaps}(H)\}. \end{aligned}$$

Puesto que $(m_i+H)\cap(H\setminus(n+\mathbb{N}_0)) = (m_i+H)\setminus(n+\mathbb{N}_0)$ y este conjunto tiene cardinal $n - m_i - g$, concluimos la primera afirmación $\#\Lambda_i^* = n - m_i$. La segunda afirmación se deduce del hecho anterior ya que la secuencia (m_i) es creciente. ■

En consecuencia, para $m_i \leq n - c$, la cota de orden para la distancia mínima del código Castillo C_i es igual a la cota de Goppa, es decir $d_{ORD}(i) = d_G(C_i) = n - m_i$.

Por tanto, en lo que sigue estudiaremos el caso $m_i > n - c$. Para un entero w, $0 < w < c$, definimos el conjunto

$$D(w) = \{(l, m) : l \in \text{Gaps}(H), m \in M, l - m = w\}.$$

El lema siguiente establece algunas propiedades fundamentales del conjunto $D(w)$. La primera hace referencia a la simetría del conjunto $D(w)$, mientras que las otras dos a su cardinal.

Lema 91 *El conjunto $D(w)$ satisface las siguientes propiedades.*

(a) $(l, m) \in D(w)$ si y sólo si $(c - 1 - m, c - 1 - l) \in D(w)$.

(b) Si $w \in H$ entonces $D(w) = \emptyset$.

(c) $\#D(c - 1) = 1$. Si $w \in Gaps(H)$ y $w \neq c - 1$ entonces $\#D(w) \geq 2$.

Demostración. (a) $(c - 1 - m) - (c - 1 - l) = l - m = w$. (b) Si $(l, m) \in D(w)$ entonces $l = m + w$ lo cual es una contradicción ya que $m, w \in H$ y $l \in \text{Gaps}(H)$. (c) Si $w \in \text{Gaps}(H)$ entonces $(w, 0), (c - 1, c - 1 - w) \in D(w)$, pero si $w = c - 1$ estos son iguales. ■

Note que los elementos del conjunto $D(w)$ para $w \in \text{Gaps}(H)$ están sobre la recta $y = x - w$ con $0 < x < c = 2g$. En la Figura 3.1 se muestran, sobre la recta $y = x - w$, los conjuntos $D(w)$ para los semigrupos $H = \langle 4, 7\rangle = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, \rightarrow\}$ y $H = \langle 5, 6\rangle = \{0, 5, 6, 10, 11, 12, 15, 16, 17, 18, 20 \rightarrow\}$ respectivamente.

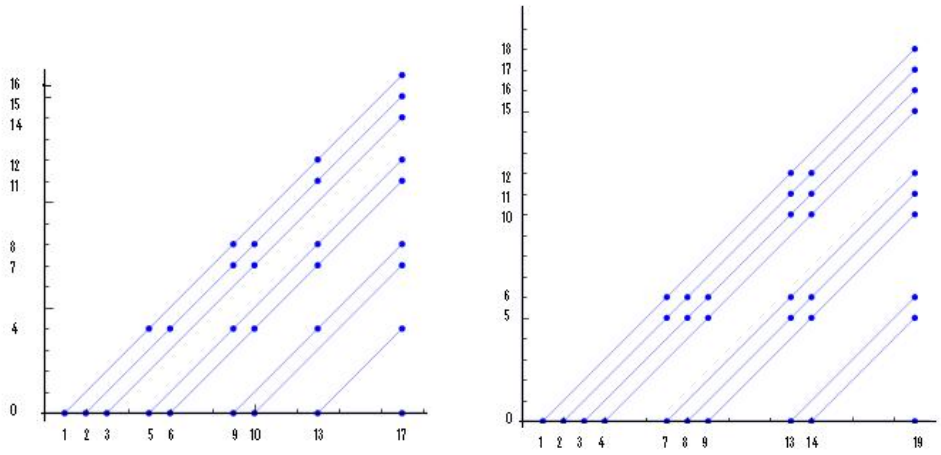


Figura 3.1: Los conjuntos $D(w)$ para $H = \langle 4, 7\rangle$ y $H = \langle 5, 6\rangle$ respectivamente.

Proposición 92 *Si $m_i > n - c$, entonces*

$$\#\Lambda_i^* = \begin{cases} n - m_i + \#D(n - m_i) & si \quad m_i < n \\ \#D(m_i - n) & si \quad m_i > n \end{cases}.$$

Demostración. Primero supongamos que $n - c < m_i < n$. Consideremos los conjuntos $A = \{m \in (m_i + H) \cap M : m < n\}$, $B = \{m \in (m_i + H) \cap M : n \leq m < m_i + c\}$ y $C = \{m \in (m_i + H) \cap M : m \geq m_i + c\}$. Note que $\Lambda_i^* = (m_i + H) \cap M = A \cup B \cup C$. Calculemos el cardinal de cada uno de estos conjuntos. Veamos que $\#A = \#C = \omega_i$, donde ω_i es el número de elementos de H menores que $n - m_i$. En efecto, $m \in A$ si y sólo si $m = m_i + h < n$, para algún $h \in H$, i.e. $h < n - m_i$. Análogamente, $m \in C$ si y sólo si $m = n + l \geq m_i + c$, para algún $l \in \text{Gaps}(H)$ i.e. $c - 1 - l < n - m_i$ y por la simetría de H se tiene la afirmación. Ahora probaremos que $\#B = n - m_i - 2\omega_i + \#D(n - m_i)$. En efecto, $m \in B$ si y sólo si $m = m_i + h = n + l$ para algún $h \in H$ con $n - m_i < h < c$ y $l \in \text{Gaps}(H)$, i.e. $h + c - 1 - l = n + c - 1 - m_i$. Por la simetría de H esta igualdad es $h + h' = h_{n+g-m_i}$, donde $h' = c - 1 - l \in H$. De acuerdo a [30, Thm. 5.24] el número de soluciones de la ecuación $h^{(1)} + h^{(2)} = h_{g+n-m_i}$ con $h^{(1)}, h^{(2)} \in H$, es $n - m_i + \#\tilde{D}(g + n - m_i - 1)$, donde $\tilde{D}(t) = \{(x, y) : x, y \in \text{Gaps}(H), x + y = h_{t+1}\}$. Como $(x, y) \in \tilde{D}(g + n - m_i - 1)$ si y sólo si $(x, c - 1 - y) \in D(n - m_i)$ se tiene que $\#\tilde{D}(g + n - m_i - 1) = \#D(n - m_i)$. Por otra parte, existen ω_i soluciones de $h^{(1)} + h^{(2)} = h_{g+n-m_i}$ tales que $h^{(1)} < n - m_i$ y otras ω_i soluciones tales que $h^{(1)} \geq c$, Así, sumando los anteriores resultados obtenemos nuestra afirmación sobre $\#B$ y la primera igualdad de la proposición. La segunda igualdad es inmediata. Si $m_i > n$, entonces $m \in \Lambda_i^*$ si y sólo si $m = m_i + h = n + l$, i.e. si y sólo si $(l, h) \in D(m_i - n)$. ■

En consecuencia, para $n - c < m_i < n$, los números $\#D(n - m_j)$, para $i \leq j \leq g$, determinan la mejora de la cota de orden $d_{ORD}(i)$ sobre la cota de Goppa $d_G(C_i)$.

Corolario 93 *Si $n-m_i \in H$, entonces $\#\Lambda_i^* = n-m_i$. Así, $d_{ORD}(i) = n-m_i = d_G(C_i)$.*

Note que para $m_i < n$ se podría tener una mejora de la cota de Goppa, $d_G = n-m_i$ solamente cuando $n-m_i$ es una laguna de H. El máximo valor posible de dicha mejora es obtenido también como consecuencia de la Proposición 92 y el Corolario 93.

Corolario 94 *Si $m_i < n$, entonces* $d_{ORD}(i) \leq \min\{h \in H : h \geq n - m_i\}$.

En general, la igualdad en el anterior corolario no siempre se tiene, para $n - m_i \in \text{Gaps}(H)$, como lo muestra el siguiente ejemplo.

Ejemplo 95 (Código de Suzuki sobre $\mathbb{F}_8$) *Consideremos los códigos unipuntuales sobre la curva de Suzuki $\mathcal{S}$ del Ejemplo 84, dada por la ecuación afín $y^8 - y = x^{10} - x^3$ sobre $\mathbb{F}_8$. Sabemos que los elementos del conjunto de dimensiones correspondientes a las dimensiones 49 y 50 son respectivamente $m_{49} = 62$ y $m_{50} = 63$. Así, por el Corolario 94 se tiene que $d_{ORD}(49) \leq 8$ y $d_{ORD}(50) \leq 8$. Un cálculo directo, utilizando la secuencia $(\#\Lambda_i^*, 1 \leq i \leq 64)$ del Ejemplo 84, muestra que $d_{ORD}(49) = d_{ORD}(50) = 6$. De otra parte, por la Proposición 51(3) se tiene que la verdadera distancia mínima de estos códigos es $d(C_{49}) = d(C_{50}) = 8$. Esto muestra, el hecho sorprendente, que la fórmula del Corolario 94 puede proporcionar el valor real de la distancia mínima de un código aunque no coincida con la cota de orden d_{ORD}.*

El siguiente resultado muestra que cuando $m_i = n - l_g$ se obtiene una mejora de la cota de orden sobre la cota de Goppa.

Lema 96 *Si $m_i = n - l_g$ entonces $d_{ORD}(i) = c$. En consecuencia, $d_{ORD}(i) > d_G(C_i)$.*
Demostración. Por el Lema 91(c), $D(l_g) = 1$ y por la Proposición 92, $\#\Lambda_i^* = c$. Por tanto, por lo demostrado en la Proposición 90 se sigue el resultado. ■

Por una simple inspección podemos afirmar que el anterior valor no es el único para el cual se tiene la desigualdad estricta entre la cota de orden y la cota de Goppa, como lo muestra el siguiente resultado.

Lema 97 *Si $n - m_i \in \text{Gaps}(H)$, es el elemento final de un desierto de H, entonces $d_{ORD}(i) > d_G(C_i)$.*
Demostración. Análogamente a la prueba del lema anterior y utilizando el Corolario 93 obtenemos el resultado. ■

Para algunos tipos particulares de semigrupos se tiene la igualdad en el Corolario 94, como mostraremos a continuación. En lo que resta de este capítulo nos restringiremos a semigrupos generados por dos elementos y semigrupos telescópicos.

3.2. Semigrupos generados por dos elementos consecutivos.

En esta sección suponemos que $H = \langle a, a+1\rangle$ es un semigrupo generado por dos elementos consecutivos. Éste es, entre otros, el semigrupo de Weierstrass del punto infinito de la curva Hermitiana, ver Ejemplo 35.

Utilizaremos la notación de la Subsección 2.2(2). Sea $l_s \in L_t$, identificaremos l_s con (x, y), denotado por $l_s \simeq (x, y)$, si tiene representación normal $l_s = xa + y(a+1)$ donde $0 \leq y < a$ y $-a < x < 0$. Note que l_s es la única laguna en el desierto L_t que es primer elemento de una pareja de $D(l_s)$. Para los demás desiertos entre $t+1$ y $a-1$ (estos son $a-1-t$ desiertos) se tiene que $(l_u, l_u - l_s) \in D(l_s)$ con $l_u \simeq (x', y')$ si se cumple que $x' \geq x$ y $y' \geq y$. Definimos los conjuntos

$$A = \{l_u \simeq (x', y') : l_u \geq l_s, x' \geq x\} \text{ y } B = \{l_u \simeq (x', y') : l_u \geq l_s, y' < y\}.$$

Lema 98 *Sean A y B como antes. Entonces se verifica*

(1) $\#A = 1 + (-x)(x + (a-t)) + \frac{-x(-x-1)}{2}$.

(2) $\#B = \frac{(y-t)(y-t-1)}{2}$.

Demostración. Consideremos los desiertos L_γ para $\gamma = t+1, \ldots, a-1$. (1) Los primeros $x + (a-t) \geq 0$ desiertos tienen $-x$ elementos que pertenecen a A. Para los demás $(a-1-t) - x - (a-t) = -x-1$ desiertos posteriores se tienen respectivamente $(-x-1), (-x-2), \ldots, 1$ elementos en A. En consecuencia, $\#A = 1+(-x)(x+(a-t))+\frac{-x(-x-1)}{2}$. (2) Existen $y-t-1$ desiertos que tienen respectivamente $y-t-1, y-t-2, \ldots, 1$ elementos en B. En consecuencia $\#B = \frac{(y-t)(y-t-1)}{2}$. ■

Lema 99 *Si $l_s \in Gaps(H)$, $l_s \in L_t$ y $l_s \simeq (x, y)$, entonces $\#D(l_s) = -x(x+a-t+1)$.*
Demostración. Note que $\#D(l_s) = \#A - \#B$. Por el lema anterior y el hecho que $x + y = t - 1$ se tiene el resultado. ■

Corolario 100 *Para $1 \leq t < a-1$.*

$$\#D\left(l_{(t-1)a-\frac{t(t-1)}{2}+1}\right) = \#D\left(l_{ta-\frac{t(t-1)}{2}}\right) = a - t.$$

Demostración. Puesto que $l_{(t-1)a-\frac{t(t-1)}{2}+1} = (t-1)a+t \simeq (-1,t)$ y $l_{ta-\frac{t(t-1)}{2}} = ta-1 \simeq (t-a,a-1)$. Las afirmaciones se siguen del Lema 99. ■

Note que el Corolario 100 muestra la igualdad en el cardinal del conjunto D en el caso de la primera y última laguna de cada desierto L_t, para todo $t = 1, 2..., a-1$. Ahora veamos que cuando l es un elemento intermedio en el desierto L_t se tiene que el cardinal de $D(l)$ es mayor o igual que $a-t$.

Lema 101 *Para cada $t = 1, 2..., a-1$. Si $l_{(t-1)a-\frac{t(t-1)}{2}+1} < l < l_{ta-\frac{t(t-1)}{2}}$, entonces*

$$\#D(l) \geq a-t.$$

Demostración. Supongamos que $l \simeq (x,y)$. En consecuencia, $x = -1-k$ para algún $1 \leq k \leq a-t-2$. Así, por el Lema 99, $\#D(l) = a-t+k(a-t-k-1)$ y puesto que $a-t-1-k > 0$ se tiene el resultado. ■

Para el caso $m_i < n$. Sea $n-m_i = l_s \in \text{Gaps}(H)$ y supongamos que $l_s \in L_t$, entonces $(t-1)a+(t-1) < l_s < ta$. Es decir, $l_s = ta-\lambda$ para $1 \leq \lambda \leq a-t$.

Teorema 102 *Sea $m_i < n$. Si $n-m_i = l \in L_t$, entonces*

$$d_{ORD}(i) = ta = \text{mín}\{h \in H : h \geq n-m_i\}.$$

Demostración. Por el Corolario 100 y el Lema 101 se tiene que $\#D(n-m_i) \geq a-t$. Así, por la Proposición 92, $\#\Lambda_i^* \geq l+(a-t) = ta+(a-t-\lambda) \geq ta$. Por tanto, utilizando el Corolario 94, obtenemos el resultado. ■

Finalmente, consideramos el caso en el que $m_i > n$. Entonces $m_i = n+l_{i-n+g}$.

Teorema 103 *Si $m_i - n = l_{i-n+g} \in L_t$, entonces $d_{ORD}(i) = a-t$.*
Demostración. Es consecuencia del Corolario 100 y el Lema 101. ■

3.2.1. Códigos Hermitianos.

Sea $\mathcal{H} : y^q+y = x^{q+1}$ la curva Hermitiana de género $g = \frac{q(q-1)}{2}$ sobre $\mathbb{F}_{q^2}$. Recuerde que esta tiene q^3 puntos racionales afines más el punto Q en infinito. El semigrupo de Weierstrass de Q es $H = H(Q) = \langle q, q+1 \rangle$, ver Ejemplo 35.

Para cada $m_i \in M$ consideremos el código Hermitiano $C_i = C(\mathcal{H}, D, m_iQ)$ donde D es la suma de los q^3 puntos racionales de $\mathcal{H}$ diferentes de Q. Claramente la longitud de C_i es $n = q^3$ y la dimensión es $k(C_i) = i$.

La cota de orden $d_{ORD}(i)$ sobre la distancia mínima de los códigos Hermitianos, es como sigue. Por el Corolario 93 y el Teorema 102, $d_{ORD}(i) = \min\{h \in H : h \geq n - m_i\}$ para $i \leq n - g$. De otra parte, por el Teorema 103, $d_{ORD}(i) = q - t$ para $n - g < i \leq n$, donde $m_i = n + l_{i-n+g}$ con $l_{i-n+g} \in L_t$ (es una laguna en el t-ésimo desierto).

La distancia mínima de los códigos Hermitianos fue establecida por Kyeongcheol Yang y P. Vijay Kumar en [62]. Note que en este caso la cota $d_{ORD}(i)$ coincide con la verdadera distancia mínima $d(C_i)$ de los códigos Hermitianos. La tabla siguiente resume la nueva caracterización de los valores de la distancia mínima $d(C_i)$ de los códigos Hermitianos C_i para todo $i = 1, \ldots, n$.

i	$d(C_i)$	condición
$i \leq n - g$	$n - m_i$	si $n - m_i \in H$
	qt	si $n - m_i \in L_t$
$n - g < i \leq n$	$q - t$	$m_i - n \in L_t$

Esta nueva caracterización del verdadero valor de la distancia mínima de códigos Hermitianos es la más simple de las conocidas en la literatura (ver [62] y [30]) y resalta el hecho de que la distancia mínima sólo difiere de la cota de Goppa cuando $m_i = n - l_w$ para toda laguna l_w. Observe también que se puede construir un código [64,53,8] sobre $\mathbb{F}_{16}$ que es un nuevo record, según las tablas MinT [40].

3.3. Semigrupos generados por dos elementos cualesquiera.

En esta sección supondremos que $H = \langle a, b \rangle$ con $a < b$ y $\mathrm{mcd}(a, b) = 1$. Primero estudiaremos el caso en el que $n - c < m_i < n$.

Lema 104 *Si $n - m_i = l \in Gaps(H)$, sea s tal que $h_{s-1} < l < h_s$, entonces $\#\Lambda_i^* \geq h_s$.*
Demostración. Por la Proposición 92, es suficiente demostrar que $\#D(l) \geq h_s - l$. Como $(l_k, m_j) \in D(l)$ si y sólo si $l_k - m_j = l$ si y sólo si $m_j + c - 1 - l_k = c - 1 - l$. Sea $m = c - 1 - l \in M$. De acuerdo a [30, Lemma 5.27], existe una laguna en el intervalo $[m - \#D(l), m]$. Como $\{l, l + 1, ..., h_s - 1\} \subset \mathrm{Gaps}(H)$, por la simetría se tiene que $\{c - h_s, ..., c - 1 - l = m\} \subset H$. Entonces $m - \#D(l) < c - h_s$ y por tanto $\#D(l) \geq h_s - l$. ■

El siguiente resultado muestra que cuando H es el semigrupo generado por dos elementos cualesquiera entonces también se tiene la igualdad en el Corolario 94.

Teorema 105 *Si $m_i < n$, entonces $d_{ORD}(i) = \min\{h \in H : h \geq n - m_i\}$.*
Demostración. Si $n - m_i \in H$ entonces el resultado se sigue por el Corolario 93. Supongamos que $n - m_i \in \text{Gaps}(H)$. Si $n - m_i = c - 1$ entonces, por el Lema 91(c), se tiene que $\#D(l_g) = 1$, luego $\Lambda_i^* = c$ y $d_{ORD}(i) = c$. En otro caso, si $n - m_i = l_t \neq c - 1$, podemos escribir $h_{s-1} < n - m_i < h_s$ con $a \leq h_s \leq c - a$ por la simetría de H. Entonces $m_j = n - h_s \in M$, así $\#\Lambda_j^* = h_s$ y por el Lema 104 se concluye la prueba. ■

Ejemplo 106 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Por el Ejemplo 43 se tiene que la curva Norma-Traza $\mathcal{X}$ sobre $\mathbb{F}_8$ dada por la ecuación afín $x^7 = y^4 + y^2 + y$ tiene género $g = 9$ y 33 puntos racionales sobre $\mathbb{F}_8$. El semigrupo de Weierstrass del único polo Q de x es $H = H(Q) = \langle 4, 7\rangle = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, \rightarrow\}$. Así, el conjunto de dimensiones es $M = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18 - 31, 33, 34, 35, 37, 38, 41, 42, 45, 49\}$. En la tabla siguiente se resumen los valores para la cota de orden de los códigos Norma-Traza sobre $\mathbb{F}_8$ de dimensión $k \leq 23$, todos estos se obtienen como consecuencia del Teorema 105.*

k	1	2	3	4	5	6	7	8	9	10	11	12
m_k	0	4	7	8	11	12	14	15	16	18	19	20
$d_{ORD}(k)$	32	28	25	24	21	20	18	18	16	14	14	12
k	13	14	15	16	17	18	19	20	21	22	23	
m_k	21	22	23	24	25	26	27	28	29	30	31	
$d_{ORD}(k)$	11	11	11	8	7	7	7	4	4	4	4	

Vamos a estudiar ahora el caso $m_i > n$. Recuerde que $m_i = n + l$ con $l \in \text{Gaps}(H)$.

Para $t = 1, 2, \ldots, a - 1$, consideremos los números $\lambda_t = tb - a$. Es claro que cada uno de estos números es una laguna de H y las llamaremos *lagunas especiales* de H. Además definamos $\lambda_0 = 0$.

En la Figura 3.2 hemos señalado con una barra las lagunas especiales para los semigrupos $H = \langle 4, 7\rangle$ y $H = \langle 5, 6\rangle$ respectivamente. También hemos incluido el valor de los conjuntos $D(w)$ para $w \in \text{Gaps}(H)$. Note que cuando $H = \langle a, a + 1\rangle$, es el semigrupo es generado por dos elementos consecutivos, las lagunas especiales son los primeros elementos en cada desierto L_t para $t = 1, \ldots, a - 1$. Observemos también que las lagunas especiales son los elementos $l \in \text{Gaps}(H)$ para los cuales el cardinal del conjunto $D(l)$ es minimal con respecto a las anteriores lagunas. Esto lo justificamos en el siguiente resultado.

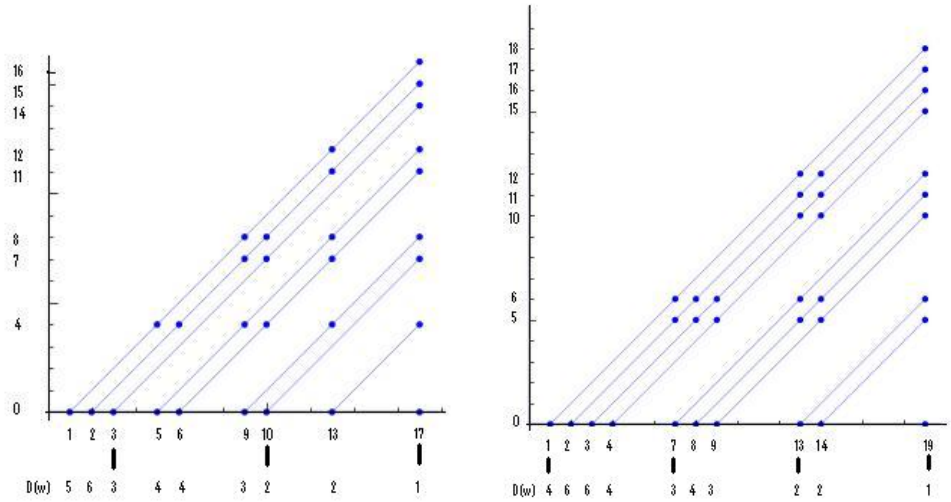


Figura 3.2: Lagunas especiales de $H = \langle 4, 7\rangle$ y $H = \langle 5, 6\rangle$ respectivamente.

Lema 107 *Si $m_i = n + l$ donde $l \in Gaps(H)$ tal que $\lambda_t \leq l < \lambda_{t+1}$ entonces*

$$\#D(l) \geq \#D(\lambda_t) = a - t.$$

Demostración. Si $l = \lambda_t$, entonces $(l_k, m_j) \in D(\lambda_t)$ si y sólo si $l_k - m_j = \lambda_t$, esto es, si y sólo si $m_j + c - 1 - l_k = c - 1 - \lambda_t$. Como $c - 1 - \lambda_t = (a - 1 - t)b$, de acuerdo a [30, Lemma 5.27], existen $a - t$ pares que satisfacen esta igualdad. Ahora la prueba del caso $\lambda_t < l < \lambda_{t+1}$. Análogamente $(l_k, m_j) \in D(l)$ si y sólo si $m_j + c - 1 - l_k = c - 1 - l$. Sean $m_{j'} = c - 1 - l_k$, $m_s = c - 1 - l$ y supongamos que $m_s = xa + yb$. Luego, como $c - i - \lambda_{t+1} < m_s < c - 1 - \lambda_t$ i.e. $(a - 2 - y)b < m_s < (a - 1 - t)b$, entonces $0 \leq y \leq a - 1 - t$. Por [30, Lemma 5.27], el número de soluciones de $m_j + m_{j'} = m_s$ es $(x + 1)(y + 1)$. Por tanto,

$$(x+1)(y+1) > \left(\frac{(a-2-t-y)b}{a} + 1\right)(y+1) \geq (a-2-t-y) + (y+1) = a - 1 - t.$$

En consecuencia, $\#D(l) \geq a - t$. ■

Ahora, directamente del Lema 107 obtenemos el siguiente resultado que establece los valores de $d_{ORD}(i)$ cuando $m_i > n$. Es decir, $m_i = n + l_{i-n+g}$.

Teorema 108 *Sea $m_i > n$. Si $\lambda_t \leq l_{i-n+g} < \lambda_{t+1}$, entonces $d_{ORD}(i) = a - t$.*

Ejemplo 109 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Continuando con el Ejemplo 133. Por el Teorema 108 se tienen los valores para la cota de orden de los códigos Norma-Traza sobre $\mathbb{F}_8$ de dimensión $24 \leq k \leq 32$. Hemos resaltado los valores correspondientes a las lagunas especiales de H.*

k	*24*	*25*	**26**	*27*	*28*	*29*	**30**	*31*	**32**
m_k	*33*	*34*	**35**	*37*	*38*	*41*	**42**	*45*	**49**
$d_{ORD}(k)$	*4*	*4*	**3**	*3*	*3*	*3*	**2**	*2*	**1**

En resumen, cuando el semigrupo $H(Q)$ es generado por dos elementos, los Teoremas 105 y 108 nos permiten calcular la cota de orden $d_{ORD}(i)$ para todos los códigos Castillo $C_i = C(\mathcal{X}, D, m_i Q)$ para $i = 1, \ldots, n$. En la siguiente sección obtendremos resultados similares en el caso de semigrupos telescópicos.

3.4. Semigrupos telescópicos.

En esta sección supondremos que $H = \langle a_1, a_2, \ldots, a_k \rangle$ es un semigrupo telescópico, ver Subsección 2.2(3). Para $i = 1, \ldots, k$, sea $\delta_i = \text{mcd}(a_1, ..., a_i)$. Nos limitaremos al caso en el que $\delta_{k-1} > 1$, $\delta_k = 1$ y $a_k = \text{máx}(a_1, \ldots, a_k)$. La mayoría de las pruebas en esta sección son similares a las correspondientes en la sección anterior y por tanto se omitirán.

Primero estudiaremos el caso de los códigos no abundantes, es decir $m_i < n$.

Lema 110 *Sea $n - c < m_i \leq n - (\delta_{k-1} - 1)a_k$. Si $n - m_i \in Gaps(H)$, sea s tal que $h_{s-1} < n - m_i < h_s$, entonces $\#\Lambda_i^* \geq h_s$.*

La prueba es similar a la prueba del Lema 104, pero usando [32, Lemma 6.9] en lugar de [30, Lemma 5.27]. Como consecuencia directa de este lema tenemos el siguiente resultado.

Teorema 111 *Si $m_i \leq n-(\delta_{k-1}-1)a_k$ entonces $d_{ORD}(i) = \text{mín}\{h \in H : h \geq n - m_i\}$.*

Ejemplo 112 (Códigos de Suzuki sobre $\mathbb{F}_8$) *Consideremos los códigos de Suzuki sobre $\mathbb{F}_8$ del Ejemplo 95. El semigrupo de Weierstrass de su único punto Q en infinito es $H = \langle 8, 12, 10, 13 \rangle$. Este semigrupo es telescópico de género $g = 14$ y su conductor es $c = 28$. Note que $\delta_3 = 2$ y $a_4 = 13$. Entonces por el Teorema 111, se tiene el valor de la cota de orden para $0 \leq m_i \leq 51$. Estos son:*

k	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
m_k	*0*	*8*	*10*	*12*	*13*	*16*	*18*	*20*	*21*	*22*	*23*	*24*	*25*
$d_{ORD}(k)$	*64*	*56*	*54*	*52*	*51*	*48*	*46*	*44*	*43*	*42*	*41*	*40*	*39*
k	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*
m_k	*26*	*28*	*29*	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
$d_{ORD}(k)$	*38*	*36*	*35*	*34*	*33*	*32*	*31*	*30*	*29*	*28*	*28*	*26*	*25*
k	*27*	*28*	*29*	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	
m_k	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*	*50*	*51*	
$d_{ORD}(k)$	*24*	*23*	*22*	*21*	*20*	*20*	*18*	*18*	*16*	*16*	*16*	*13*	

Entre estos, obtenemos un código $[64, 37, \geq 16]$ *que es un record de acuerdo a las tablas MinT [40].*

Ahora, estudiaremos el caso de los códigos abundantes, es decir cuando $m_i > n$.

Para $t = 0, \ldots, \delta_{k-1} - 1$, consideremos los números $\lambda_t = c - 1 - ta_k$. Todos estos números son lagunas de H y las llamaremos *lagunas especiales* de H.

Lema 113 *Sea H un semigrupo telescópico. Entonces se satisface lo siguiente:*

(a) $\#D(\lambda_t) = t + 1$ *para todo* $t = 0, \ldots, \delta_{k-1} - 1$.

(b) si $m_i = n + l$, *donde* l *es una laguna tal que* $\lambda_s < l < \lambda_{s-1}$, *entonces*

$$\#D(l) \geq \#D(\lambda_s) = s + 1.$$

La prueba es similar a la prueba del Lema 107, de nuevo utilizando [32, Lemma 6.9]. En consecuencia obtenemos el siguiente resultado.

Teorema 114 *Sea* $m_i \geq n + \lambda_{\delta_{k-1}-1}$. *Si* $m_i = n + l_{i-n+g}$ *y* $\lambda_s \leq l_{i-n+g} < \lambda_{s-1}$, *entonces* $d_{ORD}(i) = s + 1$.

Ejemplo 115 (Códigos de Suzuki sobre $\mathbb{F}_8$) *Continuando con el Ejemplo 112. El Teorema 114 nos da la cota de orden d_{ORD} para los valores $m_i \geq 78$. Hemos resaltado los valores de las lagunas especiales.*

k	**60**	*61*	*62*	*63*	**64**
m_k	**78**	*79*	*81*	*83*	**91**
$d_{ORD}(k)$	**2**	*2*	*2*	*2*	**1**

Entre estos códigos encontramos dos records, de acuerdo a las tablas MinT [40]. Es decir, obtenemos códigos con parámetros $[64, 62, \geq 2]$ *y* $[64, 63, \geq 2]$.

Los valores de m_i en el intervalo $n - (\delta_{k-1} - 1)a_k < m_i < n + l_g - (\delta_{k-1} - 1)a_k$ no están cubiertos por los resultados previos en el caso de semigrupos telescópicos en general. En la siguiente sección nos limitaremos al caso de los semigrupos telescópicos procedente de la curva de Suzuki, obteniendo la caracterización de la cota de orden d_{ORD} para todos los códigos de Suzuki.

3.5. Códigos de Suzuki.

En esta sección completaremos el cálculo de la cota de orden, $d_{ORD}(i)$, de los códigos de Suzuki no cubiertos en la sección anterior, es decir para los valores m_i con

$$n - l_g + \delta_3 + (\delta_3 - 1)a_2 < m_i < n + \delta_3 + (\delta_3 - 1)a_2.$$

Sea $q = 2q_0^2$, donde $q_0 \geq 2$ es una potencia de 2. La curva de Suzuki $\mathcal{S}$ es definida sobre $\mathbb{F}_q$ por la ecuación afín $y^q - y = x^{q_0}(x^q - x)$. Esta curva tiene género $g = q_0(q-1)$ y q^2 puntos racionales afines, más un punto Q en infinito, ver Ejemplo 84. El semigrupo de Weierstrass $H = H(Q)$, es generado por la secuencia telescópica $a_1 = q$, $a_2 = q + 2q_0$, $a_3 = q + q_0$, $a_4 = q + 2q_0 + 1$. Entonces $\delta_3 = q_0$. Además, se tienen los siguientes hechos, ver la Subsección 2.2.

1. $c - 1 = \delta_3 + (\delta_3 - 1)(a_2 + a_4)$.

2. Si $h \in H$ entonces existen enteros no negativos $x_1 \geq 0$, $0 \leq x_2 < \delta_3$, $0 \leq x_3 < 2$ y $0 \leq x_4 < \delta_3$ tal que h tiene representación *normal* $h = x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4$.

En este intervalo se distinguen dos tipos de desiertos de H: aquellos de longitud menor que $\delta_3 = q_0$ son llamados *cortos*, mientras que los demás son llamados *largos*. Note que hay $\delta_3 - 1$ desiertos largos, $L^{(t)} = [(t-1)a_4 + 1, ta_1 - 1]$, $t = 1, ..., \delta_3 - 1$. El conjunto de lagunas pertenecientes a un desierto largo (resp. corto) es denotado por $\text{Gaps}_l(H)$ (resp. $\text{Gaps}_c(H)$). Por tanto, $\text{Gaps}_l(H) = \cup_{t=1,...,\delta_3-1} L^{(t)}$.

Ejemplo 116 (Código de Suzuki sobre $\mathbb{F}_{32}$) *Consideremos la curva de Suzuki* $\mathcal{S}$ *dada por la ecuación afín* $y^{32} - y = x^{36} - x^5$ *sobre* $\mathbb{F}_{32}$. *El semigrupo de Weierstrass en el único punto* Q *en infinito es* $H = H(Q) = \langle 32, 36, 40, 41 \rangle$. *En la siguiente tabla se listan las lagunas de* H *en la primera fila y los respectivos valores de* $\#D(l)$ *en la segunda fila. Hemos separado los desiertos de* H *para identificar los desiertos cortos y largos.*

También resaltamos las lagunas super especiales que definiremos más adelante. Note que precisamente para estas lagunas los valores de $\#D(l)$ son minimales con respecto a sus lagunas antecesoras, esta observación nos permitirá probar el resultado crucial de esta sección, ver Lema 120.

1	*2*	*3*	**4**	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
31	*44*	*39*	**16**	*27*	*42*	*41*	*24*	*24*	*40*	*43*	*32*	*33*	*34*
15	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*
39	*32*	*36*	*32*	*35*	*35*	*39*	*36*	*25*	*24*	*36*	*36*	*24*	*16*
29	*30*	*31*	*33*	*34*	*35*	**37**	*38*	*39*	*42*	*43*	**44**	**45**	*46*
33	*36*	*25*	*24*	*32*	*24*	**15**	*28*	*23*	*22*	*26*	**12**	**12**	*18*
47	*48*	*49*	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*	*60*
25	*16*	*18*	*16*	*24*	*20*	*24*	*22*	*17*	*16*	*24*	*24*	*16*	*12*
61	*62*	*63*	*65*	*66*	*67*	*69*	*70*	*71*	*74*	*75*	**78**	*79*	*83*
24	*26*	*18*	*18*	*24*	*18*	*12*	*22*	*18*	*16*	*16*	**10**	*14*	*13*
84	*85*	**86**	*87*	*88*	*89*	*90*	*91*	*92*	*93*	*94*	*95*	*97*	*98*
8	*9*	**8**	*9*	*8*	*12*	*12*	*8*	*8*	*15*	*16*	*11*	*12*	*16*

99	*101*	*102*	*103*	*106*	*107*	*110*	*111*	*115*	**119**		*124*		
12	*9*	*16*	*13*	*12*	*12*	*8*	*11*	*8*	**5**		*4*		
125	*126*	*127*	*129*	*130*	*131*	*133*	*134*	*135*	*138*	*139*			
6	*6*	*4*	*6*	*8*	*6*	*6*	*10*	*8*	*8*	*8*			
142	*143*	*147*	*151*	*165*	*166*	*167*	*170*	*171*	*174*	*175*			
6	*8*	*6*	*4*	*3*	*4*	*3*	*4*	*4*	*4*	*5*			
179	*183*	*206*	*207*	*211*	*215*	*247*							
4	*3*	*2*	*2*	*2*	*2*	*1*							

Recuerde que los valores mayores que 119 se tienen resueltos por los resultados de la sección anterior. Las lagunas $\lambda_0 = 247, \lambda_1 = 206, \lambda_2 = 165, \lambda_3 = 124$ son las lagunas especiales definidas antes del Lema 113. Note que también para estas lagunas el valor del cardinal de $D(\lambda_t)$ es minimal con respecto a sus lagunas anteriores.

Comencemos por estudiar el caso $n - m_i \in \mathrm{Gaps}_c(H)$.

Lema 117 *Si $l \in Gaps(H)$ con $l < \delta_3 + (\delta_3 - 1)a_2$ entonces $\#D(l) \geq \delta_3$.*

Demostración. $(l_k, m_j) \in D(l)$ si y sólo si $m_j + c - 1 - l_k = c - 1 - l$. ahora, como $(\delta_3 - 1)a_4 < c - 1 - l = m$, entonces $m \in H$. Sea $m = \sum_{i=1}^{4} x_i a_i$ la representación normal de m. Entonces $\#D(l) \geq \prod_{i=1}^{4}(x_i + 1) > \sum_{i=1}^{4} x_i \geq \delta_3 - 1$. ■

Lema 118 *Si $n - m_i = l \in Gaps_c(H)$, sea s tal que $h_{s-1} < l < h_s$. Entonces*

$$\#\Lambda_i^* \geq h_s.$$

Demostración. Note que $h_s - l < \delta_3$. Entonces por la Proposición 92 y el Lema 117 se deduce el resultado. ■

Como consecuencia directa obtenemos el siguiente resultado. Este muestra que las lagunas de los desiertos cortos satisfacen la igualdad en el Corolario 94.

Teorema 119 *Si $n - m_i \in Gaps_c(H)$, entonces*

$$d_{ORD}(i) = \text{mín}\{h \in H : h \geq n - m_i\}.$$

Vamos a estudiar ahora el caso en el que $n - m_i \in \text{Gaps}_l(H)$. Para $0 < t < \delta_3 - 1$, consideremos los números

$$\lambda_2^+(t) = ta_2 + \delta_3, \quad \lambda_4^+(t) = ta_4 + \delta_3 \quad \text{y} \quad \lambda_4^-(t) = ta_4 - \delta_3.$$

Además, sean $\lambda_2^+(0) = \lambda_4^+(0) = \delta_3$ y $\lambda_4^-(0) = 0$. Note que todos estos números, excepto $\lambda_4^-(0) = 0$, son lagunas de H y las llamaremos lagunas *super especiales* de H. Más aún, note que $\lambda_2^+(t), \lambda_4^+(t)$ pertenecen a desiertos largos y para todo t se tiene que

$$\lambda_4^-(t) < \lambda_2^+(t) \leq \lambda_4^+(t) < \lambda_4^-(t+1).$$

En el siguiente resultado calculamos el cardinal de los conjuntos $D(w)$ cuando w es una laguna super especial de H y mostramos que en estas lagunas se alcanza el mínimo.

Lema 120 *Sea l, t dos enteros tales que l es una laguna de H y $0 \leq t < \delta_3 - 1$. Entonces se tienen las siguientes afirmaciones.*

(a) $\#D(\lambda_2^+(t)) = \#D(\lambda_4^+(t)) = \delta_3(\delta_3 - t)$.

(b) Si $t \neq 0$, entonces $\#D(\lambda_4^-(t)) = (\delta_3 + 1)(\delta_3 - t)$.

(c) Si $\lambda_4^-(t) < l < \lambda_2^+(t)$, entonces $\#D(l) \geq (\delta_3 + 1)(\delta_3 - t)$

(d) Si $\lambda_2^+(t) < l < \lambda_4^+(t)$, entonces $\#D(l) \geq \delta_3(\delta_3 - t) + \lambda_4^+(t) - l$.

(e) Si $\lambda_4^+(t) < l < \lambda_4^-(t+1)$, entonces $\#D(l) \geq \delta_3(\delta_3 - t)$.

(f) Si $\lambda_4^+(t) < l < (t+1)a_1$, entonces $\#D(l) \geq (t+1)a_1 - l$.

Demostración. (a) Para $i = 2, 4$ note que $(l, m) \in D(\lambda_i^+(t))$ si y sólo si $m+c-1-l = c-1-\lambda_i^+(t)$. Como $c-1-\lambda_2^+(t) = (\delta_3-1-t)a_2+(\delta_3-1)a_4$ y $c-1-\lambda_4^+(t) = (\delta_3-1)a_2+(\delta_3-1-t)a_4$, un cálculo directo, utilizando la unicidad de la representación normal, prueba la afirmación.
(b) Similar al anterior. Note que $c-1-\lambda_4^-(t) = \delta_3 a_1+(\delta_3-1-t)a_4$.
(c) $(l_k, m_j) \in D(l)$ si y sólo si $m_j+c-1-l_k = c-1-l$. Las lagunas en este intervalo son de la forma $l = \lambda_4^-(t)+w$ y $l = \lambda_2^+(t)-w$ con $0 < w < \delta_3-t$. Así $c-1-l = \delta_3 a_1+(\delta_3-t-1)a_4-w = \delta_3 a_1+wa_2+(\delta_3-t-1-w)a_4$ y $c-1-l = (\delta_3-t-1)a_2+(\delta_3-1)a_4+w = (\delta_3-t-1-w)a_2+\delta_3 a_1+a_3+(w-1)a_4$ respectivamente. Entonces $\#D(l) \geq (\delta_3+1)(\delta_3-t-w)(w+1) \geq (\delta_3+1)(\delta_3-t)$ y $\#D(l) \geq (\delta_3+1)(\delta_3-t-w)2w \geq (\delta_3+1)(\delta_3-t)$ respectivamente.
(d) Sea $l = \lambda_4^+(t)-\alpha$ con $0 < \alpha < t$. $(l_k, m_j) \in D(l)$ si y sólo si $m_j+c-1-l_k = c-1-l$. Como $c-1-l = (\delta_3-1-\alpha)a_2+(\delta_3-1-t+\alpha)a_4$, obtenemos $\#D(l) \geq (\delta_3-\alpha)(\delta_3-t+\alpha) = \delta_3(\delta_3-t)+\alpha(t-\alpha)$.
(e) Consideremos dos casos. Si $\lambda_4^+(t) < l < (t+1)a_1$ entonces $(l_k, m_j) \in D(l)$ si y sólo si $m_j+c-1-l_k = c-1-l$. Sea $l(w) = (t+1)a_1-w\delta_3$ con $0 < w \leq 2(\delta_3-t)-1$. Para w par, $c-1-l(w) = (\delta_3-t-1-w/2)a_1+a_3+(w/2-1)a_2+(\delta_3-1)a_4$, luego $\#D(l(w)) \geq \delta_3(\delta_3-t)+\delta_3(w(\delta_3-t-w/2)-(\delta_3-t))$. Para w impar, $c-1-l(w) = (\delta_3-t-1-(w-1)/2)a_1+(w-1)/2a_2+(\delta_3-1)a_4$, luego $\#D(l(w)) \geq \delta_3(\delta_3-t)+\delta_3(w-1)/2(\delta_3-t-1-(w-1)/2)$. Ahora, si $l = l(w)+\alpha$ con $0 < \alpha < \delta_3$, un razonamiento similar al del numeral (d) de este lema demuestra que $\#D(l) > \#D(l(w))+\alpha$. El segundo caso a considerar es $(t+1)a_1 < l < \lambda_4^-(t+1)$. Podemos restringirnos a $(t+1)a_1 < l < a_3+ta_2$, ya que los otros enteros en el intervalo anterior no son lagunas. Entonces $(l_k, m_j) \in D(l)$ si y sólo si $m_j+c-1-l_k = c-1-l$. Sea $l(\alpha) = a_3+ta_2-\alpha$ con $0 < \alpha < \delta_3-t$. Por tanto $c-1-l(\alpha) = (\delta_3-1)a_1+a_3+(\delta_3-1-t-\alpha)a_2+(\alpha-1)a_4$ y $\#D(l(\alpha)) \geq \delta_3(\delta_3-t)+\delta_3\alpha(\delta_3-t-1-\alpha)$. Ahora consideremos los números $a_3+ta_2-2i\delta_3 \pm \alpha$ con $0 < i \leq t$ y $0 < \alpha < \delta_3$. Las lagunas en nuestro intervalo son de la forma $l(\alpha) = ia_1+a_3+(t-i)a_2-\alpha$ y $l(\alpha) = ia_1+a_3+(t-i)a_4+\alpha$, con $0 < \alpha < \delta_3-t+i$. Entonces $c-1-l(\alpha) = (\delta_3-i-1)a_1+a_3+(\delta_3-1-t+i-\alpha)a_2+(\alpha-1)a_4$ y $c-1-l(\alpha) = (\delta_3-i)a_1+(\alpha-1)a_2+(\delta_3-1-t+i-\alpha)a_4$, respectivamente. En ambos casos obtenemos $\#D(l) \geq \delta_3(\delta_3-t)$.
(f) Es consecuencia de la primera parte del numeral anterior. ■

El Lema 120 nos permitirá calcular la cota de orden $d_{ORD}(i)$ para todos los códigos de Suzuki $C_i = C(m_i)$, con m_i en el intervalo $n-(\delta_3-1)a_4 < m_i < n+\delta_3+(\delta_3-1)a_2$, como lo demuestran los siguientes teoremas.

Teorema 121 *Sea $m_i < n$ tal que $n - m_i \in Gaps_l(H)$. Para $0 \leq t < (\delta_3 - 1)$ se tiene lo siguiente.*

(1) Si $ta_4 < n - m_i \leq \lambda_2^+(t)$, entonces $d_{ORD}(i) = \lambda_2^+(t) + \delta_3(\delta_3 - t)$.

(2) Si $\lambda_2^+(t) < n - m_i \leq \lambda_4^+(t)$, entonces $d_{ORD}(i) = \lambda_4^+(t) + \delta_3(\delta_3 - t)$.

(3) Si $\lambda_4^+(t) < n - m_i < (t+1)a_1$, entonces

$$d_{ORD}(i) = (t+1)a_1 = \text{mín}\{h \in H : h \geq n - m_i\}.$$

Demostración. (1) Escribamos $n - m_i = \lambda_2^+(t) - w$ con $0 \leq w < \delta_3 - t$. La Proposición 92 y el Lema 120(c), implican que $\#\Lambda_i^* \geq \lambda_2^+(t) - w + (\delta_3+1)(\delta_3 - t) \geq \lambda_2^+(t) + \delta_3(\delta_3 - t)$. (2) Escribamos $n - m_i = \lambda_4^+(t) - w$ con $0 \leq w < t$. La Proposición 92 y el Lema 120(d), implican que $\#\Lambda_i^* = n - m_i + \#D(l) \geq \lambda_4^+(t) - w + \delta_3(\delta_3 - t) + w \geq \lambda_4^+(t) + \delta_3(\delta_3 - t)$. (3) Se sigue inmediatamente de la Proposición 92 y el Lema 120(f). ■

Ejemplo 122 (Códigos de Suzuki sobre $\mathbb{F}_8$) *Utilizando el Teorema 121 podemos calcular la cota de orden para los valores pendientes del Ejemplo 112, en el caso de los códigos de Suzuki no abundantes. Hemos resaltado las lagunas super especiales.*

k	*39*	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	**49**	*50*
m_k	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*	*60*	*61*	**62**	*63*
$d_{ORD}(k)$	*12*	*12*	*10*	*10*	*8*	*8*	*8*	*8*	*8*	*8*	**6**	*6*

De acuerdo a los Teoremas 119 y 121, para toda laguna en un desierto corto y casi todas las lagunas en los desiertos largos se tiene la igualdad en el Corolario 94. Finalmente, el siguiente resultado completa el cálculo de la cota de orden d_{ORD} para los faltantes códigos de Suzuki abundantes.

Teorema 123 *Sea $m_i > n$, es decir $m_i = n + l_{i-n+g}$.*

(1) Si $\lambda_4^-(t) \leq l_{i-n+g} < \lambda_2^+(t)$ para $0 \leq t \leq \delta_3 - 2$, entonces $d_{ORD}(i) = (\delta_3+1)(\delta_3 - t)$.

(2) Si $\lambda_2^+(t) \leq l_{i-n+g} < \lambda_4^-(t+1)$ entonces $d_{ORD}(i) = \delta_3(\delta_3 - t)$.

(3) Si $l_{i-n+g} = \lambda_4^-(\delta_3 - 1)$ entonces $d_{ORD}(i) = (\delta_3 + 1)$.

Demostración. Las afirmaciones (1) y (2) se siguen directamente de la Proposición 92 y el Lema 120, numerales (c), (d) y (e). (3) Ya que $c - 1 - \lambda_4^-(\delta_3 - 1) = \delta_3 a_1$, se tiene que $\Lambda_i^* = \delta_3 + 1$. Entonces la afirmación se sigue del numeral (2) de este teorema con $t = \delta_3 - 2$. ■

Ejemplo 124 (Códigos de Suzuki sobre $\mathbb{F}_8$) *Utilizando el Teorema 123 podemos calcular la cota de orden para los valores pendientes del Ejemplo 115 para los códigos de Suzuki abundantes. Hemos resaltado las lagunas super especiales.*

k	*51*	**52**	*53*	*54*	*55*	*56*	*57*	*58*	**59**
m_k	*65*	**66**	*67*	*68*	*69*	*70*	*71*	*73*	**75**
$d_{ORD}(k)$	*6*	**4**	*4*	*4*	*4*	*4*	*4*	*4*	**3**

De estos se tiene un código $[64, 58, \geq 4]$ *que es un record según las tablas MinT [40].*

Ejemplo 125 (Códigos de Suzuki sobre $\mathbb{F}_{32}$) *En este ejemplo calculamos la cota de orden de todos los códigos de Suzuki sobre* $\mathbb{F}_{32}$*, ver Ejemplo 116. La longitud de estos códigos es* $n = 1024$*. En la tabla siguiente presentamos la dimensión* k *y la cota de orden* $d_{ORD}(k)$ *para la distancia mínima de los códigos Suzuki que mejoran la cota de Goppa. Para los demás valores de* k *se tiene que* $d_{ORD}(k) = 1025 - g(k) - k$*, donde* $g(k)$ *es el número de lagunas menores que* m_k*.*

k	$d_{ORD}(k)$	k	$d_{ORD}(k)$	k	$d_{ORD}(k)$
654	*248*	*782*	*120*	*862-864*	*40*
686	*216*	*786*	*116*	*866-868*	*36*
690	*212*	*790-791*	*112*	*870-896*	*32*
694-695	*208*	*794-795*	*108*	*897-903*	*20*
718	*184*	*798-800*	*104*	*904-934*	*16*
722	*180*	*802-804*	*100*	*935-939*	*15*
726-727	*176*	*806-814*	*96*	*940-967*	*12*
730-731	*172*	*815-816*	*94*	*968-970*	*10*
734-736	*168*	*817-818*	*92*	*971-993*	*8*
750	*152*	*822-823*	*80*	*994*	*5*
754	*148*	*826-827*	*76*	*995-1010*	*4*
758-759	*144*	*830-832*	*72*	*1011-1019*	*3*
762-763	*140*	*834-836*	*68*	*1020-1023*	*2*
766-768	*136*	*838-855*	*64*	*1024*	*1*
770-772	*130*	*856*	*57*		
774-777	*128*	*857-859*	*56*		

Capítulo 4

Jerarquía de pesos de códigos Castillo

Este capítulo trata sobre los pesos de Hamming generalizados de códigos Castillo. Se pueden distinguir dos partes. En la primera parte (Sección 4.1) caracterizamos la cota de orden solo para el segundo peso de Hamming de códigos Castillo. Utilizando algunos resultados del capítulo anterior, determinamos parcialmente esta cota en el caso de códigos con semigrupo de Weierstrass generado por dos elementos (Subsección 4.1.1). Cuando el semigrupo es generado por dos elementos consecutivos la cota es calculada completamente (Subsección 4.1.2). En particular, para códigos Hermitianos esta cota coincide con el verdadero valor del segundo peso de Hamming. Ésta caracterización es más simple que las conocidas (ver Ejemplo 148). Estos resultados fueron publicados en [52]. En la segunda parte de este capítulo (Sección 4.2) introducimos nuevos conceptos para estudiar los pesos de Hamming generalizados de los códigos Castillo en general. Obtenemos un intervalo en el que los códigos Castillo son r-ésimos MDS. Utilizando este resultado proponemos una nueva cota inferior d_w para la distancia mínima de códigos castillo (Subsección 4.2.2). En los ejemplos trabajados, esta cota es tan buena como la cota de orden, si bien no hemos podido encontrar relación entre ellas. Finalmente, en la Subsección 4.2.3, mostramos que el primer entero $w_i + 1$ para el cuál los códigos Hermitianos son $(w_i + 1)$-ésimo MDS, coincide con el verdadero valor del *toque* de los códigos Hermitianos (este es el primer elemento que satisface la igualdad en la cota singleton generalizada). Por tanto, obtenemos por primera vez el rango MDS de todos los códigos Hermitianos. Estos resultados se recogen en [54].

4.1. Cota de orden para el segundo peso de Hamming.

En esta sección caracterizamos la cota de orden para el segundo peso de Hamming de códigos Castillo.

Sea $\mathcal{X}$ una curva Castillo con respecto al punto racional Q, de género g sobre $\mathbb{F}_q$. Sean $H = \{h_1 = 0, h_2, \dots\}$ el semigrupo de Weierstrass de Q, $\text{Gaps}(H) = \{l_1, \dots, l_g\}$ el conjunto de lagunas de H y $M = \{m_1, \dots, m_n\}$ el conjunto de dimensiones.

De acuerdo al Teorema 78, la cota de orden para el segundo peso de Hamming de los códigos Castillo $C_i = C(\mathcal{X}, D, m_i Q)$, para $i = 1, \dots, n$, es:

$$d_2^*(i) = \min_{1 \le j_1 < j_2 \le i} \#\Lambda^*_{j_1,j_2},$$

donde $\Lambda^*_{j_1,j_2} = \Lambda^*_{j_1} \cup \Lambda^*_{j_2}$.

Para $1 \le j_1 < j_2 \le i$ definimos el conjunto

$$M_{j_1,j_2} = \{(l,m) \in D(m_{j_2} - m_{j_1}) : m - (n - m_{j_2}) \in H\},$$

donde $D(w) = \{(l,m) : l \in \text{Gaps}(H), m \in M, l - m = w\}$, como en el capítulo anterior.

Por el Lema 91, se tiene que $M_{j_1,j_2} = \varnothing$, si $m_{j_2} - m_{j_1} \in H$. El siguiente resultado establece algunas propiedades del cardinal de M_{j_1,j_2}.

Lema 126 *Los conjuntos M_{j_1,j_2} verifican las siguientes propiedades.*

(1) Si $m_{j_1} < n$, entonces $0 \le \#M_{j_1,j_2} \le \#D(n - m_{j_1})$.

(2) Si $n - m_{j_1} \in H$, entonces $\#M_{j_1,j_2} = 0$.

(3) Si $n - m_{j_1} \in Gaps(H)$ y $n - m_{j_2} \in H$, entonces $\#M_{j_1,j_2} = \#D(n - m_{j_1})$.

Demostración. (1) Sea $(l,m) \in M_{j_1,j_2}$. Así, $l - m = m_{j_2} - m_{j_1}$ y $m - (n - m_{j_2}) \in H$. Por tanto, $(l, m - (n - m_{j_2})) \in D(n - m_{j_1})$. (2) Si $(l,m) \in M_{j_1,j_2}$, entonces $l - m = m_{j_2} - m_{j_1}$ y $m = (n - m_{j_2}) + \rho$ para algún $\rho \in H$ es decir $l = (n - m_{j_1}) + \rho$. Si $n - m_{j_1} \in H$ esta ecuación no tiene solución. (3) Sea $(l,m) \in D(n - m_{j_1})$. Entonces $l - m = n - m_{j_1} = (m_{j_2} - m_{j_1}) + (n - m_{j_2})$. Por tanto, $(l, m + (n - m_{j_2})) \in M_{j_1,j_2}$. ■

El conjunto M_{j_1,j_2} puede usarse para calcular el cardinal de $\Lambda^*_{j_1,j_2}$, como lo muestra el siguiente resultado.

Teorema 127 *Para $1 \le j_1 < j_2 \le i$ se tiene que*

$$\#\Lambda^*_{j_1,j_2} = \#\Lambda^*_{j_1} + \#D(m_{j_2} - m_{j_1}) - \#M_{j_1,j_2}.$$

Demostración. Note que $\Lambda^*_{j_1,j_2} = \Lambda^*_{j_1} \cup (((m_{j_2}+H) \setminus (m_{j_1}+H)) \cap M)$. Además, $\#((m_{j_2}+H) \setminus (m_{j_1}+H)) = \#D(m_{j_2}-m_{j_1})$ ya que $m_{j_2}+m = m_{j_1}+l$ si y sólo si $(l,m) \in D(m_{j_2}-m_{j_1})$. Luego, si $m-(n-m_{j_2}) = \rho \in H$, entonces $m_{j_2}+m \notin M$ pues $m_{j_2}+m = n+\rho$. Por tanto, $\#\left(((m_{j_2}+H) \setminus (m_{j_1}+H)) \cap M\right) = \#D(m_{j_2}-m_{j_1}) - \#M_{j_1,j_2}$. ■

Corolario 128 *Para $1 \leq j_1 < j_2 \leq i$ se tiene que $\#\Lambda^*_{j_1,j_2} \geq \#\Lambda^*_{j_1}$.*
Si $m_{j_2}-m_{j_1} \in H$ entonces se da la igualdad.
Demostración. El resultado se sigue del Teorema 127. La segunda afirmación se deduce del hecho que $\#D(m_{j_2}-m_{j_1}) = 0$ cuando $m_{j_2}-m_{j_1} \in H$. ■

Corolario 129 *Para $1 \leq j_1 < j_2 \leq i$, se tiene que $\#\Lambda^*_{j_1,j_2} \geq n-m_{j_1}+\#D(m_{j_2}-m_{j_1})$.*
Si $n-m_{j_1} \in H$ o si $n-m_{j_1} \in Gaps(H)$ y $n-m_{j_2} \in H$ entonces se da la igualdad.
Demostración. El resultado se sigue del Teorema 127, el Lema 126(1) y el hecho que $\#\Lambda^*_{j_1} = n-m_{j_1}+\#D(n-m_{j_1})$. ■

Utilizando el Teorema 127 y algunos resultados del capítulo anterior, en la siguiente sección determinamos explícitamente la cota de orden para el segundo peso de Hamming de códigos Castillo con semigrupo de Weierstrass generado por dos elementos.

4.1.1. Semigrupos generados por dos elementos cualesquiera.

En esta sección asumiremos que H es el semigrupo generado por dos elementos, $H = \langle a,b \rangle$ con $a < b$ y $\mathrm{mcd}(a,b) = 1$.

Sea $m \in H$, $m < n$. Diremos de m que es un polo de *tipo I*, si $m = \beta b$ para $\beta = 1, \ldots, a-1$. En otro caso diremos de m que es un polo de *tipo II*.

Recuerde que cuando $b = a+1$ entonces existen $a-1$ desiertos que denotamos por $L_1, \ldots, L_{a-1}$, ver la Subsección 2.2. Para cada desierto L_t, denotamos su elemento inicial y final por $l_{t_0} = (t-1)a+t$ y $l_{t_f} = ta-1$ respectivamente.

Comenzaremos estudiando los códigos Castillo no abundantes $C_i = C(m_i)$ para $i \leq n-g$, es decir cuando $0 < m_i < n$.

Teorema 130 *Si m_i es un polo de tipo II y $n-m_i+a \in H$, entonces $d^*_2(i) = n-m_i+a$.*
Demostración. Sea $m_t = m_i - a$. Por el Corolario 128, $\#\Lambda^*_{t,i} = \#\Lambda^*_t = n-m_i+a$. Luego $d^*_2(i) \leq n-m_i+a$. Para tener la igualdad debemos demostrar que $\#\Lambda^*_{j_1,j_2} \geq n-m_i+a$ para todo j_1, j_2 con $1 \leq j_1 < j_2 \leq i$. Ya que $\#\Lambda^*_{j_1,j_2} \geq \#\Lambda^*_{j_1} \geq \#\Lambda^*_t$ si $j_1 \leq t$. Podemos asumir que $j_1 > t$. Así $\#D(m_{j_2}-m_{j_1}) \geq a-1$ pues $0 < m_{j_2}-m_{j_1} < a < 2b-a$. Por el Corolario 129, $\#\Lambda^*_{j_1,j_2} \geq n-m_{j_1}+\#D(m_{j_2}-m_{j_1}) \geq n-m_{j_1}+a-1 \geq n-m_i+a$. ■

Corolario 131 *Si m_i es un polo de tipo II y $n - m_i \in H$, entonces $d_2^*(i) = n - m_i + a$.*

Corolario 132 *Sea $b = a + 1$. Si m_i es un polo de tipo II y $n - m_i = l_{t_0}$, entonces $d_2^*(i) = n - m_i + a$.*
Demostración. $n - m_i + a = ta + t \in H$. ■

Ejemplo 133 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Del Ejemplo 43 se conoce que la curva Norma-Traza $\mathcal{X}$ sobre $\mathbb{F}_8$, dada por la ecuación afín $x^7 = y^4 + y^2 + y$, tiene género $g = 9$ y 33 puntos racionales sobre $\mathbb{F}_8$. El semigrupo de Weierstrass del único polo Q de x es $H = H(Q) = \langle 4, 7\rangle = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, \rightarrow\}$. Por tanto, el conjunto de dimensiones es $M = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18 - 31, 33, 34, 35, 37, 38, 41, 42, 45, 49\}$. Luego 4,8,11,12,15,16,18,19,20,22,23,24,25,26,27,28,29,30,31 son los polos de tipo II. En la tabla siguiente se resumen los valores de la cota de orden $d_2^*(i)$ para el segundo peso de Hamming de los códigos unipuntuales $C_i = C(\mathcal{X}, D, m_iQ)$ cuando m_i es un polo de tipo II que satisface la hipótesis del Teorema 130.*

i	2	4	5	6	8	9	10	12	14	16	17	20	21
m_i	4	8	11	12	15	16	18	20	22	24	25	28	29
$d_2^*(i)$	32	28	25	24	21	20	18	16	14	12	11	8	7

Note que los seis polos $m_{11} = 19$, $m_{15} = 23$, $m_{18} = 26$, $m_{19} = 27$, $m_{22} = 30$ y $m_{23} = 31$ no satisfacen las condiciones del Teorema 130. Por tanto, son candidatos para mejorar la cota de gonalidad para el segundo peso de Hamming como veremos.

De acuerdo al Teorema 130, cuando m_i es un polo de tipo II y $n - m_i + a \in H$, entonces la cota de orden $d_2^*(i)$ es igual a la cota gonalidad para C_i (ver Corolario 33), ya que por la Proposición 49(2), $\gamma_2 = a$. En el siguiente teorema demostraremos que cuando $b \neq a + 1$, m_i es un polo de tipo II y $n - m_i + a \in Gaps(H)$, entonces la cota $d_2^*(i)$ es mejor que la cota gonalidad.

Teorema 134 *Sea $b \neq a + 1$. Si m_i es un polo de tipo II y $n - m_i + a \in Gaps(H)$, entonces $d_2^*(i) > n - m_i + a$.*
Demostración. Sea $m_t = m_i - a$ y $m_s = m_i - (b - a)$. Por el Corolario 129, $\#\Lambda_{s,i}^* \geq n - m_s + \#D(m_i - m_s) = n - m_s + a - 1 = n - m_i + b - 1 > n - m_i + a$. Como $n - m_t \in Gaps(H)$, por el Corolario 128, $\#\Lambda_{t,i}^* = \#\Lambda_t^* > n - m_t = n - m_i + a$. Ahora, sea j_1, j_2 tal que $1 \leq j_1 < j_2 \leq i$. Si $j_1 > s$, entonces $m_{j_2} - m_{j_1} < b - a$ así $\#D(m_{j_2} - m_{j_1}) \geq a$ y por el Corolario 129, $\#\Lambda_{j_1,j_2}^* \geq n - m_{j_1} + \#D(m_{j_2} - m_{j_1}) \geq n - m_{j_1} + a > n - m_i + a$. Si $j_1 < t$, por el Corolario 128, $\#\Lambda_{j_1,j_2}^* \geq \#\Lambda_{j_1}^* \geq n - m_{j_1} > n - m_t = n - m_i + a$. Finalmente, si $b < 2a$ y $t \leq j_1 \leq s$, podemos suponer que $m_{j_2} - m_{j_1} < a < 2b - a$. Así

$\#D(m_{j_2} - m_{j_1}) \geq a-1$ y por el Corolario 129, $\#\Lambda^*_{j_1,j_2} \geq n - m_{j_1} + \#D(m_{j_2} - m_{j_1}) \geq n - m_{j_1} + a - 1 > n - m_i + a$. ■

Corolario 135 *Sea $b = a+1$. Si m_i es un polo de tipo II, $n - m_i + a \in Gaps(H)$ y $n - m_i + (b-a) \in H$, entonces $d^*_2(i) = n - m_i + a$.*
Demostración. En la prueba del Teorema 134, como $n - m_s = n - m_i + (b-a) \in H$, por el Corolario 129, $\#\Lambda^*_{s,i} = n - m_s + \#D(m_i - m_s) = n - m_s + a - 1 = n - m_i + b - 1 = n - m_i + a$. ■

Observación 136 *Note que la condición del Corolario 135 se satisface únicamente cuando $n - m_i = l_{t_f} \in Gaps(H)$. En este caso, $d^*_2(i) = (t+1)a - 1$, ya que $n - m_i + a = (t+1)a - 1 \in Gaps(H)$ y $n - m_i + 1 = ta \in H$.*

Corolario 137 *Sea $b \neq a+1$. Si m_i es un polo de tipo II, $n - m_i + a \in Gaps(H)$ y $n - m_i + (b-a) \in H$, entonces $n - m_i + a < d^*_2(i) \leq n - m_i + b - 1$.*
Demostración. En la prueba del Teorema 134 note que $n - m_s = n - m_i + (b-a) \in H$. Entonces, por el Corolario 129, $\#\Lambda^*_{s,i} = n - m_s + \#D(m_i - m_s) = n - m_s + a - 1 = n - m_i + b - 1$ ■

Ejemplo 138 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Consideremos los polos de tipo II no cubiertos en el Ejemplo 133. Por el Corolario 137, la cota de orden $d^*_2(i)$ para el segundo peso de Hamming de C_i, donde m_i es uno de estos polos, es $d^*_2(i) = n - m_i + 5$ o $d^*_2(i) = n - m_i + 6$. Un Calculo directo demuestra que para $i = 11, 15, 18, 22$ se satisface la primera igualdad y para $i = 19, 23$ se satisface la segunda igualdad. Es decir, $d^*_2(11) = 18$, $d^*_2(15) = 14$, $d^*_2(18) = d^*_2(19) = 11$ y $d^*_2(22) = d^*_2(23) = 7$. Note que para todos estos seis valores se tiene una mejora sobre la cota gonalidad.*

Ahora estudiaremos el caso cuando m_i es un polo de tipo I. Demostraremos que cuando $b \neq a+1$, para todos estos polos, se tiene una mejora sobre la cota gonalidad.

Teorema 139 *Sea $b \neq a+1$. Si m_i es un polo de tipo I, entonces*

$$d^*_2(i) > n - m_i + a.$$

Demostración. Sean $m_t = m_i - (b-a)$ y $m_s = m_i - b$. Por el Corolario 129, $\#\Lambda^*_{t,i} \geq n - m_t + \#D(m_i - m_t) = n - m_t + a - 1 = n - m_i + b - 1$. Si $j_1 \leq s$ entonces, por el Corolario 128, $\#\Lambda^*_{j_1,j_2} \geq \#\Lambda^*_{j_1} \geq n - m_{j_1} \geq n - m_s = n - m_i + b$. Si $s < j_1 < t$, entonces $0 < m_{j_2} - m_{j_1} < b < 2b - a$ y $\#D(m_{j_2} - m_{j_1}) \geq a - 1$. Así, por el Corolario 129, $\#\Lambda^*_{j_1,j_2} \geq n - m_{j_1} + \#D(m_{j_2} - m_{j_1}) \geq n - m_{j_1} + a - 1 \geq n - m_t + a = n - m_i + b$.

Si $t < j_1 < j_2 \leq i$, entonces $0 < m_{j_2} - m_{j_1} < b - a$ y $\#D(m_{j_2} - m_{j_1}) \geq a$. Así, por el Corolario 129, $\#\Lambda^*_{j_1,j_2} \geq n - m_{j_1} + \#D(m_{j_2} - m_{j_1}) \geq n - m_{j_1} + a > n - m_i + a$. ■

Corolario 140 *Sea $b \neq a + 1$. Si m_i es un polo de tipo I y $n - m_i + (b - a) \in H$, entonces $n - m_i + a < d^*_2(i) \leq n - m_i + b - 1$.*
Demostración. En la prueba del Teorema 139, $n - m_t = n - m_i + (b - a) \in H$. Por tanto, $\#\Lambda^*_{t,i} = n - m_i + b - 1$. ■

Ejemplo 141 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Del Ejemplo 133 se tiene que hay tres polos de tipo I, estos son: $m_3 = 7$, $m_7 = 14$ y $m_{13} = 21$. Por el Corolario 140, la cota de orden para el segundo peso de Hamming de C_i, donde m_i es uno de estos polos, es $d^*_2(i) = n - m_i + 5$ o $d^*_2(i) = n - m_i + 6$. Un cálculo directo muestra que $d^*_2(3) = 31$, $d^*_2(7) = 24$ y $d^*_2(13) = 16$. Para todo estos valores se tiene también una mejora sobre la cota gonalidad.*

Ahora estudiaremos el caso en que $m_i > n$. Recuerde que $m_i = n + l$ con $l \in \text{Gaps}(H)$. Para cada $t = 1, 2, \ldots, a - 1$, consideremos las lagunas especiales $\lambda_t = tb - a$, ver la Sección 3.3.

Lema 142 *Si $m_i = n + \lambda_t$, entonces $d^*_2(i) = a - t + 1$.*
Demostración. Sea $m_s = m_i - b$, por el Corolario128, $\#\Lambda^*_{s,i} = \#\Lambda^*_s = a - t + 1$. Para todo j_1, j_2 con $1 \leq j_1 < j_2 \leq i$, por el Corolario 128 y el Lema 107, $\#\Lambda^*_{j_1,j_2} \geq \#\Lambda^*_{j_1} \geq a - t + 1$. Cuando $t = 1$, entonces $m_s = n - a$. Pero $\#\Lambda^*_s = a$ y por el Lema 104, $\#\Lambda_j \geq a$ para $m_s < m_j < n$. ■

Teorema 143 *Si $m_i = n + l$ con $\lambda_t \leq l < \lambda_{t+1}$, entonces $d^*_2(i) = a - t + 1$.*
Demostración. Note que $n + \lambda_t \leq m_i < n + \lambda_{t+1}$. Sea $m_s = n + \lambda_t$. De acuerdo al Lema 142 podemos suponer que $s \leq j_1 < j_2 \leq i$. Por tanto, $\#\Lambda^*_{j_1,j_2} \geq \#(\Lambda^*_{j_1} \cup \{m_{j_2}\}) \geq a - t + 1$ ya que $\#\Lambda^*_{j_1} \geq a - t$. ■

Observación 144 *Los valores de m_i en el rango $n < m_i < n + \lambda_1$ no están cubiertos por los resultados previos, excepto si $b = a + 1$, ya que $\lambda_1 = 1$. En general, cuando $b \neq a + 1$ se tiene que $a \leq d^*_2(i) \leq d^*_2(n - g)$ en este intervalo.*

Ejemplo 145 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Para los códigos Norma-Traza C_i con $i = 24, \ldots, 32$ es decir $m_i > n$. Por el Ejemplo 133, estos m_i son: 33, 34, 35, 37, 38, 41, 42, 45, 49. De acuerdo al Teorema 143, la cota de orden $d^*_2(i)$ para el segundo peso de Hamming de estos códigos abundantes es $d^*_2(26) = d^*_2(27) = d^*_2(28) = d^*_2(29) = 4$,*

$d_2^*(30) = d_2^*(31) = 3$ *y* $d_2^*(32) = 2$. *Para* $i = 24, 25$, *por la Observación 144 se tiene que* $4 \leq d_2^*(i) \leq 7$. *Un cálculo directo muestra que* $d_2^*(24) = d_2^*(25) = 6$.

En la siguiente sección completaremos el cálculo explícito de la cota de orden d_2^* para el segundo peso de Hamming de códigos con semigrupo de Weierstrass generado por dos elementos consecutivos.

4.1.2. Semigrupos generados por dos elementos consecutivos.

Cuando $H = \langle a, a+1 \rangle$, es un semigrupo generado por dos elementos consecutivos, podemos calcular la cota de orden d_2^* en su totalidad.

Teorema 146 *Sea* $H = \langle a, a+1 \rangle$. *Si* m_i *es un polo de tipo II y* $n - m_i = l \in L_t \backslash \{l_{t_0}, l_{t_f}\}$, *entonces*

$$d_2^* = (t+1)a - 1.$$

Demostración. Sean j_1, j_2 con $1 \leq j_1 < j_2 \leq i$. Probaremos que $\#\Lambda^*_{j_1,j_2} \geq (t+1)a-1$. La prueba se divide naturalmente en tres partes: (1) sea $m_s = n - ta - t - 1$, entonces $n - m_s = ta + t + 1 = l_{(t+1)_0}$. Si $j_1 \leq s$, por el Corolario 128 y el Teorema 102, $\#\Lambda^*_{j_1,j_2} \geq \#\Lambda^*_{j_1} \geq (t+1)a$. (2) Sea $m_u = n - ta + 1$, entonces $n - m_u = ta - 1 = l_{t_f}$. Si $s < j_1 < u$, con $n - m_{j_1} \in H$ y $m_{j_2} - m_{j_1} < a$, entonces $\#D(m_{j_2} - m_{j_1}) \geq a - 1$ y por el Corolario 129, $\#\Lambda^*_{j_1,j_2} = n - m_{j_1} + \#D(m_{j_2} - m_{j_1}) \geq n - m_{j_1} + a - 1 \geq n - m_u + a = (t+1)a - 1$. (3) Finalmente, si $u \leq j_1 < j_2 \leq i$. Sea $m_{j_1} = n - l_{t_0} - k_{j_1}$ y $m_{j_2} = n - l_{t_0} - k_{j_2}$ con $1 \leq k_{j_2} < k_{j_1} \leq a - 1 - t$. Por el Corolario 129, $\#\Lambda^*_{j_1,j_2} = \#\Lambda^*_{j_1} + \#D(m_{j_2} - m_{j_1}) - \#M_{j_1,j_2} = n - m_{j_1} + \#D(n - m_{j_1}) + \#D(m_{j_2} - m_{j_1}) - \#M_{j_1,j_2} \geq (t-1)a + t + k_{j_1} + a - t + a - 1 - \#M_{j_1,j_2} \geq (t+1)a - 1$. ■

Teorema 147 *Sea* $H = \langle a, a+1 \rangle$. *Si* m_i *es un polo de tipo I y* $n - m_i + 1 \in H$, *entonces*

$$d_2^*(i) = n - m_i + a.$$

Demostración. Similar a la prueba del Teorema 139, pero usando el hecho que cuando $n - m_t = n - m_i + 1 \in H$, entonces $\#\Lambda^*_{t,i} = n - m_i + a$. ■

Ejemplo 148 (Códigos Hermitianos) *Sea* $\mathcal{H} : y^q + y = x^{q+1}$ *la curva Hermitiana de género* $g = \frac{q(q-1)}{2}$ *sobre* $\mathbb{F}_{q^2}$. *Recuerde que esta tiene* q^3 *puntos racionales afines más el punto* Q *en infinito. El semigrupo de Weierstrass de* Q *es* $H = H(Q) = \langle q, q+1 \rangle$, *ver Ejemplo 35.*

Para cada $m_i \in M$ consideremos el código Hermitiano $C_i = C(\mathcal{H}, D, m_i Q)$ donde D es la suma de los q^3 puntos racionales de $\mathcal{H}$ diferentes de Q. De acuerdo a los anteriores resultados obtenemos la cota de orden para el segundo peso de Hamming de todos los códigos Hermitianos. Estos valores se resumen en la tabla siguiente.

m_i	$d_2^*(i)$	*condición*
$m_i < n$	$n - m_i + q$	$n - m_i \in H$ *o* $n - m_i = tq + t - q$
	$qt + q - 1$	$n - m_i \in L_t \setminus \{tq + t - q\}$
$m_i > n$	$q - t + 1$	$m_i - n \in L_t$

En [2] se puede verificar que esta cota de hecho da el verdadero valor de los segundos pesos de Hamming de los códigos Hermitianos. Note que esta caracterización es más simple que la dada en [2].

En general, la cota de orden para los demás pesos de Hamming generalizados de códigos Castillo es difícil de determinar a partir de los resultados previos. En lo que sigue calcularemos algunos pesos de Hamming generalizados que satisfacen la cota singleton generalizada, para códigos Castillo en general, utilizando nuevos conceptos. En el caso de los códigos Hermitianos mostraremos que este es el máximo rango MDS.

4.2. Rango MDS de códigos Castillo.

Sea $I_n = \{1, \ldots, n\}$. Para cualquier $i \in I_n$ denotaremos por $I_i = \{1, \ldots, i\}$ el segmento inicial en I_n y por $\overline{I}_i = I_n \setminus I_i = \{i+1, \ldots, n\}$ su complemento en I_n.

Sea $M = \{m_1, \ldots, m_n\}$ el conjunto de dimensiones de la cadena de códigos Castillo. Recuerde que por el Lema 2.3, $M = \{m \in H : m < n\} \cup \{n + \text{Gaps}(H)\} = H \setminus (n + H)$.

Ahora, podemos reescribir el conjunto Λ_i^*, definido en la ecuación (2.2), como

$$\Lambda_i^* = \{j \in I_n : m_i + m_j \in M\}.$$

Note que $\Lambda_i^* \subset I_{n+1-i}$. Más aún, para códigos Castillo, $\{1, n+1-i\} \subset \Lambda_i^*$, pues por el Lema 86, $m_i + m_{n+1-i} = m_n$ para todo $i = 1, \ldots, n$. Además, si $j \in \Lambda_i^*$ se sabe, por el Corolario 76, que la pareja de vectores $(\mathbf{b}_i, \mathbf{b}_j)$ se comporta bien, donde $\mathbf{b}_i = ev(f_i)$ y $m_i = -v_Q(f_i)$. Por tanto, diremos de un elemento $j \in \Lambda_i^*$ que *se comporta bien* con i.

Definimos los conjuntos:

$$R_i^* = \{j \in I_{n-i} : m_i + m_j \notin M\} \quad \text{y} \quad F_i^* = \overline{I}_{n+1-i} = \{n+2-i, \ldots, n\}.$$

Note que para cada $i = 1, \ldots, n$ los conjuntos Λ_i^*, R_i^* y F_i^* son una partición de I_n. Además, diremos de un elemento $j \in R_i^*$ que *se comporta regular* con i, pues solo sabemos que esta entre dos elementos que se comportan bien con i. También, diremos de un elemento $j \in F_i^*$ que *se comporta fatal* con i, pues no existe posibilidad para que se comporte bien.

Ejemplo 149 *Consideremos el semigrupo de Weierstrass, $H = \langle 3, 4 \rangle$, del punto en infinito de la curva Hermitiana sobre $\mathbb{F}_9$. En la siguiente tabla, la primera fila (separada por la doble línea), contiene el conjunto de dimensiones M. Las demás filas (en color) contienen la información de los conjuntos Λ_i^* (azul claro), R_i^* (azul medio) y F_i^* (azul oscuro) para cada $i \in I_n$ (el primer valor de la izquierda en cada fila). Además, si $j \in \Lambda_i^*$ entonces $m_i + m_j = m_k \in M$ y por la Proposición 76, $\rho(\mathbf{b}_i, \mathbf{b}_j) = k$. Por tanto, si $j \in \Lambda_i^*$ hemos incluido en la posición (i, j) el valor de k.*

0	3	4	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	28	29	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
2	4	5	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		25	26		27	
3	5	6	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		25	26		27		
4	7	8	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		25	26			27			
5	8	9	11	12	13	14	15	16	17	18	19	20	21	22	23	24		25	26			27				
6	9	10	12	13	14	15	16	17	18	19	20	21	22	23	24		25	26			27					
7	10	11	13	14	15	16	17	18	19	20	21	22	23	24		25	26			27						
8	11	12	14	15	16	17	18	19	20	21	22	23	24		25	26			27							
9	12	13	15	16	17	18	19	20	21	22	23	24		25	26			27								
10	13	14	16	17	18	19	20	21	22	23	24		25	26			27									
11	14	15	17	18	19	20	21	22	23	24		25	26			27										
12	15	16	18	19	20	21	22	23	24		25	26			27											
13	16	17	19	20	21	22	23	24		25	26			27												
14	17	18	20	21	22	23	24		25	26			27													
15	18	19	21	22	23	24		25	26			27														
16	19	20	22	23	24		25	26			27															
17	20	21	23	24		25	26			27																
18	21	22	24		25	26			27																	
19	22	23		25	26			27																		
20	23	24	25	26			27																			
21	24		26			27																				
22		25			27																					
23	25	26		27																						
24	26		27																							
25		27																								
26	27																									
27																										

Por ejemplo, $\Lambda_{18}^* = \{1, 2, 3, 4, 6, 7, 10\}$, $R_{18}^* = \{5, 8, 9\}$ y $F_{18}^* = \{11, 12, \ldots, 27\}$.

Por la propiedad de conmutatividad de la suma se tiene la siguiente propiedad de "simetría" de los conjuntos Λ^*, R^* y F^* como sigue.

Lema 150 *Para todos $i, j \in I_n$ se tiene lo siguiente:*

$$j \in \Lambda_i^* \ \ (\textit{respectivamente } R_i^*, F_i^*) \Longleftrightarrow i \in \Lambda_j^* \ \ (\textit{respectivamente } R_j^*, F_j^*).$$

Demostración. Las tres afirmaciones se deducen de la conmutatividad de la suma. ■

Para $i \leq n-g$, si $n-m_i \in H$, es decir $n-m_i = m_{i'} \in M$ para algún $i' \in I_n$, entonces existe una relación "antisimétrica" entre los conjuntos Λ_i^*, R_i^* y F_i^* y los conjuntos $\Lambda_{i'}^*$, $R_{i'}^*$ y $F_{i'}^*$. Esto es, si j se comporta regular (o fatal) con i, entonces $n+1-j$ se comporta bien con i' y viceversa. Esta propiedad se establece a continuación.

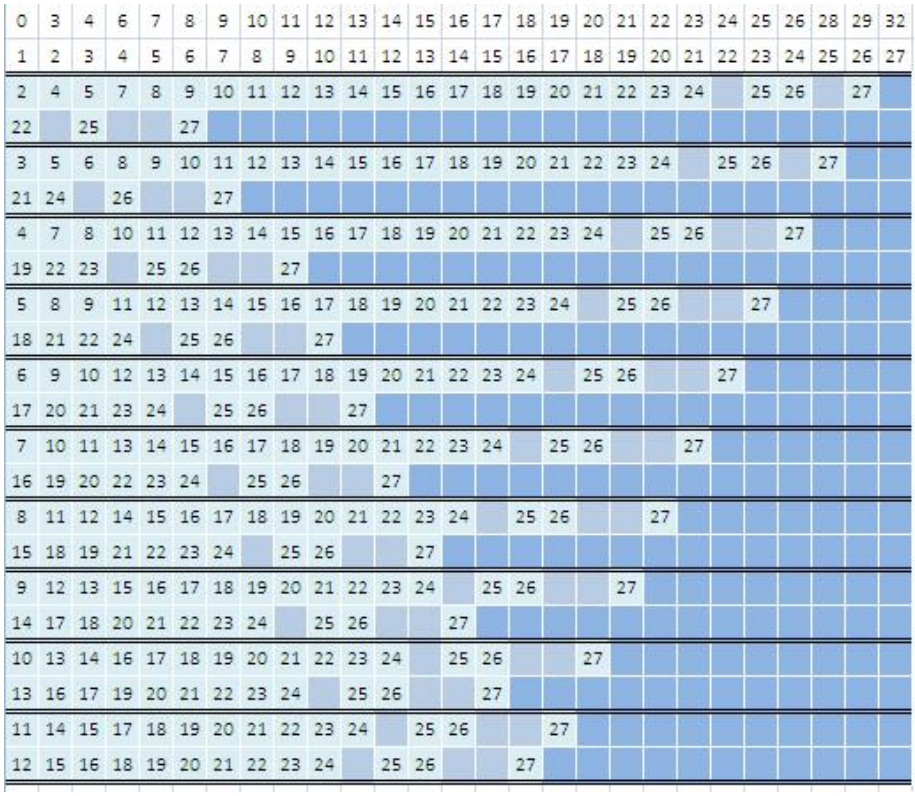
Proposición 151 *Para $i \leq n-g$. Si $n-m_i \in H$, escribamos $n-m_i = m_{i'} \in M$, entonces se tienen las siguientes propiedades:*

(1) $j \in R_i^*$ si y sólo si $n+1-j \in \Lambda_{i'}^*$.

(2) $j \in F_i^*$ si y sólo si $n+1-j \in \Lambda_{i'}^*$.

Demostración. (1) Por la Proposición 154, $j \in R_i^*$ si y sólo si $m_{n+1-j}-m_i \in \mathrm{Gaps}(H)$, por la Ecuación 2.3, si y sólo si $n-m_i+m_{n+1-j} = m_{i'}+m_{n+1-j} \in M$, esto es, si y sólo si $n+1-j \in \Lambda_{i'}^*$. (2) $j \in F_i^*$ si y sólo si $m_j+m_i > m_n$, esto es, $m_i > m_n-m_j = m_{n+1-j}$ es decir, si y sólo si $n > m_{i'}+m_{n+1-j}$ y por la Ecuación 2.3, si y sólo si $m_{i'}+m_{n+1-j} \in M$, es decir $n+1-j \in \Lambda_{i'}^*$. ■

Ejemplo 152 *Para ilustrar la propiedad anterior utilizamos el Ejemplo 149. En la siguiente tabla hemos agrupado en parejas los valores que satisfacen las hipótesis de la Proposición 151. Las filas del primer grupo (sin color) corresponden a los valores m_i e i respectivamente. En los demás grupos, la primera fila corresponde a los valores de los conjuntos Λ_i^*, R_i^*, F_i^* y la segunda fila a los de $\Lambda_{i'}^*$, $R_{i'}^*$, $F_{i'}^*$, con $m_{i'} = n-m_i$. En otras palabras, la propiedad de "antisimetría" dada en la Proposición 151 establece que recorrer la fila de i de izquierda a derecha es equivalente a recorrer la fila de i' de derecha a izquierda cambiando la tonalidad de los colores.*



Por ejemplo, $\Lambda_2^* = I_{21} \cup \{23, 24, 26\}$, $R_2^* = \{22, 25\}$ *y* $F_2^* = \{27\}$. *Ahora como* $n - m_2 = 27 - 3 = 24 = m_{22}$, *entonces* $\Lambda_{22}^* = \{1, 3, 6\}$, $R_{22}^* = \{2, 4, 5\}$ *y* $F_2^* = \overline{I}_6$

El siguiente par de lemas establecen propiedades de R_i^*.

Lema 153 *Si* $c \leq m_i \leq n - m_2$, *entonces* $\{n - i - k : k = 0, \ldots, m_2 - 2\} \subset R_i^*$.
Demostración. $m_{n-i-k} + m_i = m_n - m_{i+k+1} + m_i = m_n - (k + 1) \notin M$, ya que $0 < k + 1 < m_2$. ■

Lema 154 *Para todos* $i, j \in I_n$ *las siguientes afirmaciones son equivalentes:*

(1) $j \in R_i^*$.

(2) $m_{n+1-j} - m_i \in Gaps(H)$.

(3) $m_{n+1-i} - m_j \in Gaps(H)$.

Demostración. (1) $\Leftrightarrow$ (2): $m_{n+1-j} - m_i = l \in \text{Gaps}(H)$ si y sólo si $m_n - l = m_i + m_j$ si y sólo si $j \in R_i^*$. (1) $\Leftrightarrow$ (3): es similar al anterior. ■

Note que $R_i^* = I_{n+1-g} \setminus \Lambda_i^*$. Así, utilizando las Proposiciones 90 y 92 se tiene una caracterización simple para el cardinal de R_i^* para todo $i \in I_n$.

Proposición 155 *Sea $g(i)$ el número de lagunas menor que m_i. Para cada $i \in I_n$ se tiene que*

$$\#R_i^* = \begin{cases} g(i) - \#D(n-m_i) & si \quad i < n-g \\ n+1-i-\#D(m_i-n) & si \quad n-g \leq i \leq n \end{cases}.$$

Demostración. De acuerdo a las Proposiciones 90 y 92, se tiene que

$$\#\Lambda_i^* = \begin{cases} n-m_i+\#D(n-m_i) & \text{si} \quad i < n-g \\ \#D(m_i-n) & \text{si} \quad n-g \leq i \leq n \end{cases}.$$

De otro lado, como $\#\Lambda_i^* = n+1-i-\#R_i^*$ y $m_i = g(i)+i-1$. Combinando estos dos hechos se obtiene el resultado deseado. ■

Corolario 156 *Si $n-m_i \in H$, entonces $\#R_i^* = g(i)$.*
Demostración. Ya que $\#D(n-m_i) = 0$, si $n-m_i \in H$. ■

Corolario 157 *Sea $n-m_i \in Gaps(H)$. Entonces se satisface lo siguiente*

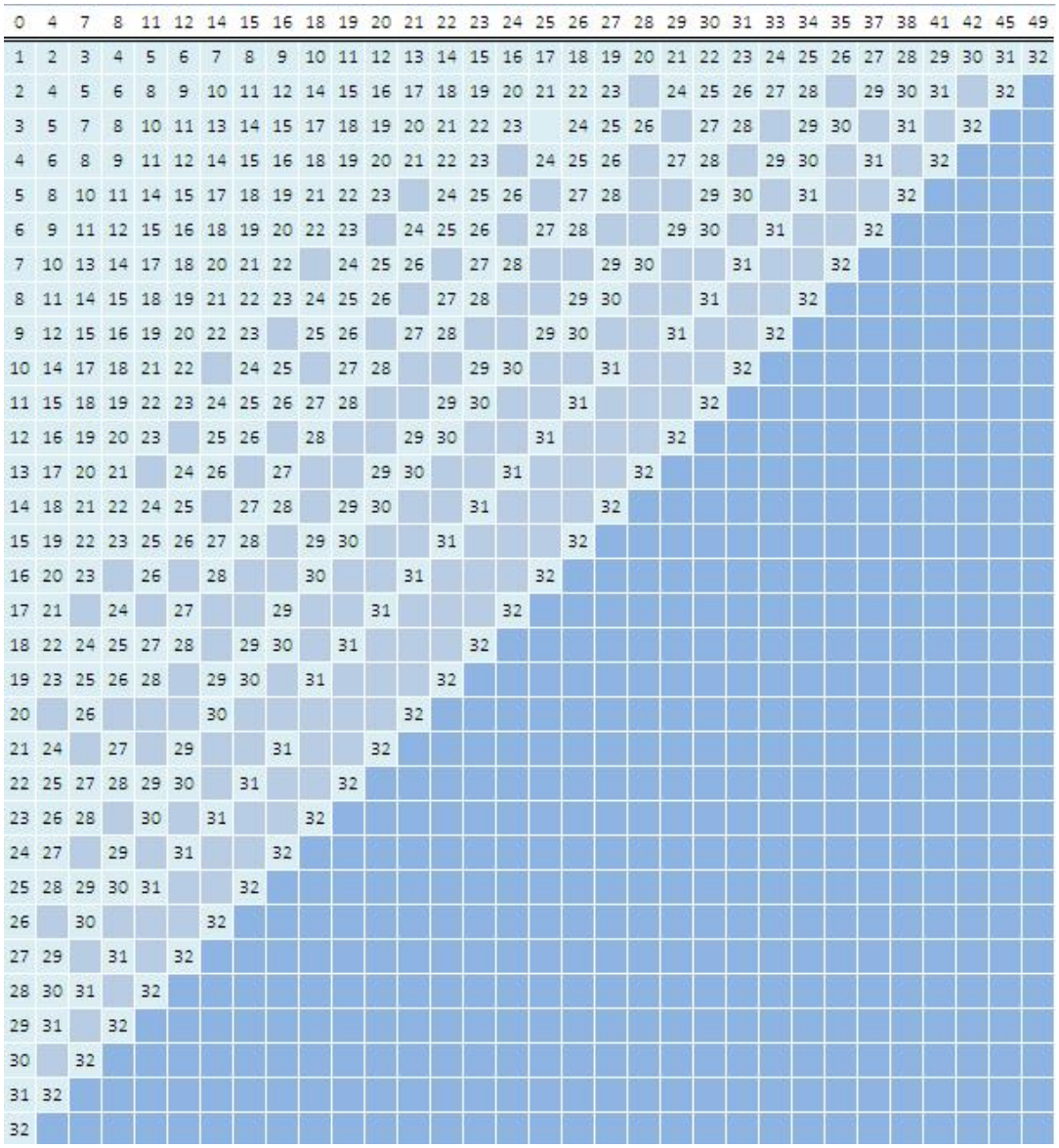
(a) si $n-m_i = l_g$, entonces $\#R_i^* = g(i)-1$.

(b) si $n-m_i \in Gaps(H) \setminus \{l_g\}$, entonces $\#R_i^* \leq g(i)-2$.

Demostración. De acuerdo al Lema 91(c), $D(l_g) = 1$ y si $l \in \text{Gaps}(H) \setminus \{l_g\}$, entonces $D(l) \geq 2$. Por tanto, de la Proposición 155 se tiene la afirmación. ■

Ejemplo 158 *Del Ejemplo 149, obtenemos la secuencia $(\#R_i^*, 1 \leq i \leq 27)$ para todos los códigos Hermitianos sobre $\mathbb{F}_9$. Esta es: (0, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 2, 3, 3, 1 ,1, 1, 0, 0).*

Ejemplo 159 *Similar al Ejemplo 149, consideremos el semigrupo de Weierstrass, $H = \langle 4, 7\rangle$, del punto en infinito de la curva Norma-Traza sobre $\mathbb{F}_8$. La tabla siguiente muestra los valores de los conjuntos Λ_i^*, R_i^* y F_i^* para cada $i \in I_n$. De esta tabla obtenemos la secuencia $(\#R_i^*, 1 \leq i \leq 32)$: (0, 3, 5, 5, 7, 7, 8, 7, 8, 9, 7, 9, 9, 7, 6, 9, 9, 5, 5, 9, 6, 3, 4, 4, 2, 4, 2, 1, 1, 1, 0, 0).*



0	4	7	8	11	12	14	15	16	18	19	20	21	22	23	24	25	26	27	28	29	30	31	33	34	35	37	38	41	42	45	49
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	4	5	6	8	9	10	11	12	14	15	16	17	18	19	20	21	22	23		24	25	26	27	28		29	30	31		32	
3	5	7	8	10	11	13	14	15	17	18	19	20	21	22	23		24	25	26		27	28		29	30		31		32		
4	6	8	9	11	12	14	15	16	18	19	20	21	22	23		24	25	26		27	28		29	30		31		32			
5	8	10	11	14	15	17	18	19	21	22	23		24	25	26		27	28			29	30		31			32				
6	9	11	12	15	16	18	19	20	22	23		24	25	26		27	28			29	30		31			32					
7	10	13	14	17	18	20	21	22		24	25	26		27	28			29	30			31			32						
8	11	14	15	18	19	21	22	23	24	25	26		27	28			29	30			31			32							
9	12	15	16	19	20	22	23		25	26		27	28			29	30			31			32								
10	14	17	18	21	22		24	25		27	28			29	30			31				32									
11	15	18	19	22	23	24	25	26	27	28			29	30			31				32										
12	16	19	20	23		25	26		28			29	30			31				32											
13	17	20	21		24	26		27			29	30			31				32												
14	18	21	22	24	25		27	28		29	30			31				32													
15	19	22	23	25	26	27	28		29	30			31				32														
16	20	23		26		28			30			31				32															
17	21		24		27			29			31				32																
18	22	24	25	27	28		29	30		31				32																	
19	23	25	26	28		29	30		31				32																		
20		26				30						32																			
21	24		27		29			31			32																				
22	25	27	28	29	30		31			32																					
23	26	28		30		31			32																						
24	27		29		31			32																							
25	28	29	30	31			32																								
26		30				32																									
27	29		31		32																										
28	30	31		32																											
29	31		32																												
30		32																													
31	32																														
32																															

4.2.1. Pesos de Hamming generalizados de códigos Castillo.

Para cada $i \in I_n$ consideramos $f_i \in \mathcal{L}(\infty Q)$, tal que $-v_Q(f_i) = m_i$, y $\mathbf{b}_i = ev(f_i)$. Entonces $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ es una base de $\mathbb{F}_q^n$. Consideremos la cadena de códigos

$$(0) = C_0 \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n,$$

donde $\mathrm{C}_i = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$.

Para cada subconjunto $I \subset I_n$ definimos

$$C_i(I) = \{\mathbf{c}^I \in \mathbb{F}_q^n : \mathbf{c} \in C_i\} \text{ donde } c_i^I = \begin{cases} c_i & \text{si } i \in I \\ 0 & \text{si } i \notin I \end{cases}.$$

Como $C_i(I) = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_i^I \rangle$, obtenemos la siguiente cadena de códigos

$$(0) = C_0(I) \subset C_1(I) \subset \cdots \subset C_n(I) = \mathbb{F}_q^n(I).$$

Ahora, como $\#I = \dim \mathbb{F}_q^n(I)$, existen $\#I+1$ códigos distintos en la anterior cadena. Además, se tiene que

$$\mathcal{B}^I = \{\mathbf{b}_k^I : \mathbf{b}_k^I \in C_k(I) \setminus C_{k-1}(I)\}$$

es una base para $\mathbb{F}_q^n(I)$, puesto que $\mathbb{F}_q^n(I) = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_n^I \rangle$ y si $\mathbf{b}_k^I \in C_{k-1}(I)$, entonces $\mathbf{b}_k^I$ es linealmente dependiente de $\{\mathbf{b}_1^I, \ldots, \mathbf{b}_{k-1}^I\}$.

En consecuencia,

$$\#I = \dim \mathbb{F}_q^n(I) = \#\{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}(I)\}. \tag{4.1}$$

Asociado al código $C_i(I)$ definimos su *dual restringido* a I como

$$C_i(I)^{\perp_I} = \{\mathbf{v} \in \mathbb{F}_q^n : \operatorname{sop}(\mathbf{v}) \subset I \text{ y } \mathbf{v} \cdot \mathbf{u} = 0 \text{ para todo } \mathbf{u} \in C_i(I)\} = C_i(I)^\perp \cap \mathbb{F}_q^n(I).$$

Por tanto, $\dim \mathbb{F}_q^n(I) = \dim C_i(I) + \dim C_i(I)^{\perp_I}$.

Ahora, estudiaremos los pesos de Hamming generalizados del código Castillo C_i. Para $i \in I_n$ (fijo), consideremos el conjunto

$$\mathcal{D}_r = \{C : C \text{ es un subcódigo de } C_i \text{ y } \dim C = r\}.$$

En lo que resta de este capítulo supondremos que $C \in \mathcal{D}_r$ y que I es el soporte de C, es decir $I = \operatorname{sop}(C)$.

Lema 160 *Si $C \in \mathcal{D}_r$ y $I = sop(C)$, entonces $C \subset C_i^\perp(I)^{\perp_I}$.*

Demostración. Sea $\mathbf{c} \in C \subset C_i$. Para todo $\mathbf{u} \in C_i^\perp$ se tiene que $0 = \mathbf{c}\cdot\mathbf{u} = \sum_{j=1}^n c_j u_j = \sum_{j \in I} c_j u_j = \mathbf{c}\cdot\mathbf{u}^I$. Así, $c\cdot\mathbf{u}^I$ para todo $\mathbf{u}^I \in C_i^\perp(I)$. Por tanto, $c \in C_i^\perp(I)^\perp$ y el resultado se sigue ya que $\operatorname{sop}(c) \subset I$. ■

Por la Proposición 87, para todo $i \in I_n$ existe $\mathbf{x} \in (\mathbb{F}_q^*)^n$ tal que $C_i^\perp = \mathbf{x} * C_{n-i}$. Por tanto, $C_i^\perp(I) = \mathbf{x}^I * C_{n-i}(I)$ y es claro que $\dim C_i^\perp(I) = \dim C_{n-i}(I)$.

En consecuencia, escribimos la ecuación (4.1) como:

$$\#I = \#\{k \in I_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\} + \#\{k \in \overline{I}_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\}. \tag{4.2}$$

Como $I = \mathrm{sop}(C)$, por la Definición 6, estimar el r-ésimo peso de Hamming de C_i es estimar el mínimo de $\#I$. Entonces la estrategia que usaremos es la de encontrar una cota inferior para cada uno de los anteriores sumandos. En este sentido, probaremos el siguiente par de lemas. En las pruebas de los Lemas 161 y 162 y del Teorema 163, usamos ideas similares a las pruebas de los Lemas 1-4 de [58].

Lema 161 *Sea $m_i + m_j = m_k$. Si $\mathbf{b}_i^I \in C_{i-1}$ o $\mathbf{b}_j^I \in C_{j-1}$, entonces $\mathbf{b}_k^I \in C_{k-1}$.*
Demostración. Como $m_i + m_j = m_k$, entonces $\mathbf{b}_i * \mathbf{b}_j = \sum_{t=1}^{k} \lambda_t b_t$ con $\lambda_k \neq 0$. Así, $\mathbf{b}_i^I * \mathbf{b}_j^I = \sum_{t=1}^{k} \lambda_t \mathbf{b}_t^I$. Supongamos que $\mathbf{b}_i^I \in C_{i-1}$, entonces $\mathbf{b}_i^I = \sum_{t=1}^{i-1} \alpha_t \mathbf{b}_t^I$ y $\mathbf{b}_i^I * \mathbf{b}_j^I = \sum_{t=1}^{i-1} \alpha_t (\mathbf{b}_t^I * \mathbf{b}_j^I) = \sum_{t=1}^{i-1} \alpha_t (\mathbf{b}_t * \mathbf{b}_j)^I$. Como $\rho(\mathbf{b}_t * \mathbf{b}_j) < k$ para todo $t < i$, entonces $\mathbf{b}_t * \mathbf{b}_j = \sum_{u=1}^{k-1} \beta_u \mathbf{b}_u$. Luego, reagrupando términos $\mathbf{b}_i^I * \mathbf{b}_j^I = \sum_{u=1}^{k-1} \gamma_u \mathbf{b}_u^I$. Por tanto, $\mathbf{b}_k^I = 1/\lambda_k \sum_{t=1}^{k-1} (\gamma_t - \lambda_t) \mathbf{b}_t^I$ es decir $\mathbf{b}_k^I \in C_{k-1}(I)$. El otro caso es similar. ■

Para $C \in \mathcal{D}_r$ definimos los conjuntos

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^I \in C_{k-1}\} \text{ y } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lema 162 *Si $j \in \overline{I}_{n-i}$ y $\mathbf{b}_j^I \notin C_{j-1}(I)$, entonces $n + 1 - j \in R_{T_C}^*$*
Demostración. Argumentaremos por contradicción. Supongamos que $n+1-j \notin R_{T_C}^*$. Como $n + 1 - j \in I_i$, entonces $j \in \Lambda_{T_C}^* = \bigcup_{t \in T_C} \Lambda_t^*$. Por tanto, existe algún $k \in T_C$ tal que $n + 1 - j \in \Lambda_k^*$. Entonces $m_{n+1-j} + m_k = m \in M$ es decir $(m_n - m) + m_k = m_j$. Como $k \in T_C$, entonces $\mathbf{b}_k^I \in C_{k-1}(I)$. Por el Lema 161, $\mathbf{b}_j^I \in C_{j-1}(I)$. ■

Para cada $T \subset I_{n-i}$ definimos el conjunto

$$W_T = \{k \in \overline{I}_{n-i} : n + 1 - k \in R_T^*\}.$$

Por el Lema 162, $\{k \in \overline{I}_{n-i} : \mathbf{b}_k^I \notin C_{k-1}\} \subset W_{T_C}$.

Teorema 163 *Sea $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ y } \#W_T \geq r\}$.*

(1) $\#\{k \in \overline{I}_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\} \geq r$.

(2) $\#\{k \in I_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\} \geq n - i - \xi_r$.

Demostración. (1) Consideremos $A = \{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}(I) \text{ y } \mathbf{b}_k^I \in C_{n-i}(I)\}$ y $B = \{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}(I) \text{ y } \mathbf{b}_k^I \notin C_{n-i}(I)\}$. Entonces $A \cap B = \emptyset$ y $\mathbb{F}_q^n(I) = \langle A \rangle \oplus \langle B \rangle$, donde $\oplus$ denota la suma directa, $\langle A \rangle = \{b_k : k \in A\}$ y $\langle B \rangle = \{b_k : k \in B\}$. Como $\langle A \rangle \subset C_{n-i}(I)$ y por el Lema 160, $r = \dim C \leq \dim C_{n-i}(I)^{\perp_I} = \dim \mathbb{F}_q^n(I) - \dim C_{n-i}(I) \leq \dim \mathbb{F}_q^n(I) - \dim\langle A \rangle = \dim\langle B \rangle \leq \#B$. Por otro lado, como $b_k^I \notin C_{n-i}(I)$ implica que $b_k \notin C_{n-i}$ i.e. $k > n - i$. Por tanto, $B = \{k \in \overline{I}_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\}$. (2) Como $\#\{k \in I_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\} = \#I_{n-i} \setminus T_C = n - i - \#T_C$, basta con probar que $\#T_C \leq \xi_r$. Ahora, de acuerdo al lema 162, $\{k \in \overline{I}_{n-i} : \mathbf{b}_k^I \notin C_{k-1}(I)\} \subset W_{T_C}$ y por el numeral (1) de este teorema, $\#W_{T_C} \geq r$. Como $T_C \subset I_{n-i}$, entonces $\{T_C : C \in \mathcal{D}_r\} \subset \{T \subset I_{n-i} : \#W_{T_C} \geq r\}$. Por tanto, $\#T_C \leq \text{máx}\{\#T_{C'} : C' \in \mathcal{D}_r\} \leq \xi_r$. ■

Corolario 164 *Para cada $i \in I_n$, el r-ésimo peso de Hamming del código castillo C_i satisface $d_r(C_i) \geq n - i + r - \xi_r$.*

Demostración. Se deduce de la Ecuación (4.2) y el Teorema 163. ■

La cota inferior para el r-ésimo peso de Hamming de los códigos Castillo dada en el Corolario 164 la llamaremos la cota de Shibuya-Sakaniwa para códigos Castillo. Note que la cota dada en [58] funciona para códigos duales, mientras la cota del Corolario 164 se usa directamente sobre los códigos Castillo primarios.

Para todos $i, j \in I_n$, definimos

$$X_i(j) = R_j^* \cap I_i \quad \text{y} \quad w_i = \text{máx}\{\#X_i(j) : j \in I_{n-i}\}.$$

Además, definimos $w_0 = 0$.

Note que $X_i(n - i) = R_{n-i}^*$, ya que $R_{n-i}^* \subset I_i$. En consecuencia, $w_i \geq \#R_{n-i}^*$.

Lema 165 *Si $T \subset I_{n-i}$, entonces $\#W_T \leq w_i$.*

Demostración. Para cada $j \in T$ sea $W_j = \{k \in \overline{I}_{n-i} : n + 1 - k \in R_j^*\}$. Entonces $\#W_j = \#X_i(j)$ ya que $k \in W_j$ si y sólo si $n + 1 - k \in X_i(j)$. En consecuencia, el resultado se sigue por la definición de w_i. ■

Teorema 166 *Para cada $i \in I_n$. Si $w_i + 1 \leq r \leq i$, entonces el r-ésimo peso de Hamming del códigos Castillo C_i satisface $d_r(C_i) = n - i + r$.*

Demostración. Por un lado note que $\xi_r = 0$ en el Teorema 163. Pues, por el Lema 165, no existe $T \neq \emptyset$, $T \subset I_{n-i}$ tal que $\#W_T \geq w_i + 1$. Luego, $d_r(C_i) \geq n - i + r$. La igualdad se tiene por la cota singleton generalizada, ver Proposición 7(2). ■

Ejemplo 167 (Códigos Hermitianos sobre $\mathbb{F}_9$) *Consideremos los códigos Castillo sobre la curva Hermitiana $\mathcal{H}$ sobre $\mathbb{F}_9$ dada por la ecuación afín $y^3 + y = x^4$. Del Ejemplo*

149 se obtiene la secuencia $(w_i : 1 \leq i \leq 27)$*: (0, 1, 1, 2, 3, 3, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 0, 0). De otra parte, toda la jerarquía de pesos de todos los códigos Hermitianos fue determinada por Angela Barbero y Carlos Munuera en [2], utilizando este artículo en la siguiente tabla calculamos los pesos de Hamming generalizados* $d_r(C_i)$ *de los códigos Hermitianos* C_i *sobre* $\mathbb{F}_9$*. Para cada código* C_i *calculamos solo hasta el toque* τ_i *de* C_i *que resaltaremos en negrilla, ver Definición 10.*

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$d(C_i)$	**27**	24	23	21	20	19	18	17	16	15	14	13	12	11
$d_2(C_i)$		**27**	**26**	24	23	22	21	20	19	18	17	16	15	14
$d_3(C_i)$				**26**	24	23	**23**	21	20	19	18	17	16	15
$d_4(C_i)$					**26**	**25**		**23**	**22**	**21**	**20**	**19**	**18**	**17**

i	15	16	17	18	19	20	21	22	23	24	25	26	27
$d(C_i)$	10	9	8	7	6	6	4	3	3	3	2	**2**	**1**
$d_2(C_i)$	13	12	11	10	9	8	7	6	5	4	3		
$d_3(C_i)$	14	13	12	11	10	9	8	7	6	**6**	**5**		
$d_4(C_i)$	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**				

Note que para cada $i = 1, \ldots, 27$ *el toque* τ_i *de* C_i *coincide con el primer valor* $w_i + 1$ *para el cual se tiene la igualdad de la cota singleton generalizada, ver el Teorema 166. Es decir, para cada* $i = 1, \ldots, 27$ *se tiene que* $\tau_i = w_i + 1$*. Este hecho es verdad para todos los códigos Hermitianos como demostraremos en la Subsección 4.2.3.*

Puesto que los códigos Castillo satisfacen la propiedad de isometría dual, ver la Proposición 87. Podemos obtener un intervalo MDS de los códigos Castillo primarios usando [58, Prop. 5] sobre su dual isométrico. Resaltamos que el intervalo MDS de los códigos Castillo, dado por el Teorema 166, es mejor que el obtenido por [58, Prop. 5] sobre su dual isométrico. Esto se puede comprobar, para $i = 1, 2, 3, 4, 7$ en los códigos Hermitianos C_i del Ejemplo 167.

4.2.2. Nueva cota para la distancia mínima de códigos Castillo.

De manera análoga a como en [58] se obtuvo la cota de Shibuya-Sakaniwa para la distancia mínima, usaremos el Teorema 166 para obtener una nueva cota inferior para la distancia mínima de los códigos Castillo C_i para todo $i \in I_n$.

Teorema 168 *Para cada* $i \in I_n$*. La distancia mínima del código Castillo* C_i *verifica*

$$d(C_i) \geq d_w(i) = n + 1 - i - w_{n-i}.$$

Demostración. Por la Proposición 7(1), máx$\{n+1-d_r(C_i) : 1 \leq r \leq i\} = n+1-d(C_i)$. Como $d_r(C_i^{\perp}) = d_r(C_{n-i})$, por la Proposición 7(3), $n+1-d(C_i) \notin \{d_r(C_{n-i}) : 1 \leq r \leq n-i\}$ y además $\overline{I}_{n+1-d(C_i)} \subset \{d_r(C_{n-i}) : 1 \leq r \leq n-i\}$. Por tanto, si $n-i+2-d(C_i) \leq r \leq n-i$, entonces $d_r(C_{n-i}) = i+r$. Luego, comparando con el Teorema 166, se tiene que $w_{n-i}+1 \geq n-i+2-d(C_i)$ es decir, $d(C_i) \geq n+1-i-w_{n-i}$. ■

Ejemplo 169 (Códigos Norma-Traza sobre $\mathbb{F}_8$) *Consideremos los códigos Castillo sobre la curva Norma-Traza $\mathcal{X}$ sobre $\mathbb{F}_8$, dada por la ecuación afín $x^7 = y^4 + y^2 + y$. Usando el Ejemplo 159 obtenemos los valores de w_i para todo $i \in I_{32}$. En consecuencia, obtenemos, por el Teorema 168, la cota $d_w(i)$ para todo $i \in I_{32}$. En la siguiente tabla resumimos estos valores.*

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
w_i	0	1	1	2	3	4	4	5	6	7	8	9	7	8	9	9
$d_w(i)$	32	28	25	24	21	20	18	18	16	14	14	12	11	11	11	8
i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
w_i	7	8	9	9	8	9	8	7	8	7	7	5	5	3	0	0
$d_w(i)$	7	7	7	4	4	4	4	4	4	3	3	3	3	2	2	1

Note que la cota $d_w(i)$ para la distancia mínima de los códigos Norma-Traza sobre $\mathbb{F}_8$, coinciden con los valores de la cota de orden calculada en la sección 3.4.

Ahora, la cota d_w mejora la cota de Shibuya-Sakaniwa sobre la distancia mínima, [58, Thm. 1]. Esto se puede comprobar, en el ejemplo anterior, para todos los códigos Norma traza abundantes, pues en este caso la cota de Shibuya-Sakaniwa es negativa, y para los códigos Norma traza no abundantes con $i = 8, 11, 14, 15, 18, 19, 21, 22, 23$, pues para estos la cota de Shibuya-Sakaniwa es respectivamente 17,13,10,9,6,5,3,2,1.

Lema 170 *Si $n - m_i \in H$, entonces $w_{n-i} = g(i)$.*
Demostración. Por el Corolario 156, $\#X_{n-i}(i) = \#R_i^* = g(i)$. Si $j \in I_i$ entonces, por la Proposición 155, $\#R_i^* \geq \#R_j^*$. En consecuencia, $\#X_{n-i}(i) = \#(R_i^* \cap I_{n-i}) \geq \#(R_j^* \cap I_{n-i}) = \#X_{n-i}(j)$, ya que $R_i \subset I_{n-i}$, $R_j \subset I_{n-j}$ y $I_{n-i} \subset I_{n-j}$. Por tanto, $w_{n-i} = \#X_{n-i}(i) = g(i)$. ■

Cuando $n - m_i \in H$, el siguiente corolario establece que la cota d_w es igual a la cota de Goppa. En este caso, por el Corolario 93, ésta también coincide con la cota de orden.

Corolario 171 *Si $n - m_i \in H$, entonces $d_w(i) = d_{ORD}(i) = d_G(C_i) = n - m_i$.*
Demostración. Se deduce del Teorema 168, el Lema 170 y el hecho que para $m_i < n$, $m_i = i + g(i) - 1$. ■

En consecuencia, para $m_i < n$ se podría tener una mejora de la cota de Goppa, solo cuando $n-m_i \in \text{Gaps}(H)$. De acuerdo al Teorema 170, la Proposición 155 y el hecho que $w_{n-i} \geq \#R_i^*$, el valor máximo posible de dicha mejora es $d_w(i) \leq n-m_i+\#D(n-m_i)$.

En lo que resta de esta sección, bajo algunas condiciones especificas, calculamos explícitamente la cota $d_w(i)$, cuando $n-m_i \in \text{Gaps}(H)$.

Lema 172 *Sean $n-m_i = l \in Gaps(H)$ y $m_{s-1} < l < m_s$. Para todo j con $m_i \geq m_j \geq n-m_s$ se tiene que $\#X_{n-i}(j) = \#R_j^* - (i-j)$.*
Demostración. Como $R_j^* \subset I_{n-j}$, $I_{n-i} \subset I_{n-j}$ y $X_{n-i}(j) = R_j^* \cap I_{n-i}$, es suficiente probar que $\{n-i+k : k = 1, \ldots, i-j\} \subset R_j^*$. En efecto, $m_{n-i+k}+m_j = m_n - m_{i-k+1} + m_j \notin M$, pues $0 < m_{i-k+1} - m_j < m_2$ para todo k con $1 \leq k \leq i-j$. ■

El siguiente resultado muestra el primer valor para el cuál se puede tener una mejora sobre la cota de Goppa.

Lema 173 *Si $n-m_i = l_g$, entonces $w_{n-i} = \#R_i^* = g(i)-1$.*
En consecuencia, $d_w(i) = n-m_i+1$.
Demostración. Para todo $j \in I_i$ se tiene que $\#X_{n-i}(j) = \#(R_j^* \cap I_{n-i}) \leq \#R_j^* - 1$, ya que $R_j^* \subset I_{n-j}$, $I_{n-i} \subsetneq I_{n-j}$ y $n-j \in R_j^*$. Por otro lado, si $j \neq i$, entonces $n-m_j \in H$. Por el Corolario 156, $\#R_j^* = g(j)$. Por tanto, $\#X_{n-i}(j) \leq g(j)-1 \leq g(i)-1 = \#R_i^*$. La última igualdad por el Corolario 157(a). ■

Teorema 174 *Sean $n-m_i = l \in Gaps(H) \setminus \{l_g\}$ y $m_{s-1} < l < m_s$. Si para todo j con $m_i \geq m_j \geq n-m_s$ se tiene que $\#D(n-m_j) \geq m_s-n+m_j$, entonces $w_{n-i} = g-m_s+l$.*
Demostración. Ya que $n \geq 2c-m_2$, entonces $n-m_s \geq c$. La demostración se divide naturalmente en tres partes. (1) Supongamos que j es tal que $m_i \geq m_j \geq n-m_s$. Por el Lema 172, $\#X_{n-i}(j) = \#R_j^* - (m_i-m_j) = g - \#D(n-m_j) - (m_i-m_j) \leq g-(m_s-n+m_j)-(m_i-m_j) = g-m_s+l$. Por el Lema 172, la igualdad se da cuando $m_j = n-m_s$. (2) Supongamos que j es tal que $n-m_s \geq m_j \geq c$. Como $m_s-l \leq m_2-1$, por el Lema 153, $\#X_{n-i}(j) \leq \#R_j^* - m_s + l \leq g-m_s+l$. (3) Supongamos que j es tal que $m_j < c$. Entonces $k \in X_{n-i}(j)$ si y sólo si $k \in R_j^*$ y $k \in I_{n-i}$, i.e. $m_k < m_{n+1-i}$, por la Proposición 154, si y sólo si $l = m_{n+1-j} - m_k > m_{n+1-j} - m_{n+1-i} = m_i - m_j$. Por tanto, $\#X_{n-i}(j) \leq g - \overline{g}(m_i-m_j) < g-m_s+l$ ya que $m_i-m_j > m_s-l$ y $\overline{g}(m_i-m_j) > \overline{g}(m_s-l) = m_s-l$, donde $\overline{g}(w)$ denota el número de lagunas menores o iguales que w. ■

Corolario 175 *Si se satisfacen las condiciones del Teorema 174, entonces*

$$d_w(i) = m_s = \text{mín}\{h \in H : h \geq n-m_i\}.$$

Demostración. Es consecuencia de los Teorema 168 y 174. ■

Las hipótesis del Teorema 174 se satisfacen, por ejemplo, en los códigos Castillo con semigrupos de Weierstrass generado por dos elementos (ver el Lema 104), para semigrupos telescópicos en el intervalo $n - c < m_i \leq n - (\delta_{k-1} - 1)a_k$ (ver el Lema 110) o en los desiertos cortos y gran parte de los desiertos largos, en el caso de códigos Suzuki (ver los Lemas 118 y 120). En consecuencia, al menos para estos casos, la cota $d_w(i)$ sobre la distancia mínima de C_i es tan buena como la cota de orden, $d_{ORD}(i)$. En general no encontramos relación entre estas cotas.

En la siguiente sección completamos el calculo de la cota d_w sobre la distancia mínima de los códigos hermitianos abundantes, es decir $m_i > n$. En este caso, al igual que la cota de orden, esta coincide con el verdadero valor de la distancia mínima de los códigos Hermitiano [62]. Más aún, demostraremos en la siguiente sección que el intervalo MDS dado por el Teorema 166, corresponde al máximo rango MDS de los códigos Hermitianos.

4.2.3. Rango MDS de códigos Hermitianos.

Sea $\mathcal{H} : y^q + y = x^{q+1}$ la curva Hermitiana de género $g = \frac{q(q-1)}{2}$ sobre $\mathbb{F}_{q^2}$. Recuerde que esta tiene q^3 puntos racionales afines más el punto Q en infinito. El semigrupo de Weierstrass de Q es $H = H(Q) = \langle q, q+1 \rangle$, ver Ejemplo 35.

Para cada $m_i \in M$ consideremos el código Hermitiano $C_i = C(\mathcal{H}, D, m_i Q)$ donde D es la suma de los q^3 puntos racionales de $\mathcal{H}$ diferentes de Q.

En lo que sigue completaremos en cálculo de la cota d_w para todos los códigos Hermitianos. En consecuencia, obtenemos el toque, y por tanto el rango MDS, de todos los códigos Hermitianos.

Lema 176 *Sea $m_i = n + l$ con $l \in L_t$. Para todo j con $m_j = n + \widetilde{l}$ y $l \geq \widetilde{l} \geq l_{t_0}$ se tiene que $\#X_{n-i}(j) = \#R_j^* - l + \widetilde{l}$.*

Demostración. Como $R_i^* \subset I_{n-j}$, $I_{n-i} \subset I_{n-j}$ y $X_{n-i}(j) = R_j^* \cap I_{n-i}$, es suficiente demostrar que $\{n - i + \alpha : \alpha = 1, \ldots, i - j\} \subset R_j^*$. En efecto, $m_{n-i+\alpha} + m_j = m_n - m_{i-\alpha+1} + m_j \notin M$ ya que $0 < m_{i-\alpha+1} - m_j < m_2$ para todo α con $1 \leq \alpha \leq i - j$. ■

Ahora, note que podemos reescribir el conjunto $D(w)$ como:

$$D(w) = \{l \in \text{Gaps}(H) : l - w \in M\}.$$

Para $0 < u < c$, denotaremos por $\text{Gaps}_{>u} = \{l \in \text{Gaps}(H) : l > u\}$ el conjunto de

lagunas mayores que u. Por el Lema 154, también podemos reescribir los conjuntos

$$R_i^* = \{l \in \text{Gaps}(H) : m_{n+1-i} - l \in M\} \text{ y } X_{n-i}(j) = \{l \in R_j^* : l > m_i - m_j\}.$$

Además se tienen las propiedades siguientes para el conjunto R_i^*.

Lema 177 *Para cada $i \in I_n$ se tiene que $R_i^* = \{l \in \text{Gaps}(H) : m_i + l \in M\}$.*
Demostración. $m_{n+1-i} - l = n + l_g - m_i - l = n + l_g - (m_i + l)$. ■

Proposición 178 *El conjunto R_i^* satisface las propiedades siguientes*

(1) si $c \leq m_i < n$, entonces $R_i^* = \text{Gaps}(H) \setminus D(n - m_i)$.

(2) si $m_i > n$, escribamos $m_i = n + l$, entonces $\{l + R_i^*\} = \text{Gaps}(H)_{>l} \setminus D(l)$.

Demostración. (1) Si $n - m_i \in H$, entonces $D(n - m_i) = \emptyset$ y por la Proposición 155, el resultado se sigue por razones de cardinalidad. Si $n - m_i \in \text{Gaps}(H)$, entonces $\widetilde{l} \in \text{Gaps}(H) \setminus D(n-m_i)$ si y sólo si $\widetilde{l} - (n-m_i) \in \text{Gaps}(H)$ si y sólo si $n + \widetilde{l} - (n-m_i) = m_i + \widetilde{l} \in M$ y por el lema anterior, si y sólo si $\widetilde{l} \in R_i^*$. (2) $\widetilde{l} \in \text{Gaps}(H)_{>l} \setminus D(l)$ si y sólo si $\widetilde{l} - l \in \text{Gaps}(H)$ si y sólo si $m_i + (\widetilde{l} - l) = n + \widetilde{l} \in M$ y por el lema anterior, si y sólo si $\widetilde{l} - l \in R_i^*$. ■

Lema 179 *Sea $m_i = n + l$ con $l \in \text{Gaps}(H)$. Entonces se tiene que*

(1) para todo j con $i \geq j > n - g$, si escribimos $m_j = n + \widetilde{l}$ donde $\widetilde{l} \leq l$, entonces $\#X_{n-i}(j) = \#(Gaps_{>l}(H) \setminus D(\widetilde{l}))$. Más aún, $\{\widetilde{l} + X_{n-i}(j)\} = Gaps_{>l}(H) \setminus D(\widetilde{l})$.

(2) para todo j con $j < n - g$ se satisface $X_{n-i}(j) = Gaps_{>m_i - m_j}(H) \setminus D(n - m_j)$.

Demostración. (1) $\bar{l} \notin D(\widetilde{l})$ si y sólo si $\bar{l} - \widetilde{l} \in \text{Gaps}(H)$ Así, $m_j + (\bar{l} - \widetilde{l}) = n + \bar{l} \in M$ es decir $\bar{l} - \widetilde{l} \in R_j^*$. Además, si $\bar{l} > l$, entonces $\bar{l} - \widetilde{l} > l - \widetilde{l} = m_i - m_j$. En consecuencia, $\bar{l} - \widetilde{l} \in X_{n-i}(j)$. (2) $\bar{l} \in X_{n-i}(j)$ si y sólo si $\bar{l} \in R_j^*$ y $\bar{l} > m_i - m_j$, esto es, si y sólo si $\bar{l} \in \text{Gaps}(H) \setminus D(n - m_j)$ y $\bar{l} > m_i - m_j$. Es decir, $\bar{l} \in \text{Gaps}_{>m_i - m_j}(H) \setminus D(n - m_j)$. ■

Para cada laguna $l \in \text{Gaps}(H)$, sea $m(l)$ el número de polos menores que l. Para semigrupos generados por dos elementos consecutivos se tiene que si $l \in L_t$, entonces $m(l) = 1 + 2 + \cdots + t = \frac{t(t+1)}{2}$. Además, note que para todo $m_i > n$, es decir $m_i = n + l$, se tiene que $m_i = g + i - 1 + m(l)$.

Teorema 180 *Si $m_i = n + l$ con $l \in L_t$, entonces $w_{n-i} = n + 1 - i - q + t$.*
Demostración. Sea $m_{i'} = n + l_{t_0}$, donde l_{t_0} es la laguna inicial en el desierto L_t.

La demostración se divide naturalmente en tres partes: (1) Supongamos que j es tal que $i \geq j \geq i'$, es decir $m_j = n + \widetilde{l}$ con $l \geq \widetilde{l} \geq l_{t_0}$. Como $\#D(\widetilde{l}) \geq q - t$ y por el Lema 176, entonces $\#X_{n-i}(j) \leq \#R_j^* = n + 1 - j - \#D(\widetilde{l}) \leq n + 1 - j - q + t = n + 1 - i' - (j - i') - q + t = \#X_{n-i}(i')$. (2) Supongamos que j es tal que $i' > j > n - g$, es decir, $m_j = n + \widetilde{l}$ con $\widetilde{l} < l$. Como $\#(\text{Gaps}_{>l}(H) \cap D(\widetilde{l})) \geq q - t - 1$, ya que $D(\widetilde{l})$ tiene al menos un elemento en cada desierto posterior a L_t, y por el Lema 179(1), entonces $\#X_{n-i}(j) = \#\text{Gaps}_{>l}(H) - \#(\text{Gaps}_{>l}(H) \cap D(\widetilde{l})) \leq g - l - m(l) - q + t = n + 1 - i - q + t = \#X_{n-i}(i')$. (3) Finalmente, supongamos que j es tal que $m_i - l_g < m_j < n$, ya que si $m_j \leq m_i - l_g$ entonces $X_{n-i}(j) = \varnothing$, pues el primer elemento de R_j^* tiene que ser al menos $n - m_j$ y $n - m_j \geq n - m_i + l_g = n + l_g - m_i = m_{n+1-i}$ por tanto no esta en I_{n-i}. Si $n - m_j \in H$, entonces existen al menos $q - t - 1$ lagunas entre l y $m_i - m_j = l + (n - m_j)$ ya que $n - m_j \geq q$. Entonces $\#X_{n-i}(j) = \#\text{Gaps}_{>m_i - m_j}(H) \leq \#(\text{Gaps}_{>l}(H) - (q - t - 1) = g - l - m(l) - q + t = n + 1 - i - q + t$. Si $n - m_j \in \text{Gaps}(H)$, entonces supongamos que $m_{s-1} < n - m_j < m_s$ y sea $m_k = n - m_s \in M$. Así, $\#X_{n-i}(j) = \#(\text{Gaps}_{>m_i - m_j}(H) \setminus D(n - m_j)) \leq \#\text{Gaps}_{>m_i - m_k}(H) = \#X_{n-i}(k)$ ya que $\#D(n - m_j) \geq m_j - m_k$. Por el caso anterior se tiene la desigualdad deseada. ■

Corolario 181 *Sea $m_i > n$. Si $m_i = n + l$ con $l \in L_t$, entonces $d_w(i) = q - t$.*
Demostración. Es consecuencia directa de los Teoremas 168 y 180. ■

Note que de los Corolarios 171, 175 y 181 se tiene que la cota d_w coincide con el verdadero valor de la distancia mínima de los códigos Hermitianos [62], y tiene la misma caracterización sencilla dada por la cota de orden en la Sección 3.2.1.

Finalmente, mostramos que el intervalo dado por el Teorema 166 establece el rango MDS de todos los códigos Hermitianos, como se establece a continuación.

Teorema 182 *Para cada $i \in I_n$, el entero $w_i + 1$ es el toque del código Hermitiano C_i.*
Demostración. Si $i = n$ es inmediato. Si $g \leq i < n$, entonces $0 \leq m_{n-i} < n$ y consideraremos dos casos: (1) Si $n - m_{n-i} \in H$, por el Lema 170, $w_i = g(n - i)$. Así, por el Teorema 166, $d_{w_i+1}(C_i) = n - i + w_i + 1 = (n - i) + g(n - i) + 1 = m_{n-i} + 2$. De otro lado, $d(C_{n-i}) = n - m_{n-i}$ y por la Proposición 7(3), $n + 1 - d(C_{n-i}) = m_{n-i} + 1 \notin \{d_r(C_i)\}_{r=1,\ldots,i}$. Por tanto, $w_i + 1$ es el toque de C_i. (2) Si $n - m_{n-i} = l \in \text{Gaps}(H)$. Supongamos que $l \in L_t$, por el Lema 173 y el Teorema 174, $w_i = g(n - i) - qt + l$. Así, por el Teorema 166, $d_{w_i+1}(C_i) = n - i + w_i + 1 = (n - i) + g(n - i) - qt + l + 1 = m_{n-i} + l - qt + 2 = n + 2 - qt$. De otro lado, $d(C_{n-i}) = qt$ y por la Proposición 7(3), $n + 1 - d(C_{n-i}) = n + 1 - qt \notin \{d_r(C_i)\}_{r=1,\ldots,i}$. Por tanto, $w_i + 1$ es el toque de C_i. Finalmente, si $1 \leq i < g$, entonces $m_{n-i} > n$. Supongamos que $m_{n-i} - n \in L_t$.

Por el Teorema 180, $w_i = i + 1 - q + t$. Por tanto, por el Teorema 166, $d_{w_i+1}(C_i) = n - i + w_i + 1 = n + 2 - q + t$. De otro lado, $d(C_{n-i}) = q - t$ y por la Proposición 7(3), $n + 1 - d(C_{n-i}) = n + 1 - q - t \notin \{d_r(C_i)\}_{r=1,\ldots,i}$. Por tanto, $w_i + 1$ es el toque de C_i. ■

Ejemplo 183 (Códigos Hermitianos sobre $\mathbb{F}_{16}$) *Consideremos los códigos Castillo sobre la curva Hermitiana $\mathcal{H}$ sobre $\mathbb{F}_{16}$ dada por la ecuación afín $y^4 + y = x^5$. Ésta tiene 64 puntos racionales afines más el punto en infinito $Q = (0 : 1 : 0)$, que es el polo común de x y y. El semigrupo de Weierstrass de Q es $H = H(Q) = \langle 4, 5 \rangle$, ver Ejemplo 35. Para cada $m_i \in M$ consideremos el código Hermitiano $C_i = C(\mathcal{H}, D, m_i Q)$ donde D es la suma de los q^3 puntos racionales de $\mathcal{H}$ diferentes de Q. Toda la jerarquía de pesos de todos códigos Hermitianos fue determinada en [2]. En la tabla siguiente calculamos los pesos de Hamming generalizados $d_r(C_i)$ de los códigos Hermitianos C_i sobre $\mathbb{F}_{16}$. Para cada código C_i calculamos solo hasta el toque τ_i de C_i que resaltaremos en negrilla, ver Definición 10. Note que $\tau_i = w_i + 1$ segun el Teorema 182.*

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
m_i	0	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21
w_i	0	1	1	2	3	3	4	5	6	6	4	5	6	6	6	5
d	**64**	60	59	56	55	54	52	51	50	49	48	47	46	45	44	43
d_2		**64**	**63**	60	59	58	56	55	54	53	52	51	50	49	48	47
d_3				**63**	60	59	59	56	55	54	54	52	53	50	49	48
d_4					**63**	**62**	60	59	58	57	56	55	54	53	52	51
d_5							**62**	60	59	58	**58**	56	55	54	53	52
d_6								**62**	60	59		**58**	56	55	54	**54**
d_7									**62**	**61**			**58**	**57**	**56**	

i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
m_i	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
w_i	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
d	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27
d_2	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31
d_3	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
d_4	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35
d_5	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36
d_6	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37
d_7	**54**	**53**	**52**	**51**	**50**	**49**	**48**	**47**	**46**	**45**	**44**	**43**	**42**	**41**	**40**	**39**

i	*33*	*34*	*35*	*36*	*37*	*38*	*39*	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*
m_i	*38*	*39*	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*	*50*	*51*	*52*	*53*
w_i	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*
d	*26*	*25*	*24*	*23*	*22*	*21*	*20*	*19*	*18*	*17*	*16*	*15*	*14*	*13*	*12*	*12*
d_2	*30*	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*	*20*	*19*	*18*	*17*	*16*	*15*
d_3	*31*	*30*	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*	*20*	*19*	*18*	*17*	*16*
d_4	*34*	*33*	*32*	*31*	*30*	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*	*20*	*19*
d_5	*35*	*34*	*33*	*32*	*31*	*30*	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*	*20*
d_6	*36*	*35*	*34*	*33*	*32*	*31*	*30*	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*
d_7	**38**	**37**	**36**	**35**	**34**	**33**	**32**	**31**	**30**	**29**	**28**	**27**	**26**	**25**	**24**	**23**

i	*49*	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*	*60*	*61*	*62*	*63*	*64*
m_i	*54*	*55*	*56*	*57*	*58*	*59*	*60*	*61*	*62*	*63*	*65*	*66*	*67*	*70*	*71*	*75*
w_i	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*5*	*5*	*5*	*3*	*3*	*0*	*0*
d	*10*	*9*	*8*	*8*	*8*	*5*	*4*	*4*	*4*	*4*	*3*	*3*	*3*	*2*	**2**	**1**
d_2	*14*	*13*	*12*	*11*	*10*	*9*	*8*	*7*	*7*	*5*	*4*	*4*	*4*	*3*		
d_3	*15*	*14*	*13*	*12*	*12*	*10*	*9*	*8*	*8*	*8*	*7*	*6*	*5*	*4*		
d_4	*18*	*17*	*16*	*15*	*14*	*13*	*12*	*11*	*10*	*9*	*8*	*7*	**7**	**6**		
d_5	*19*	*18*	*17*	*16*	*15*	*14*	*13*	*12*	*11*	*10*	*9*	*8*				
d_6	*20*	*19*	*18*	*17*	*16*	*15*	*14*	*13*	*12*	**12**	**11**	**10**				
d_7	**22**	**21**	**20**	**19**	**18**	**17**	**16**	**15**	**14**							

Note que de las Proposiciones 7 y 87 y el Teorema 182, en general, para calcular los pesos de Hamming generalizados de los códigos Hermitianos es suficiente con conocer solo hasta los pesos de Hamming de orden $q-1$ *y con estos se obtienen todos los demás. Por ejemplo, si para* $i = 15$ *conocemos* $d_1 = 44$, $d_2 = 48$, $d_3 = 49$, $\tau_{15} = 7$, *es decir* $d_7 = 56$ *y para* $i = 49$ *conocemos* $d_1 = 10$, $d_2 = 14$, $d_3 = 15$, $\tau_{49} = 7$, *es decir* $d_7 = 22$, *entonces para calcular los pesos de Hamming de orden 4, 5 y 6 de* C_{15}, *por la Proposición 7(3), estos deben ser algunos de los enteros en el conjunto* $I_n \setminus \{n+1-d_r(C_{49}) : r = 1, \ldots, 49\} = \{64, ..., 56, 54, 53, 52, 49-44\}$, *entonces por la Proposición 7(1),* $d_4(C_{15}) = 52$, $d_5(C_{15}) = 53$ *y* $d_6(C_{15}) = 54$. *Análogamente,* $d_4(C_{49}) = 52$, $d_5(C_{49}) = 53$ *y* $d_6(C_{49}) = 54$.

Bibliografía

[1] H. Andersen and O. Geil, *Evaluation codes from order domain theory*, Finite Fields and their Applications, 14 (2008), pp. 92–123.

[2] A. Barbero, C. Munuera, *The Weight Hierarchy of Hermitian Codes*, SIAM Journal on Discrete Mathematics, 13 (2000), pp. 79–104.

[3] P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields and Application, 13 (2007), pp. 665–680.

[4] P. Beelen and T. Høholdt, *The decoding of algebraic geometry codes.* In E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, World Scientific, Singapore, 2008, pp. 49–98.

[5] E.R. Berlekamp, R.J. McEliece and H. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Transactions on Information Theory, 24(3) (1978), pp. 384–386.

[6] S. V. Bulygin, *Generalized Hermitian codes over $GF(2^r)$*, IEEE Transactions on Information Theory, 52 (2006), pp. 4664–4669.

[7] C. Carvalho and Fernando Torres, *On Goppa codes and Weierstrass gaps at several points*, Designs, Codes and Cryptography, 35 (2005), pp. 211–225.

[8] I.M. Duursma, *Majority coset decoding*, IEEE Transactions on Information Theory, 39 (1993), pp. 1067–1071.

[9] I. Duursma and R. Kirov *An extension of the order bound for AG codes.* In Applied Algebra, Algebraic algorithms and error-correcting codes, pp. 11-22, LNCS 5527, Springer, 2009.

[10] I. Duursma, R. Kirov and S. Park, *Distance bounds for algebraic geometric codes*, J. Pure and Applied Algebra, 215 (2011), pp. 1863–1878.

[11] G.L. Feng and T.R.N. Rao, *Decoding of algebraic geometric codes up to the designed minimum distance*, IEEE Trans. on Information Theory, 39 (1993), pp. 37–45.

[12] G.L. Feng and T.N.T. Rao, *Improved geometric Goppa codes. Part I: Basic Theory*, IEEE Transactions on Information Theory, 41 (1995), pp. 1678–1693.

[13] J. Fitzgerald and R.F. Lax, *Decoding affine variety codes using Gröbner basis*, Designs, Codes and Cryptography, 13(2) (1998), pp. 147–158.

[14] W. Fulton, *Algebraic Curves*. Benjamin, New York, 1969.

[15] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Suplemento ai Rendiconti del Circolo Matematico di Palermo, 51 (1998), pp. 25–46.

[16] A. Garcia and H. Stichtenoth, A class of polynomials over finite fields, Finite Fields and Applications, 5 (1999), pp. 424–435.

[17] O. Geil, *On codes from norm-trace curves*, Finite Fields and Their Applications, 9(3) (2003), pp. 351–371.

[18] O. Geil, *Evaluation codes from an affine variety code perspective*. In E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, World Scientific, Singapore, 2008, pp. 153–180.

[19] O. Geil and R. Matsumoto, *Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups*, J. Pure and Applied Algebra, 213(6) (2009), pp. 1152–1156.

[20] O. Geil, R. Matsumoto and D. Ruano, *Feng-Rao decoding of primary codes*, Finite Fields and their Applications, 23 (2013), pp. 35–52.

[21] O. Geil, C. Munuera, D. Ruano and F. Torres, *On the order bounds for one-point AG codes*, Advances in Mathematics of Communications, 3 (2011), pp. 489–504.

[22] V.D. Goppa, *Codes Associated with Divisors*, Problemy Peredachi Informatsii, 13(1) (1977), pp. 33–39.

[23] V.D. Goppa, *Algebraico-Geometric Codes*, Mathematics of the USSR-Izvestiya, 21 (1983), pp. 75–91.

[24] J.P. Hansen, *Codes on the Klein Quartic, Ideals and Decoding*, IEEE Transactions on Information Theory, 33(6) (1987), pp. 923–925.

[25] J.P.Hansen, *Deligne Lusztig varieties and group codes*, Lecture Notes in Mathematics, 1518 (1992), pp. 63–81.

[26] J.P. Hansen and J.P. Petersen *Automorphism of Ree type, Deligne Lasztig and function fields*. J. Reine Angew Math., 440 (1993) pp. 99–109.

[27] J. P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, Applicable Algebra in Engineering, Communication and Computing, 1 (1990), pp. 67–77.

[28] P. Heijnen and R. Pellikaan, *Generalized Hamming weights of q-ary Reed-Muller codes*. IEEE Transactions on Information Theory, 44(1) (1998) 181–196.

[29] T. Helleseth, T. Klove and J. Mykkeleveit, *The weight distribution of irreducible cyclic codes with block lengths* $n((q^l-1)/N)$, Discrete Math., 18 (1977), pp. 179-211.

[30] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic-Geometry codes*. In V.S. Pless and W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998. http://www.tue.nl/∼ruudp/paper/31.pdf

[31] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure and Applied Algebra, 162 (2001), pp. 273–290.

[32] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*. IEEE Transactions on Information Theory, 41 (1995), pp. 1720–1731.

[33] J. Lewittes, *Places of degree one in function fields over finite fields* J. Pure and Applied Algebra, 69 (1990), pp. 177-183–1156.

[34] J.H. van Lint, *Introduction to coding theory*, second edition, Springer-Verlag, 1992.

[35] J.H. van Lint and G. van der Geer, *Introduction to coding Theory and Algebraic Geometry*, Birkhauser, Verlag Basel, 1988.

[36] F.J. MacWilliams and N. Sloane, *The theory of error-correcting codes*. North-Holland, Amsterdam, 1977.

[37] G.L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography, 22 (2001), pp. 107–121.

[38] G.L. Matthews, *Codes from the Suzuki Function Field*, IEEE Transactions on Information Theory, 50(12) (2004), pp. 3298–3302.

[39] G.L. Matthews and T. Michel, *One-point codes using places of higher degree*, IEEE Transactions on Information Theory, 51 (2005), pp. 1590–1593.

[40] MinT. *Online database for optimal parameters of* (t, m, s)*-nets,* (t, s)*-sequences, orthogonal arrays, linear codes, and OOAs.* Available at http://mint.sbg.ac.at/

[41] R. Matsumoto and S. Miura, *On the Feng-Rao bound for the L-construction of Algebraic-Geometry codes*. IEICE Trans. on Fundamentals, 5 (2000), pp. 923–927.

[42] C. Munuera, *On the generalized Hamming weights of geometric Goppa codes*, IEEE Transactions on Information Theory, 40(6) (1994), pp. 2092–2099.

[43] C. Munuera and W. Olaya-León, *An introduction to Algebraic Geometry codes*. Aparecerá en: Algebra and Geometry for Reliable Communications, Contemporary Mathematics AMS (2014).

[44] C. Munuera and J. Tena, *Codificación de la información*, Pub. Universidad de Valladolid, 1997.

[45] C. Munuera and R. Pellikaan, *Equality of geometric Goppa codes and equivalence of divisors*, Journal of Pure and Applied Algebra, 90 (1993), pp. 229–252.

[46] C. Munuera and F. Torres, *Bounding the trellis state complexity of algebraic geometric codes*, Applicable Algebra in Engineering, Communication and Computing, 15 (2004), pp. 81–100.

[47] C. Munuera, A. Sepúlveda and F. Torres, *Algebraic Geometry codes from Castle curves*, In Coding Theory and Applications, Springer-Verlag, Berlin, LNCS 5228 (2008), pp. 117–127.

[48] C. Munuera, A. Sepúlveda and F. Torres, *Castle curves and codes*, Advances in Mathematics of Communication, 3 (2009), pp. 399–408.

[49] C. Munuera, A. Sepúlveda and F. Torres, *Generalized Hermitian codes*, Designs, Codes and Cryptography, 69 (2013), pp. 123–130.

[50] C. Munuera, G. Tizziotti and F. Torres, *Two-point codes on Norm-Trace curves*. In Coding Theory and Applications, Springer-Verlag, Berlin, LNCS 5228 (2008) pp. 128–136.

[51] W. Olaya-León and C. Granados-Pinzón, *Sobre la distancia mínima de códigos AG unipuntuales Castillo*, Revista Ingenieria y Ciencia, 8(16) (2012), pp. 239–255.

[52] W. Olaya-León and C. Granados-Pinzón, *The second generalized Hamming weight of certain Castle codes*. Aparecerá en: Designs, codes and cryptography, (2014). DOI: 10.1007/s10623-014-9981-1.

[53] W. Olaya-León and C. Munuera, *On the minimum distance of Castle codes*, Finite Fields and Applications, 20 (2013), pp. 55–63.

[54] W. Olaya-León and C. Munuera, *On the generalized Hamming Weights of Castle codes*, Preprint (2014).

[55] R. Pellikaan, *On special divisors and the two variable zeta function of algebraic curves over finite fields*. In Arithmetic, geometry and coding theory, de Gruyter, Berlin, (1996) pp. 175–184.

[56] J. C. Rosales and P.A. García-Sánchez, *Numerical semigroups*. Vol. 20 of Developments in mathematics, Springer, New York, 2009.

[57] C.E. Shannon, *A Mathematical Theory of Comunication*, Bell Systems Technical J., 27 (1947), pp. 656–715.

[58] T. Shibuya and K. Sakaniwa, *A dual of well-behaving type designed minimum distance*, IEICE Transactions Fundamentals, E84-A(2) (2001), pp. 647–652.

[59] H. Stichtenoth, *A note on Hermitian codes over* $\mathbb{F}_{q^2}$, IEEE Transactions on Information Theory, 34(5) (1988), pp. 1346–1348.

[60] H. Stichtenoth, *Algebraic Functions Fields and Codes*. Springer-Verlag, Berlin, 1993.

[61] M.A. Tsfasman, S.G. Vladuts and T. Zink, *Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound*, Mathematische Nachrichten, 109 (1982), pp. 21–28.

[62] K. Yang and P.V. Kumar, *On the true minimum distances of Hermitian codes*. In Coding Theory and Algebraic Geometry, LNCS 1518, pp. 99-107, Springer-Verlag, Berlin, 1992.

[63] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Transactions on Information Theory, 37(5) (1991) pp. 1412–1418.