CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS

DEL INSTITUTO POLITÉCNICO NACIONAL

Unidad Zacatenco

Departamento de Matemáticas

Pesos Generalizados de Códigos de Goppa

TESIS QUE PRESENTA

Juan Carlos Alberto López

PARA OBTENER EL GRADO DE

MAESTRO EN CIENCIAS

EN LA ESPECIALIDAD DE MATEMÁTICAS

Director de Tesis: Dr. José G. Martínez Bernal

Ciudad de México Febrero de 2020

Contenido

Dedicado a mi Madre y a mis Abuelos

Agradecimientos

Agradezco al Cinvestav por las facilidades otorgadas para el desarrollo de mi formación académica.

Agradezco al CONACyT por la beca otorgada durante mis estudios de maestría.

Resumen

El tema de interés en este trabajo son los códigos de Goppa, los cuales son códigos lineales que se construyen a partir de curvas algebraicas definidas sobre campos finitos. Entender los parámetros de este tipo de códigos ha sido un creciente tema de estudio desde su descubrimiento por Goppa allá por los años 70's. Aunque existen muchos resultados acerca de su distancia mínima, aún no se entiende adecuadamente este parámetro para dichos códigos, a pesar de que se ha determinado completamente para varias clases de curvas; ver capítulo 5. El objetivo principal en esta tesis es presentar los resultados más conocidos, no sólo para la distancia mínima, sino también para los pesos generalizados de estos códigos y de sus códigos duales; ver capítulos 4-6. En general, son pocos los resultados en esa dirección. Un caso importante, y completamente determinado, es el de las curvas hermitianas; que no se incluye en su totalidad en el trabajo porque es demasiado técnico, y sólo se da una referencia al final. Uno de los principales obstáculos para profundizar en el estudio y desarrollo de estos temas es que se requiere un conocimiento mucho más sólido de geometría algebraica, particularmente de la teoría de campos de funciones algebraicas.

Una breve descripción del contenido del trabajo es como sigue. En el capítulo 1 se describe un contexto introductorio para los códigos de Goppa. En el capítulo 2 se introducen los conceptos preliminares de la teoría de códigos lineales, particularmente sus parámetros fundamentales, a saber, longitud, dimensión y distancia mínima. En el capítulo 3 se dan los elementos necesarios sobre campos de funciones algebraicas para entender el espacio de Riemann asociado a un divisor, y concluir con el enunciado del Teorema de Riemann-Roch, el cuál es la herramienta más importante para calcular, entre otras cosas, la dimensión–como espacio vectorial–de dicho espacio de Riemann.

En el capítulo 4 se introducen los códigos de Goppa–también conocidos en la literatura como códigos geométrico algebraicos. Damos una descripción de los parámetros de estos códigos. El capítulo 5 se dedica a dar ejemplos donde se describe su distancia mínima para varias clases de curvas algebraicas. Finalmente, en el capítulo 6, se introduce el concepto de pesos generalizados de un código lineal y se enuncian algunos de los resultados conocidos sobre dichos pesos para el caso de códigos de Goppa.

Abstract

In this work we are interested in Goppa codes, which are linear codes constructed from algebraic curves over finite fields. The understanding of the parameters of these codes has been an increasing topic of study since its discovery by Goppa in the 70's. Since then, many results about its minimum distance have been obtained, however, there is no yet an adequate understanding of these parameters, even that they are well known for several classes of curves; see chapter 5. The aim in this thesis is to present very well known results, not only for the minimum distance, but also about generalized weights of these codes and their duals; see chapters 4-6. In general, there are just a few results in that direction. An important case, and completely known, is the one of hermitian curves; because it is so technical, it is not totally described, and just a reference is given at the end. One of the main obstacles for a deep study of these topics is that a stronger knowledge of algebraic geometry is needed, particularly of the theory of algebraic functions fields.

A brief description of the content of this work is as follows. Chapter 1 describes an introductory context for the Goppa codes. In chapter 2 the preliminary concepts of linear codes are introduced, particularly its fundamental parameters, namely, length, dimension and minimum distance. In chapter 3 are given the basic elements about algebraic functions fields to understand the Riemann space associated with a divisor, and then the Riemann-Roch Theorem is skethced out. This theorem is the main tool to compute, among other things, the dimension–as a vectorial space–of the Riemann space. Chapter 4 introduce Goppa codes, also known as algebraic geometric codes. The parameters of these codes are described. In chapter 5 examples are presented, where the minimum distance of several classes of algebraic curves is computed. Finally, in

chapter 6, the definition of generalized weights of a linear code is given and some known results about these weights are presented for the case of Goppa codes.

Chapter 1

Introducción

La segunda mitad del siglo pasado fue testigo de lo que podríamos llamar la gran revolución de la información digital. Uno de los motores principales de este proceso fue la matematización de la teoría de transmisión electrónica de datos, particularmente la enfocada a la detección y corrección de errores; ver el seminario de C.E. Shannon [16] y el artículo de R.W. Hamming [4], quienes fueron los principales fundadores de esta área. Después de estos inicios, los matemáticos comenzaron a tratar los problemas fundamentales de la teoría de códigos como preguntas matemáticas, sin preocuparse necesariamente por las aplicaciones. En la década de los 70's se realizaron importantes investigaciones sobre aspectos teóricos y prácticos de la teoría de códigos, y alrededor de ese tiempo se establecieron conexiones con la geometría, la combinatoria y la teoría de latices. Actualmente, la teoría de códigos se ha convertido en una rama importante del álgebra, con numerosas conexiones con otras ramas de la matemática, como la teoría de números, y con aplicaciones en teoría de la información y criptografía.

Según las características del canal de comunicación, la información se codifica de tal manera que el proceso de transmisión sea lo más rápido y fiable posible, dando asi lugar a diferentes tipos de códigos, que entre los más importantes tenemos a los códigos geométricos. Este tipo de códigos surgieron en el periodo de 1977-1982, cuando el matemático ruso Valery Denisovich Goppa descubrió una importante conexión entre la teoría de curvas algebraicas sobre campos finitos y la teoría de códigos. Esto creó un fuerte interés en el área debido a que los principales parámetros de estos códigos

tienen una interpretación en términos de la geometría de las curvas. Muchas de estas cuestiones acerca de curvas se remontan a la época de Gauss, por ejemplo, el problema de contar puntos sobre curvas había estado más o menos latente, pero nunca había sido un tema muy destacado de las matemáticas. Sin embargo, en tiempos recientes, se ha convertido en un tema central de investigación.

La idea para la construcción de códigos geométricos es similar a la de los códigos de Reed-Solomon, los cuales resultan de evaluar polinomios en una variable sobre campos finitos. Goppa extendió esta idea mediante el uso de funciones racionales definidas sobre una curva algebraica en lugar de polinomios. Este tipo de códigos se conocen como códigos geométrico algebraicos o códigos de Goppa.

Los códigos de Goppa se vuelven relevantes en los ochentas, debido a que Michael Tsfasman, Serge Vladut y Thomas Zink demuestran la existencia de familias infinitas de este tipo de códigos que mejoran diversas cotas relacionando la tasa de información y la distancia mínima relativa, entre ellas, específicamente, la cota asintótica de Gilbert-Varshamov [5, 8, 25], cuya demostración hace uso de la teoría de curvas modulares; ver [9] para una demostración. En consecuencia, se obtiene la solución a un problema fundamental de la teoría de códigos considerado por Shannon, planteado en términos probabilísticos, pero sin dar una idea de la construcción en aquél momento.

Por otra parte, los pesos generalizados–de Hamming– asociados a un código lineal se comportan de varias maneras como pesos mínimos de códigos. Estos pesos generalizados, que incluyen a la distancia mínima del código, satisfacen por ejemplo la cota de Singleton generalizada. Los pesos generalizados fueron introducidos en 1977 por Helleseth, Klove y por Mykkeltveit en [10]. Victor Wei los introdujo de manera independiente en [26] mientras trabajaba en un problema de criptografía. Demostró que el desempeño de un código empleado en un cierto tipo de canal de transmisión está determinado por sus pesos generalizados. Descubrió que los pesos generalizados tienen interesantes propiedades matemáticas, por ejemplo, generalizan la noción de distancia mínima de un código lineal y forman una sucesión estrictamente creciente de enteros positivos. Otra propiedad fundamental, también debida a Wei, es que los pesos generalizados de un código lineal determinan completamente a los pesos generalizados

de su código dual; este resultado se conoce como la dualidad de Wei. En términos de sistemas proyectivos, la noción de pesos generalizados fue descubierta por Tsfasman, en un intento de encontrar invariantes geométricos de sistemas proyectivos.

Chapter 2

Códigos lineales

2.1 Parámetros

Definición 2.1.1. Sea $\mathbb{F}_q$ un campo con q elementos. Un código lineal C es un subespacio vectorial de $\mathbb{F}_q^n$. Si C tiene dimensión k, entonces decimos que C es un código lineal con parámetros $[n, k]$, y nos referimos a C simplemente como un $[n, k]_q$-código. El campo $\mathbb{F}_q$ se llama el *alfabeto* del código, los elementos de $\mathbb{F}_q^n$ se llaman *palabras*–del alfabeto, y los elementos de C se llaman las *palabras código*.

Definición 2.1.2. En el espacio vectorial $\mathbb{F}_q^n$ está provisto de manera natural con la métrica $d(x, y) := |\{i : x_i \neq y_i\}|$, donde $x = (x_1, \ldots, x_n)$ y $y = (y_1, \ldots, y_n)$. Esta se llama la métrica o *distancia de Hamming*. El *peso de Hamming* de un vector $x \in \mathbb{F}_q^n$ es su distancia de Hamming al origen y se denota por $w(x)$. La *distancia mínima* del código se define como $d := \min\{w(x) : 0 \neq x \in C\}$. En general, calcular la distancia mínima de un código es un problema difícil, y a menudo tenemos que conformarnos con tener una estimación basada en algunas cotas disponibles.

Cuando un código lineal, definido sobre el campo $\mathbb{F}_q$, tiene longitud n, dimensión k y distancia mínima d, nos referimos a él como un $[n, k, d]_q$-código, o simplemente un $[n, k, d]$-código cuando no es necesario enfatizar el campo $\mathbb{F}_q$.

La siguiente relación entre los parámetros de un código se llama la cota de Singleton.

Proposición 2.1.3. *Los parámetros de un $[n, k, d]$-código satisfacen que $k + d \leq n + 1$.*

Prueba. Sea $V = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0, \forall i \geq d\}$. Así, $\dim V = d-1$ y $V \cap C = \emptyset$, por tanto $n = \dim \mathbb{F}_q^n \geq \dim(C + V) = \dim C + \dim V = k + d - 1$. ∎

Definición 2.1.4. A los códigos cuyos parámetros satisfacen la igualdad en la cota de Singleton se les llama códigos de *máxima distancia separable* o simplemente *códigos MDS*. Entonces los códigos MDS tienen la mayor distancia posible entre aquéllos de longitud n y dimensión k.

Definición 2.1.5. Una matriz $G \in \mathbb{F}_q^{k \times n}$ cuyos renglones forman una base del código C se llama una *matriz generadora* del código. En tal caso $C = \{xG : x \in \mathbb{F}_q^k\}$.

2.2 Código dual

Definición 2.2.1. El espacio vectorial $\mathbb{F}_q^n$ está provisto también, de manera natural, de un producto interno (i.e. una forma bilineal simétrica no-degenerada): Si $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$, entonces definimos $(a, b) := a_1 b_1 + \cdots + a_n b_n$. Cuando $(a, b) = 0$ decimos que a y b son *ortogonales*. Entonces podemos definir un complemento ortogonal en $\mathbb{F}_q^n$, lo que nos permite asociar con cada código C otro código $C^\perp$ llamado su *código dual*:

$$C^\perp := \{y \in \mathbb{F}_q^n : (x, y) = 0 \text{ para todo } x \in C\}.$$

Definición 2.2.2. Una matriz H de orden $n - k \times n$ que sea matriz generadora del código dual $C^\perp$ se llama una *matriz de chequeo de paridad* del código C.

Observe que el código C está determinado por la matriz de chequeo de paridad H:

$$C = \{x \in \mathbb{F}_q^n : Hx^T = 0\},$$

donde x^T denota la transpuesta de x.

Definición 2.2.3. Dos códigos C_1 y C_2 de longitud n se dicen equivalentes si existe una permutación $\sigma \in S_n$ tal que $C_1 = g_\sigma C_2$, donde g_σ es el automorfismo de $\mathbb{F}_q^n$ el cual envía $(x_1, \ldots, x_n)$ en $(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Códigos equivalentes tienen los mismos parámetros, así, se estudian códigos lineales salvo equivalencia.

Es bien conocido de álgebra lineal que el espacio dual de un $[n, k, d]$-código satisface que $(C^{\perp})^{\perp} = C$ y es un $[n, n-k, d^{\perp}]$-código; donde $d^{\perp}$ es la distancia mínima de $C^{\perp}$. En particular, la longitud n de un código autodual (i.e. $C^{\perp} = C$) es par y su dimensión es $n/2$. Claramente una matriz generadora de C es una matriz de chequeo de paridad de $C^{\perp}$. 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 la de su dual $C^{\perp}$.

Chapter 3

Campos de funciones

En este capítulo recordamos los elementos necesarios de geometría algebraica para poder enunciar el Teorema de Riemann-Roch, que se utilizará en el siguiente capítulo para estudiar los códigos de Goppa.

Un *campo de funciones* es una extensión de campos F/K finitamente generada de grado de trascendencia uno. La cerradura algebraica de K en F se llama el *campo de constantes* de la extensión. En lo que sigue supondremos que el campo de constantes es igual a K. Para más detalles y resultados referimos a [9, 17, 21]. Otra referencia útil para este capítulo y el siguiente será [23].

A lo largo del trabajo, por una *curva* entenderemos una curva proyectiva nosingular absolutamente irreducible; ver capítulo 4.

3.1 Divisores

Definición 3.1.1. Un *divisor* de una curva X es un elemento del grupo abeliano libre generado por los puntos de X, es decir, es una suma formal finita $D = \sum_{P \in X} n_P P$, donde $n_P \in \mathbb{Z}$ y $n_P = 0$ para casi todo punto $P \in X$. El conjunto de divisores de X se denota por $\mathrm{Div}(X)$. El *grado* de un divisor D es el entero $\deg(D) := \sum_{P \in X} n_P$.

Definición 3.1.2. Un divisor $\sum_P n_P P$ se dice efectivo en P si $n_P \geq 0$. Un divisor se dice *efectivo* si es efectivo en cada punto P; en tal caso escribimos $\sum_{P \in X} n_P P \geq 0$.

Denotamos por $\text{supp}(D)$ al *soporte* de un divisor D, es decir, el conjunto de puntos $P \in X$ tales que $n_P \neq 0$.

3.2 Divisores principales

En esta sección introducimos la noción de un divisor principal y hacemos notar que tienen grado cero. De esto se sigue que los divisores principales forman un subgrupo del grupo de divisores de grado cero $\text{Div}^0(X)$.

Para una curva X definida sobre un campo K, denotamos por F a su campo de funciones. Y si $P \in X$, entonces denotamos por $\text{ord}_P(\cdot)$ a la valuación discreta del campo de funciones F/K determinada por P.

Lema 3.2.1. [9, Lemma 2.1] *Si $f \in F^\times$, entonces $\text{ord}_P(f) = 0$ para casi todo $P \in X$.*

Definición 3.2.2. Se define el *divisor principal* de $f \in F^\times$ como $(f) := \sum_{P \in X} n_P P$, donde $n_P := \text{ord}_P(f)$. Definiendo el *divisor de ceros* y el *divisor de polos*, respectivamente, como:

$$(f)_0 := \sum_{n_P > 0} n_P P \qquad \text{y} \qquad (f)_\infty := \sum_{n_P < 0} (-n_P) P,$$

podemos escribir $(f) = (f)_0 - (f)_\infty$. Un divisor D de X se dice *principal* si $D = (f)$ para alguna función $f \in F^\times$.

Si $f, h \in F^\times$, entonces $(fh) = (f) + (h)$ y $(f^{-1}) = -(f)$. El conjunto de todos los divisores principales es un subgrupo del grupo de divisores de la curva.

Lema 3.2.3. [9, Lemma 2.2] *Si f es un elemento no constante de F, entonces*

$$\deg (f)_0 = \deg (f)_\infty = [F : K(f)].$$

Definición 3.2.4. Dos divisores D y D' de X se dicen *linealmente equivalentes*, escrito $D \sim D'$, si $D - D'$ es un divisor principal. La clase de equivalencia de un divisor D se denota por $[D]$. El grupo de todos los divisores de X de grado cero, $\text{Div}^0(X)$, módulo el subgrupo de divisores principales se llama el *grupo de clases de divisores* o el *grupo de Picard* de X.

3.3 Diferenciales

Sea F/K una extensión de campos, y con cada $x \in F$ asociamos el símbolo $[x]$. Sea E el F-módulo libre generado por todos los símbolos $[x]$ y sea N el submódulo de E generado por los elementos de la forma:

- $[x+y]-[x]-[y]$, $x, y \in F$;
- $[\lambda x]-\lambda[x]$, $x \in F$ y $\lambda \in K$;
- $[xy]-x[y]-y[x]$, $x, y \in F$.

El módulo cociente $\Omega_K(F) := E/N$ se llama el *módulo de diferenciales* de la extensión. La *diferencial* de $x \in F$, denotada por dx, es la clase lateral de $[x]$ en $\Omega_K(F)$.

Definición 3.3.1. Sea X una curva definida sobre el campo K. El *espacio de diferenciales* de X, denotado por $\Omega(X)$, se define como

$$\Omega(X) := \Omega_K(K(X)),$$

donde $K(X)$ es el campo de funciones de X.

Ahora establecemos algunos resultados sobre $\Omega(X)$.

Proposición 3.3.2. *Sean $P \in X$ y $t \in K(X)$ un parámetro uniformizante en P.*

(*i*) *$\Omega(X)$ es un $K(X)$-espacio vectorial de dimensión uno.*

(*ii*) *Si $f \in K(X)$, entonces df es una base para $\Omega(X)$ si y sólo si la extensión $K(X)/K(f)$ es finita y separable.*

(*iii*) *Para toda $\omega \in \Omega(X)$ existe una única función $g \in K(X)$, que depende de ω y t, tal que $\omega = gdt$. Esto permite definir $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(g)$.*

(*iv*) *Sea $f \in K(X)$ regular en P. Entonces df/dt es también regular en P; donde df/dt es el elemento tal que $df = (df/dt)dt$.*

(*v*) *Si $\omega \neq 0$, entonces para casi todo $P \in X$ se tiene que $\mathrm{ord}_P(\omega) = 0$.*

Prueba. Ver [17, Prop. 4.2-4.3]. ∎

3.4 Residuo de una diferencial

Sea X una curva sobre K, F su campo de funciones y $P \in X$. Recordemos que el punto P determina una valuación discreta $\nu_P := \mathrm{ord}_P(\cdot)$ en F. Esta valuación ν_P a su vez determina un valor absoluto del campo F, digamos $|\cdot|_{\nu_P}$. Bajo estas consideraciones podemos hablar de la completación del campo F respecto del valor absoluto $|\cdot|_{\nu_P}$, el cual denotamos como $\widehat{F}_P$. Todas estas afirmaciones y los resultados siguientes pueden consultarse, por ejemplo, en [21].

Teorema 3.4.1. *Sean X una curva, $P \in X$ un punto racional y t un parámetro uniformizante en P. Entonces se satisface*

(*i*) [21, Thm. 4.2.6] *Todo elemento $z \in \widehat{F}_P$ tiene una única representación de la forma*

$$z = \sum_{i=n}^{\infty} a_i t^i, \quad \text{con } n \in \mathbb{Z} \text{ y } a_i \in K;$$

(*ii*) [21, Thm. 4.2.7] *Si $z \in F$ tiene expansión $z = \sum_{i=n}^{\infty} a_i t^i$, entonces*

$$\frac{dz}{dt} = \sum_{i=n}^{\infty} i a_i t^{i-1}.$$

Con el fin de definir el residuo de una diferencial ω, enunciamos algunos resultados necesarios.

Definición 3.4.2. Sean X una curva, $P \in X$ un punto racional y t un parámetro uniformizante en P. Si $z \in F$ tiene una expansión $z = \sum_{i=n}^{\infty} a_i t^i$ en $\widehat{F}$, definimos el *residuo* de z, con respecto a P y t, como

$$\mathrm{res}_{P,t}(z) := a_{-1}.$$

Proposición 3.4.3. [21, Thm. 4.2.9] *Si $s, t \in F$ son parámetros uniformizantes en P, entonces $\mathrm{res}_{P,s}(z) = \mathrm{res}_{P,t}(z\frac{ds}{dt})$ para todo $z \in F$.*

Contamos ahora con los elementos para definir el residuo de una diferencial.

Definición 3.4.4. Sean X una curva, $P \in X$ un punto racional y $\omega \in \Omega(X)$. Por la Proposición 3.3.2(iii), escribimos $\omega = gdt$, donde t es un parámetro uniformizante en P y $g \in K(X)$. Definimos el *residuo* de ω en P como:

$$\mathrm{res}_P(\omega) := \mathrm{res}_{P,t}(g).$$

Esta definición no depende de la elección de t. En efecto, si s es otro parámetro uniformizante y $\omega = udt = zds$, entonces $u = z\frac{ds}{dt}$, y de la Proposición 3.4.3 se sigue que

$$\mathrm{res}_{P,s}(z) = \mathrm{res}_{P,t}(z\frac{ds}{dt}) = \mathrm{res}_{P,t}(u).$$

Teorema 3.4.5. (Teorema del Residuo) *Para cualquier $\omega \in \Omega(X)$ se tiene que*

$$\sum_{P \in X} \mathrm{res}_P(\omega) = 0.$$

Prueba. Ver [21, Cor. 4.3.3]. ∎

Definición 3.4.6. Sea $0 \neq \omega \in \Omega(X)$. El *divisor* de ω en $\mathrm{Div}(X)$ se define como

$$(\omega) := \sum_{P \in X} \nu_P(\omega) P.$$

Debido a la Proposición 3.3.2(iii) el divisor (ω) está bien definido. A las diferenciales $\omega \in \Omega(X)$ para las cuales $\nu_P(\omega) \geq 0$ para todo $P \in X$ se les llama *regulares*.

Definición 3.4.7. Un *divisor canónico* de X es cualquier elemento en la clase de equivalencia del divisor (ω).

Esta definición tiene sentido debido a la Proposición 3.3.2(i). Se deduce de que si $\omega_1, \omega_2 \in \Omega(X)$ son diferenciales no cero, entonces existe una función racional $f \in K(X)^\times$ tal que $\omega_2 = f\omega_1$ y por lo tanto $(\omega_2) = (\omega_1) + (f)$.

A cada divisor D en una curva X le asociamos el siguiente K-espacio vectorial, llamado el *espacio de Riemann* del divisor:

$$L(D) = \{f \in K(X)^\times : (f) + D \geq 0\} \cup \{0\}.$$

El caso en el cual D es el divisor canónico es de especial interés. Sea $W = (\omega) \in \mathrm{Div}(X)$ el divisor canónico de X, donde ω es alguna diferencial no cero. Por definición, cada $f \in L(W)$ satisface $(f\omega) = (f) + (\omega) \geq 0$. Esto quiere decir que

$$L(W) \simeq \{\omega \in \Omega(X) : \omega \text{ es regular}\}.$$

3.5 Género de un campo de funciones

Definición 3.5.1. El *género* de un campo de funciones F/K se define como

$$g := \sup\{\deg(D) - \dim L(D) + 1 : D \in \mathrm{Div}(F)\}.$$

Notar que esta definición es legítima (el supremo en cuestión existe) dado que la diferencia $\deg(D) - \dim L(D)$ está acotada superiormente; Teorema 3.5.3. Más algebraicamente,

$$g = \min\{[F : K(f)] : f \in F]\}.$$

Existe un entero c tal que $\dim L(D) = \deg(D) + 1 - g$ cuando $\dim L(D) \geq c$. De hecho, elegir un divisor $D' \in \mathrm{Div}(F)$ tal que $g = \deg(D') - \dim L(D') + 1$ y sea $c = \deg(D') + g$. Si $\deg(D) \geq c$, entonces $\dim L(D - D') \geq \deg(D - D') + 1 - g \geq c - \deg(D') + 1 - g \geq 1$, y de modo que existe un elemento no cero $z \in L(D - D')$. Considerar el divisor $D' = D + (z)$, el cual es $\geq D'$. Observamos que $\deg(D) - \dim L(D) = \deg(D') - \dim L(D') \geq \deg(D') - \dim L(D') = g - 1$. Luego $\dim L(D) \leq \deg(D) + 1 - g$, lo cual provee la igualdad deseada.

Con el fin de lograr nuestro segundo objetivo necesitamos primero algunos lemas técnicos, la mayoría de los cuales involucran la dimensión del espacio vectorial $L(D)$ asociado a un divisor. Empezamos con el siguiente.

Lema 3.5.2. *Sean D_1 y D_2 divisores de un campo de funciones F/K con $D_1 \leq D_2$. Entonces $L(D_1) \subseteq L(D_2)$ y $\dim L(D_2)/L(D_1) \leq \deg(D_2) - \deg(D_1)$.*

El teorema que buscamos ahora se puede obtener.

Teorema 3.5.3. *Todo campo de funciones tiene género finito. Más precisamente, existe una constante $c \in \mathbb{Z}$, que sólo depende de F/K, tal que* $\deg(D) - \dim L(D) \leq c$ *para todo* $D \in \mathrm{Div}(F)$.

3.6 Teorema de Riemann-Roch

Sean X una curva sobre K (denotado por X/K) y $f \in K(X)$ una función que es regular en todas partes, excepto en un punto $P \in X$. Si f tiene un polo de orden a lo más n en P, esto puede expresarse en términos de divisores como $(f) \geq -nP$. Similarmente, para $Q \in X$ y m un entero positivo, $(f) \geq mQ - nP$ expresa además que f tiene un cero en Q de orden al menos m. Este uso de los divisores es una herramienta muy útil para describir polos y ceros de funciones.

Definición 3.6.1. Sea D un divisor de la curva X/K. Definimos

$$L(D) := \{f \in K(X)^\times : (f) + D \geq 0\} \cup \{0\}.$$

Este es el espacio vectorial de funciones racionales de la curva cuyo divisor de polos está acotado por D. Se llama el espacio de Riemann del divisor D.

Es claro que $L(D)$ es un espacio vectorial y que a todos los divisores equivalentes les corresponden espacios vectoriales isomorfos: Para esta segunda afirmación, asumir que $D \sim D'$ y entonces hacer $\varphi : L(D) \to L(D')$ dada por $x \mapsto xz$, donde z es el elemento fijo de $K(X)$ tal que $D = D' + (z)$. Es bien conocido que $\dim L(D)$ es finito para todos los divisores D de F/K [21]. Esto está íntimamente conectado con el hecho de que el género de F/K, está en efecto bien definido y es finito. Además, si $\deg(D) < 0$, entonces $L(D) = \{0\}$.

Observe que si una curva está definida sobre K y dos divisores equivalentes $D \sim D'$ en X están definidos sobre K, entonces existe una función $f \in K(X)^\times$ tal que $D - D' = (f)$.

Ahora estamos listos para enunciar el resultado más importante de este capítulo.

Teorema 3.6.2. (Riemann-Roch)[21, Thm. 1.5.15] *Sean W un divisor canónico y g el*

género del campo de funciones F/K. Entonces para todo divisor $D \in \mathrm{Div}(F)$ se tiene que

$$\dim L(D) - \dim L(W - D) = \deg(D) + 1 - g.$$

Corolario 3.6.3. (i) $\dim L(W) = g$;

(ii) $\deg(W) = 2g - 2$;

(iii) *Si* $\deg(D) > 2g - 2$, *entonces* $\dim L(D) = \deg(D) + 1 - g$.

Prueba. (i) Hacer $D = 0$ y obervar que $L(0) = K$. (ii) Hacer $D = W$. (iii) En este caso $\deg(K - D) < 0$, luego $L(K - D) = 0$. Por tanto $\dim L(D) = \deg(D) + 1 - g$. ∎

Definición 3.6.4. Un divisor D se llama *especial* si $\dim L(W - D) > 0$ y no especial en otro caso. En el caso de que D sea especial, $\dim L(W - D)$ se llama el índice de especialización y se denota por $i(D)$. Observe que si $\deg(D) > 2g - 2$, entonces D no es especial.

Finalizamos con un resultado útil en el siguiente capítulo.

Teorema 3.6.5. (Clifford) *Sea D un divisor tal que $0 \leq \deg(D) \leq 2g - 2$. Entonces*

$$\dim L(D) \leq \frac{1}{2}\deg(D) + 1.$$

Prueba. Ver [21, Thm. 1.6.13]. ∎

El siguiente teorema es de utilidad para curvas que alcanzan su número máximo de puntos racionales, por ejemplo, las curvas hermitianas que se presentan más adelante.

Teorema 3.6.6. (Hasse-Weil) *Sea X una curva sobre $\mathbb{F}_q$ de género $g \geq 0$. El número $N := |X(\mathbb{F}_q)|$ satisface que*

$$|N - (q + 1)| \leq 2gq^{1/2}.$$

Prueba. Ver [21, Thm. 5.2.3]. ∎

Chapter 4

Códigos de Goppa

Sean $\mathbb{F}_q$ un campo finito con q elementos y X una curva proyectiva nosingular absolutamente irreducible de género g definida sobre $\mathbb{F}_q$. Recordemos lo que estos adjetivos significan. Como un objeto geométrico, X es una variedad proyectiva de dimensión 1.

La propiedad de nosingularidad significa que en cada punto de X está determinada una única dirección tangente. Esta es una condición que para una curva plana proyectiva puede checarse fácilmente.

La condición de absolutamente irreducible garantiza que la curva es conexa en un cierto sentido. En efecto, si X está definida por un polinomio homogéneo f en $\mathbb{F}_q[x, y, z]$, la irreducibilidad significa que f no es el producto de dos polinomios homogéneos no-constantes de menor grado. Absolutamente irreducible es una propiedad geométrica, lo que significa que f es irreducible sobre cualquier extensión finita de $\mathbb{F}_q$, i.e. la curva X, cuando es vista sobre la cerradura algebraica de $\mathbb{F}_q$ no es una unión disjunta de otras dos curvas. En términos prácticos, cuando X está definida por la curva afin $f(x, y) = 0$, absolutamente irreducible implica que el anillo de coordenadas $\mathbb{F}_q[x, y]/(f)$ es un dominio entero y permanece así cuando el campo es remplazado por cualquier extensión finita. Esto a su vez garantiza que el campo de fracciones tiene grado de trascendencia igual a 1.

El género g de X es una medida de la complejidad de la curva X con respecto a la línea proyectiva.

4.1 Construcción

En esta sección explicamos como construir códigos lineales a partir de curvas algebraicas, siguiendo las ideas básicas de V.D. Goppa, quien los introdujo en 1981.

Sea X una curva. Sean $P_1, \ldots, P_n$ distintos puntos $\mathbb{F}_q$-racionales de la curva X, D el divisor $P_1 + \cdots + P_n$ y G otro divisor de X definido sobre $\mathbb{F}_q$ y disjunto de D. En particular, los P_i no son polos de las funciones $f \in L(G)$.

Definición 4.1.1. El código *geométrico algebraico* o *código de Goppa* $C(X, D, G)$ es la imagen del mapeo evaluación

$$\alpha : L(G) \to \mathbb{F}_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)).$$

Ahora se estiman los parámetros del código de Goppa. Su longitud es claramente n y los otros parámetros se dan en el siguiente resultado.

Teorema 4.1.2. *Los parámetros* $[n, k, d]$ *del código* $C(X, D, G)$ *satisfacen*

(*i*) $k = \dim L(G) - \dim L(G - D)$.

En particular, si $\deg(G) < n$, *entonces* $k = \dim L(G)$.

Por otra parte, si $2g - 2 < \deg(G)$, *entonces* $k = \deg(G) + 1 - g$.

(*ii*) $d \geq n - \deg(G)$.

Prueba. (i) Sea $f \in \ker \alpha$. Por tanto f se anula en $P_1, \ldots, P_n$. Como $P_1, \ldots, P_n \notin \operatorname{supp}(G)$, $f \in L(G - D)$. Si $n > \deg(G)$, $L(G - D) = 0$; por tanto α es inyectivo y $k = \dim L(G)$. Por otra parte, si $2g - 2 < \deg(G)$, entonces $k = \deg(G) + 1 - g$, por el Teorema de Riemann-Roch.

(ii) Si d es la distancia mínima del código, entonces existe $f \in L(G)$ tal que $\alpha(f)$ tiene peso $d > 0$. Suponga $f(P_i) \neq 0$ para $i = 1, \ldots, d$ y $f(P_i) = 0$ para $i = d+1, \ldots, n$. Así, $f \in L(G - P_{d+1} - \cdots - P_n)$. Como $f \neq 0$, $\deg(G) - (n-d) = \deg(G - P_{d+1} - \cdots - P_n) \geq 0$, así, $d \geq n - \deg(G)$. ∎

Corolario 4.1.3. *Sean* $C = C(X, D, G)$ *un código de Goppa con* $\deg(G) < n$ *y* $\{f_1, \ldots, f_k\}$ *una base del espacio* $L(G)$ *sobre* $\mathbb{F}_q$. *Entonces* $\{\alpha(f_1), \ldots, \alpha(f_k)\}$ *es una base de* C. *En particular, la matriz*

$$\begin{bmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{bmatrix},$$

es una matriz generadora para C.

Definición 4.1.4. El entero $d_C := n - \deg(C)$ se llama la *distancia de diseño* del código $C(X, D, G)$.

El Teorema 4.1.2 establece que la distancia mínima d de un código $C(X, D, G)$ es mayor o igual que su distancia de diseño. La pregunta de cuándo se tiene la igualdad la responde la siguiente proposición.

Proposición 4.1.5. *Supongamos que* $\dim L(G) > 0$ *y* $d_C = n - \deg(G) > 0$. *Entonces* $d = d_C$ *si y sólo si existe un divisor* D' *con* $0 \leq D' \leq D$, *tal que* $\deg(D') = \deg(G)$ *y* $\dim L(G - D') > 0$.

Prueba. Supongamos primero que $d_C = d$. Entonces existe $0 \neq f \in L(G)$ tal que la palabra código $(f(P_1), \ldots, f(P_n)) \in C(X, D, G)$ tiene precisamente $n - d = n - d_C = \deg(G)$ componentes igual a cero, digamos que $f(P_{i_j}) = 0$ para $j = 1, \ldots, \deg(G)$. Sea $D' := \sum_{j=1}^{\deg(G)} P_{i_j}$. Entonces $0 \leq D' \leq D$, $\deg(D') = \deg(G)$ y $\dim L(G - D') > 0$ (ya que $f \in L(G - D')$). Conversamente, si D' tiene las propiedades citadas, entonces elegimos un elemento $0 \neq f \in L(G - D')$. El peso de la correspondiente palabra código $(f(P_1), \ldots, f(P_n))$ es $n - \deg(G) = d_C$, lo que implica que $d = d_C$. ∎

Ejemplo 4.1.6. Sea X una curva elíptica sobre $\mathbb{F}_q$. Sean $P_1, \ldots, P_n$ puntos $\mathbb{F}_q$-racionales en X y sea $D := P_1 + \cdots + P_n$. Para elegir un código específico tenemos que elegir un divisor G que tenga soporte disjunto de D. Una posible elección para el divisor G es $G = mQ$, donde $Q = (0 : 1 : 0)$ es el punto al infinito en X y $0 < m < n$. Como X tiene género $g = 1$, el código tiene parámetros $[n, m, d]$ con $d \geq n - m$.

4.2 Código dual

En esta sección se define el código $C^*(X, D, G)$, llamado el código de Goppa dual asociado a la terna (X, D, G).

Continuamos con la notación anterior. Denotamos por $\Omega(X)$ al conjunto de diferenciales de X, y dado un divisor $E \in \mathrm{Div}(X)$, definimos

$$\Omega_X(E) := \{\omega \in \Omega(X)^\times : (\omega) \geq E\}.$$

Este es un espacio vectorial de dimensión finita, denotada por $i(A)$, y le hemos llamado el *índice de especialidad* de A, sobre $\mathbb{F}_q$. En lo que sigue, W es el divisor canónico para X, $W = (\omega)$ con $\omega \in \Omega_X(E)$. Claramente, si elegimos una diferencial ω' diferente, entonces $\omega' = f\omega$ para algún $f \in \mathbb{F}_q(X)$, por tanto $(\omega') \sim W$.

Definición 4.2.1. El *código de Goppa dual* $C^*(X, D, G)$ es la imagen de la aplicación $\mathbb{F}_q$-lineal

$$\alpha^* : \Omega_X(G - D) \to \mathbb{F}_q^n, \quad \eta \mapsto (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta)),$$

donde $\mathrm{res}_{P_i}(\eta)$ es el residuo de η en el punto P_i.

Observación 4.2.2. Se puede verificar que si $E \in \mathrm{Div}(X)$, entonces la aplicación $L(W - E) \to \Omega_X(E)$, $f \mapsto f\omega$ es una biyección. Por lo tanto, equivalentemente, $C^*(X, D, G)$ es la imagen de

$$\beta^* : L(W + D - G) \to \mathbb{F}_q^n, \quad f \mapsto (\mathrm{res}_{P_1}(f\eta), \ldots, \mathrm{res}_{P_n}(f\eta)).$$

Teorema 4.2.3. *Sean X, D y G como antes, y sean k^* y d^* la dimensión y distancia mínima, respectivamente, del código $C^*(X, D, G)$.*

(*i*) $k^* = \dim L(W + D - G) - \dim L(W - G)$.

En particular, si $\deg(G) > 2g - 2$, *entonces* $k^* = \dim L(W + D - G)$.

Por otra parte, si $\deg(G) < n$, *entonces* $k^* = n - (\deg(G) + 1 - g)$.

(*ii*) $d^* \geq \deg(G) - (2g - 2)$.

Prueba. (i) El kernel de β^* es $L(W-G)$. Si $\deg(G) > 2g-2$, entonces β^* es inyectivo. La última afirmación se sigue del Teorema de Riemann-Roch.

(ii) Análogamente como en el Teorema 4.1.2, consideremos una palabra código de peso d^* y observe que, salvo reordenamiento de $P_1, \ldots, P_n$, este código es igual a $\alpha^*(\eta)$ para un elemento no cero $\eta \in \Omega_X(G - (P_1 + \cdots + P_d))$. Por otro lado,

$$\dim \Omega_X(G - (P_1 + \cdots + P_d)) = \dim L(W - G + P_1 + \cdots + P_n) \geq 1,$$

y concluimos que el grado de tal divisor es mayor o igual a 1. ∎

Por lo visto hasta ahora, es claro que para calcular más fácilmente los parámetros del código y tener una distancia positiva, es mejor elegir los divisores D y G de modo que $2g - 2 < \deg(G) < \deg(D)$.

Teorema 4.2.4. *Los códigos $C(X, D, G)$ y $C^*(X, D, G)$ son duales uno del otro.*

Prueba. Veamos primero la inclusión $C^*(X, D, G) \subseteq C(X, D, G)^\perp$. Sean $\eta \in \Omega_X(G - D)$ y $f \in L(G)$. Mostramos que $\alpha(f) \circ \alpha^*(\eta) = 0$. Pero $\alpha(f) \circ \alpha^*(\eta) = \sum_{i=1}^n f(P_i) res_{P_i}(\eta)$. Observe que la diferencial $f\eta$, perteneciente a $\Omega_X(-D)$, puede tener polos simples sólo en el soporte de D. Por lo tanto, $\Sigma_{P \in X} res_P(f\eta) = \sum_{i=1}^n res_{P_i}(f\eta) = \sum_{i=1}^n f(P_i) res_{P_i}(\eta)$. Concluimos, por el teorema del residuo, que $\alpha(f) \circ \alpha(\eta) = 0$. Además, sabemos que

$$\dim C(X, D, G)^\perp = n - k = n - \dim L(G) + \dim L(G - D)$$

$$= \dim L(W + D - G) - \dim L(W - G) = k^*.$$

Así que $C^*(X, D, G) = C(X, D, G)^\perp$. ∎

El siguiente resultado muestra que cada código de Goppa dual se puede obtener como un código de Goppa, y viceversa.

Lema 4.2.5. *Existe una diferencial, ω, con polos simples y residuos igual a 1 en los polos del soporte de D y tal que $C^*(X, D, G) = C(X, D, W + D - G)$, donde $W = (\omega)$.*

Prueba. Elejir $\eta \in \Omega(X)$ y $f \in \mathbb{F}_q(X)$ tales que $\mathrm{ord}_{P_i}(f) = -(\mathrm{ord}_{P_i}(\eta) + 1)$. La función $f\eta$ tiene polos simples en $P_1, \ldots, P_n$. Podemos multiplicar $f\eta$ con una función

racional para obtener residuos iguales a 1 en todos los polos simples. Sea ω teniendo tales propiedades y sea $W = (\omega)$. Para todo $f \in L(W+D-G)$ se tiene que $\text{res}_{p_i}(f\omega) = f(P_i)\text{res}_{P_i}(\omega) = f(P_i)$. Entonces $\alpha(f) = \beta^*(f)$ y así tenemos $C(X, D, W + D - G) = C^*(X, D, G)$. ∎

En la Definición 2.2.3 dijimos que dos códigos son equivalentes si difieren por una permutación fija de las coordenadas. Ahora damos una nueva relación de equivalencia entre códigos, de modo que refleje la relación de equivalencia entre los divisores de la curva. A partir de ahora, cuando hablemos de códigos equivalentes, nos referimos a equivalentes de acuerdo con la siguiente definición.

Definición 4.2.6. Dos códigos no triviales C_1 y C_2, de longitud n, sobre $\mathbb{F}_q$, se dicen equivalentes si existe $\gamma \in \mathbb{F}_q^n$ tal que $C_2 = \gamma C_1$.

Es claro que la dimensión y los pesos de un código no cambian si multiplicamos por un elemento $0 \neq \gamma \in \mathbb{F}_q^n$. Así, estudiaremos las propiedades de un código salvo equivalencia.

Lema 4.2.7. *Sea $D = \sum_{i=1}^n P_i$ como antes, y sean $G, G' \in \text{Div}(X)$ cuyos soportes son disjuntos de $\text{supp}(D)$, $g(P_i) \neq 0$, la multiplicación con g es un isomorfismo entre $L(G)$ y $L(G')$, y entre $\Omega_X(G-D)$ y $\Omega_X(G'-D)$. Por lo tanto, $C(X, D, G) = \gamma C(X, D, G')$ y $C^*(X, D, G) = \gamma C(X, D, G')$, donde $\gamma = (g(P_1), \ldots, g(P_n))$.*

Prueba. Inmediato a partir del Teorema 4.1.2 y de los Lemas 4.2.5 y 4.2.7. ∎

El siguiente teorema da una condición equivalente para la existencia de un divisor G tal que $2G \sim W + D$.

Teorema 4.2.8. (Weil) *Existe un divisor G tal que $2G \sim W + D$ si y sólo si D es un cuadrado en el grupo de Picard $\text{Pic}(X)$.*

El siguiente objetivo es mostrar que $C^*(X, D, G)$ puede verse como $C(X, D, H)$ para un divisor apropiado H. El siguiente lema es un paso en esa dirección.

Lema 4.2.9. *Si existe $\eta \in \Omega(X)$ con polos simples y residuos iguales a 1 en los polos del soporte de D y tal que $2G \sim K + D$ para $K = (\eta)$, entonces $C(X, D, G)$ es autodual.*

Prueba. Sean ω y W como en el Lema 4.2.5. Se tiene $\eta = f\omega$ par alguna función racional no-cero f. Así, $K + D - G \sim W + D - G$ y, por la demostración del lema anterior, $C(X, D, K+D-G) = \gamma C(X, D, W+D-G)$, con $\gamma = (f(P_1), \ldots, f(P_n))$. Pero $f(P_i) = \mathrm{res}_{P_i}(\eta)/\mathrm{res}_{P_i}(\omega) = 1$, así, $C(X, D, G) = C(X, D, K + D - G) = C(X, D, W + D - G) = C^*(X, D, G) = C(X, D, G)^{\perp}$. ∎

Ahora investigamos la relación entre los parámetros de los códigos de Goppa.

Lema 4.2.10. *Sean $2g - 2 < \deg(G) < n$, d y d^* la distancia mínima de $C(X, D, G)$ y $C^*(X, D, G)$ respectivamente. Entonces*

(*i*) $n - \deg(G) \leq d \leq n - \deg(G) + g$;

(*ii*) $\deg(G) - (2g - 2) \leq d^* \leq \deg(G) - g + 2$.

Prueba. Las cotas inferiores son demostradas en los Lemas 4.2.5 y 4.2.7, y las cotas superiores se siguen de la cota de Singleton. ∎

Corolario 4.2.11. *Sean $2g - 2 < \deg(G) < n$. Si $g = 0$, entonces los códigos $C(X, D, G)$ y $C^*(X, D, G)$ son MDS.*

Nos gustaría ver la distancia mínima de un código como una propiedad geométrica de los divisores D y G. Siguiendo lo que se hizo en la demostración del Teorema 4.1.2, observemos que $x \in C(X, D, G)$ tiene peso $r > 0$ si $x = \alpha(f)$, con f diferente de 0 en r puntos de $\{P_1, \ldots, P_n\}$ y anularse en $n-r$ puntos. Así, $f \in L(G - P_{i(r+1)} - \cdots - P_{i(n)})$ para algún $i \in S_n$. Se deduce que existe un divisor $D' \leq D$ de grado $n - r$ tal que $L(G - D) \neq 0$. En cuyo caso, podemos suponer que α es inyectivo, i.e. $\deg(G) < n$. Si existe $D' \leq D$ con $\deg(D') = n - d$, entonces existe una palabra no cero de peso $\leq d$ en $C(X, D, G)$. Así, la distancia mínima de $C(X, D, G)$ es el menor entero d tal que existe un divisor $D' \leq D$ con $L(G - D') \neq 0$. Por lo tanto, la distancia mínima de un código puede obtenerse considerando algunos subespacios de $L(G)$.

Análogamente, si $\deg(G) \geq 2g - 2$, la distancia mínima de $C^*(X, D, G)$ es el menor entero d^* tal que existe un divisor $D' \leq D$ de grado d^*, con $L(W + D' - G) \neq 0$. Podemos enunciarlo de la siguiente manera: $x \in C^*(X, D, G)$ tiene peso $r > 0$ si

$x = \beta^*(f)$ para algún $f \in L(W + D - G)$ tal que $f\omega$ tiene residuo no cero en r puntos de $\{P_1, \ldots, P_n\}$ y residuo cero en los puntos restances. Entonces $f\omega$ es regular en $n - r$ puntos y $(f\omega) + \sum_{j=1}^{r} P_{i(j)} + G = E$, donde E es un divisor efectivo con soporte disjunto de $\{P_{i(1)}, \ldots, P_{i(r)}\}$. Así, $G - W \sim -\sum_{j=1}^{r} P_{i(j)} + E$. Recíprocamente, si se da la última igualdad, entonces $C^*(X, D, G)$ tiene una palabra de peso r. En resumen, se ha obtenido el siguiente resultado.

Teorema 4.2.12. *La distancia mínima d^* del código $C^*(X, D, G)$ es el menor número de puntos distintos $P_{i(1)}, \ldots, P_{i(d^*)}$ en el soporte de D tal que, en* $\mathrm{Pic}(X)$*, se tiene que $G - W = \sum_{j=1}^{d^*} P_{i(j)} - E$ para cualquier divisor efectivo E con soporte disjunto de $\{P_{i(1)}, \ldots, P_{i(d^*)}\}$.*

Argumentando de esta manera podemos calcular la distribución de pesos; de hecho, el número de palabras código con peso igual a r es igual a $(q - 1)$-veces el número de divisores $D' \leq D$ de grado r linealmente equivalentes a un divisor de la forma $G - W + E$ para algún $E \in L(0)$, con $\mathrm{supp}(D') \cap \mathrm{supp}(E) = \emptyset$.

4.3 Códigos de Reed-Solomon

En esta Sección describimos los códigos de Goppa asociados con un campo de funciones racionales. Este tipo de códigos se conocen como códigos de *Reed-Solomon*. Algunos de los códigos más importantes usados en la práctica pueden obtenerse de manera natural mediante este tipo de códigos.

En los años sesenta, I. Reed y G. Solomon publicaron un artículo de alrededor de cinco páginas bajo el poco ostentoso título "Polynomial codes over certain finite fields"; ver [15]. Su artículo describe una nueva clase de códigos que ahora son conocidos como códigos de Reed-Solomon. En las décadas posteriores a su descubrimiento, los códigos de Reed-Solomon han disfrutado de diversas aplicaciones; ver [27].

Ejemplo 4.3.1. Sean $\mathbb{F}_q$ un campo finito y $n = q - 1$. Sea $\beta \in \mathbb{F}_q$ un elemento primitivo. Para un entero $1 \leq k \leq n$, considere el espacio vectorial de dimensión k,

$$L_k := \{f \in \mathbb{F}_q[T] : \deg(f) \leq k - 1\},$$

y el mapeo evaluación

$$\text{ev} : L_k \to \mathbb{F}_q^n, \quad f \mapsto (f(\beta), \ldots, f(\beta^n)).$$

El mapeo "ev" es $\mathbb{F}_q$-lineal e inyectivo, ya que un polinomio $f \in L_k$ tiene a lo más $k-1$ raíces. Por lo tanto, $C_k := \{\text{ev}(f) : f \in L_k\}$ es un $[n,k]$-código sobre $\mathbb{F}_q$; los códigos obtenidos de esta forma se llaman *códigos de Reed-Solomon*. El peso de una palabra $0 \neq c = \text{ev}(f) \in C_k$ satisface

$$w(c) = |\{i : f(\beta^i) \neq 0\}| = n - |\{i : f(\beta^i) = 0\}| \geq n - \deg(f) \geq n - (k-1).$$

Por lo tanto, la distancia mínima d del código C_k satisface la desigualdad $d \geq n+1-k$. Pero por otro lado, por la cota de Singleton, $d \leq n+1-k$, asi que $d = n+1-k$.

El ejemplo anterior sirve de motivación para el siguiente resultado.

Definición 4.3.2. Sean $X = \mathbb{P}_{\overline{\mathbb{F}}_q}$, i.e. la línea proyectiva sobre $\overline{\mathbb{F}}_q$. Un código de Goppa $C(X, D, G)$, se dice que es un código racional sobre $\mathbb{F}_q$; donde $D = P_1 + \cdots + P_n$, con los P_i puntos $\mathbb{F}_q$-racionales distintos y $\text{supp}(G) \cap \text{supp}(D) = \emptyset$.

Observación 4.3.3. El término en la definición anterior proviene de una equivalencia bien conocida entre curvas y campos de funciones en una variable. Para la línea proyectiva $X = \mathbb{P}_{\overline{\mathbb{F}}_q}$ se tiene asociado su campo de funciones $\overline{\mathbb{F}}_q(X)$, el cual es un campo de funciones racionales en una variable (i.e. el campo de fracciones de un anillo de polinomios).

Hay que notar que la longitud de un código racional es a lo más $q+1$, en particular, si se trabaja con el campo $\mathbb{F}_2$, podemos tener códigos de longitud ≤ 3. Lo anterior se debe a que $X = \mathbb{P}_{\overline{\mathbb{F}}_q}$ tiene sólo $q+1$ puntos $\mathbb{F}_q$-racionales: los puntos finitos se corresponden en términos de anillos de valuación discreta con $\mathbb{F}_q[T]_{(T-a)}$, con $a \in \mathbb{F}_q$, y el punto al infinito, P_∞, con el anillo $\mathbb{F}_q[T^{-1}]_{(T^{-1})}$.

El siguiente resultado es una consecuencia inmediata del Teorema 4.1.2.

Proposición 4.3.4. *Sean $C(X, D, G)$ un código racional sobre $\mathbb{F}_q$, y n, k, d los parámetros del código. Entonces se tiene*

(*i*) $n \leq q+1$;

(*ii*) $k = 0$ *si y sólo si* $\deg(G) < 0$, *y* $k = n$ *si y sólo si* $\deg(G) > n-2$;

(*iii*) *Para* $0 \leq \deg(G) \leq n-2$, $k = \deg(G)+1$, *y* $d = n - \deg(g)$;

(*iv*) $C^{\perp}$ *es también un código racional.*

Prueba. La parte (*iv*) se deduce del Lema 4.2.5 ∎

4.4 Códigos de Reed-Solomon generalizados

Ahora se extiende la definición de códigos de Reed-Solomon, después se ve que estos son casos especiales de códigos racionales.

Definición 4.4.1. Sea $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ con los α_i distintos, y sea $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ con los v_i no-cero. El *código de Reed-Solomon generalizado* se define como el conjunto de todos los vectores

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in \mathbb{F}_q^n,$$

con $f \in \mathbb{F}_q[T]$ y $\deg(f) \leq k-1$ (para un entero fijo $k \leq n$); este código se denota como $GRS_k(\alpha, v)$.

Observación 4.4.2. Notar que en la definición anterior se pide que los α_i sean distintos, lo que implica que $n \leq q$.

Si $\alpha = (\beta, \ldots, \beta^n)$ y $v = (1, \ldots, 1)$, entonces $GRS_k(\alpha, v)$ es el código del Ejemplo 4.3.1. Obviamente, los códigos $GRS_k(\alpha, v)$ son $[n, k, n-k+1]$ códigos, para obtener la distancia mínima se procede como en el Ejemplo 4.3.1. El siguiente resultado muestra que los códigos de Reed-Solomon generalizados provienen de la geometría algebraica.

Proposición 4.4.3. *Todo código de Reed-Solomon generalizado es un código racional.*

Prueba. Sea $GRS_k(\alpha, v)$ un código con $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $v = (v_1, \ldots, v_n)$. Primero veamos el caso $n = q-1$ y $\alpha_i \neq 0$ para todo i. Sea $G = kP_\infty$ con $k \leq n$ y sea P_i un

punto finito ($i = 1, \ldots, n$) correspondiente a α_i. Sea D el divisor $P_1 + \cdots + P_n$. Entonces $L(G) = \{f \in \mathbb{F}_q[T] : \deg(f) < k\}$, y reordenando los puntos P_i, si es necesario, se tiene que

$$C(X, D, G) = \{(f(P_1), \ldots, f(P_n)) : f \in L(G)\} = \{(f(\beta), \ldots, f(\beta^n)) : f \in L(G)\},$$

con β un elemento primitivo de $\mathbb{F}_q$; éste es el código de Reed-Solomon. Para el caso general, sea $g \in \mathbb{F}_q[T]$ un polinomio tal que $g(P_i) = v_i$ (este polinomio existe por interpolación de Lagrange). Considere el divisor $G = nP_\infty - \mathrm{div}(g)$. El soporte de G es disjunto del soporte del divisor $D = P_1 + \cdots + P_n$. Como cada v_i es no cero, entonces ningún P_i es cero (o polo) de g. Por otra parte, $L(G) = gL(nP_\infty)$. Así, para $f \in L(nP_\infty)$ se tiene que $gf \in L(G)$, y entonces

$$(gf(P_1), \ldots, gf(P_n)) = (v_1 f(P_1), \ldots, v_n f(P_n)),$$

lo que demuestra que $C(X, D, G) = GRS_k(\alpha, v)$. ∎

Observación 4.4.4. Para un código racional $C(X, D, G)$ sobre $\mathbb{F}_q$, con longitud $n \leq q$, es posible demostrar que $C(X, D, G)$ es un código de Reed-Solomon generalizado.

Chapter 5

Diversos tipos de curvas

5.1 Curvas de género cero

En esta sección vemos como son los códigos de género cero, es decir, códigos sobre curvas de género cero. Aquí K es un campo perfecto, por ejemplo, un campo finito o un campo algebraicamente cerrado.

Lema 5.1.1. *Si la curva X es isomorfa a $\mathbb{P}^1$, entonces para todo divisor efectivo D de la curva se tiene que* $\dim L(D) = \deg(D) + 1$.

Teorema 5.1.2. *Sea X una curva con al menos un punto racional. Entonces X tiene género* 0 *si y sólo si es isomorfa a $\mathbb{P}^1$.*

Prueba. Toda curva isomorfa a $\mathbb{P}^1$ tiene género 0: esto se deduce del lema anterior y del Teorema de Riemann-Roch, tomando a D como un punto racional. Recíprocamente, sea X/K una curva de género 0 y P un punto racional. Por el Corolario 3.6.3(iii) se tiene que

$$\dim L(P) = \deg(P) + 1 - g = 1 + 1 - 0 = 2.$$

Existe por tanto una función racional no constante f en $L(P)$ tal que $(f) + P \geq 0$, i.e. f tiene un polo simple en P y no tiene ningún otro polo. Como P es efectivo y $\deg(P) = 1$, entonces la desigualdad $(f) + P \geq 0$ es válida sólo si $(f)_\infty = P$. Por lo tanto, f da un morfismo de grado 1 de X a $\mathbb{P}^1$, definido sobre K, ya que $f \in K(X)$, y este es un isomorfismo debido a [17, Cor. 2.4.1]. ∎

Recordemos que en la Definición 4.1.1 la aplicación

$$\alpha : L(G) \to \mathbb{F}_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n))$$

es inyectiva si $\deg(G) < n$ y la imagen de α define un $[n, k, d]$-código X. Por el Teorema 4.1.2, sus parámetros satisfacen la desigualdad $k + d \geq n + 1 - g$. Notemos que la desigualdad anterior se parece mucho a la cota de Singleton. Comparando ambas desigualdades vemos que para $\deg(G) < n$,

$$n + 1 - g \leq k + d \leq n + 1. \tag{5.1}$$

Si X es una curva de género 0, entonces $k + d = n + 1$, i.e. el código asociado es MDS. Ahora bien, según el teorema anterior, las curvas de género 0 son todas isomorfas a la línea proyectiva $\mathbb{P}^1$. Por lo que, en resumen, todos los códigos sobre curvas X de género 0 son racionales y de tipo MDS.

Ejemplo 5.1.3. Considere la curva $\mathbb{X}$ sobre $\mathbb{F}_7$: $f = X^2 - YZ = 0$. Esta curva es nosingular de género 0 y sus puntos racionales son $P_j = (j : j^2 : 1)$ con $j = 0, 1, \ldots, 6$ y $Q = (0 : 1 : 0)$. Sean $x = X/Z$ y $L(mQ)$ el espacio vectorial cuya base viene dada por las funciones x^i con $i = 0, 1, \ldots, m$. Sea $D = P_0 + \cdots + P_6$. La matriz de chequeo de paridad para el código $C^*(\mathbb{X}, D, mQ)$ está dada por

$$\begin{bmatrix} 1 & \cdots & 1 \\ x(P_0) & \cdots & x(P_6) \\ \vdots & & \vdots \\ x^m(P_0) & \cdots & x^m(P_6) \end{bmatrix},$$

y al evaluar las funciones en los puntos se tiene

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 6 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1^m & 2^m & \cdots & 6^m \end{bmatrix}.$$

El Teorema 4.2.3 nos da la dimensión del código $C^*(\mathbb{X}, D, mQ)$: $k^* = 7 - \deg(G) - 1 + 0 = 7 - m - 1 = 6 - m$, así que $m \leq 6$; y el Lema 4.2.10 nos da la distancia mínima $d^* = \deg(G) - g + 1 = m + 2$. En particular, si $m = 3$, entonces $d^* = 5$.

5.2 Curvas elípticas

En esta sección consideramos códigos de género uno, es decir, cuando la curva es una curva elíptica. Este tipo de curvas provee una familia infinita de códigos con buenos parámetros.

Definición 5.2.1. Una curva elíptica sobre un campo K es un par (X, O), donde X es una curva proyectiva nosingular de género uno y O es un punto racional de X.

Iniciamos discutiendo la relación entre la distancia mínima de un código de género uno y el grupo de puntos racionales de la curva elíptica.

En la Eq. (5.1) se llegó a la desigualdad: $n + 1 - g \leq k + d \leq n + 1$. Si X es una curva elíptica sobre $\mathbb{F}_q$, tenemos sólo dos opciones para la distancia mínima del código $C(X, D, G)$: $d = n - k$ o bien $d = n - k + 1$.

Fijamos alguna notación para esta sección:

- $X/\mathbb{F}_q$ es una curva elíptica;
- $X(\mathbb{F}_q)$ es el conjunto de puntos $\mathbb{F}_q$ racionales de X;
- $D = \{P_1, \ldots, P_n\}$ es un subconjunto de puntos racionales de $X(\mathbb{F}_q)$;
- G es un divisor de grado k, con $2g - 2 < k < n$ y $\text{supp}(G) \cap D = \emptyset$.

Sean G un grupo abeliano con elemento cero O y D un subconjunto finito de G, para un entero $0 < k < n$ y un elemento $b \in G$, denotamos (cf. [7])

$$N_G(k, b, D) = |\{S \subseteq D : |S| = k, b = \sum_{x \in S} x\}|.$$

Sea X una curva elíptica definida sobre $\mathbb{F}_q$ con un punto racional O. El conjunto de puntos racionales $X(\mathbb{F}_q)$ forman un grupo abeliano con elemento cero O, y es isomorfo al grupo de Picard $\text{Div}^0(X)/P(X)$, donde $P(X)$ es el grupo de divisores principales. Denotamos por $\oplus$ a la suma en el grupo $X(\mathbb{F}_q)$.

Proposición 5.2.2. *Sean $X/\mathbb{F}_q$ una curva elíptica, $D = \{P_1, \ldots, P_n\}$ un subconjunto de $X(\mathbb{F}_q)$ tal que los puntos racionales (no necesariamente distintos) $O, P \notin D$. Sea $G = (k-1)O + P$, $0 < k < n$. Sea $H = X(\mathbb{F}_q)$ dotado de la estructura de grupo con elemento cero O. Entonces el código $C(X, D, G)$ es de tipo MDS si y sólo si $N_H(k, P, D) = 0$. Y la distancia mínima d es igual a $n-k$ si y sólo si $N_H(k, P, D) > 0$.*

Prueba. Tenemos dos elecciones para la distancia mínima de $C(X, D, G)$, a saber, $n-k$ y $n-k+1$; esto debido a la desigualdad en la Eq. (5.1).

Así, $C(X, D, G)$ no es MDS, i.e. $d = n-k$ si y sólo si existe una función $f \in L(G)$ tal que el vector $(f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n$ tiene peso $n-k$. Esto equivale a que f tenga k ceros en D, digamos, $P_{i_1}, \ldots, P_{i_k}$. Es decir, que el divisor principal asociado a f, que denotamos por (f), satisface

$$(f) \geq -(k-1)O - P + P_{i_1} + \cdots + P_{i_k},$$

lo cual es equivalente a, pues ambas desigualdades tienen grado cero,

$$(f) = -(k-1)O - P + P_{i_1} + \cdots + P_{i_k}.$$

i.e.

$$P \sim (k-1)O + P_{i_1} + \cdots + P_{i_k}.$$

Como la ley geométrica del grupo $X(\mathbb{F}_q)$ y la ley algebraica del grupo de Picard son las mismas [17, Prop. 3.4], entonces

$$P = P_{i_1} \oplus \cdots \oplus P_{i_k}.$$

Es decir, $N_H(k, P, D) > 0$. Se deduce que el código $C(X, D, G)$ es MDS si y sólo si $N_H(k, P, D) = 0$. ∎

Observación 5.2.3. En general, si G es un divisor de grado k en X, entonces para cualquier punto racional $Q \in X(\mathbb{F}_q)$, como $\deg(G - (k-1)Q) = 1$, por el Teorema de Riemann-Roch, existe un único punto racional $P \in X(\mathbb{F}_q)$ tal que G es equivalente a $(k-1)Q + P$. Suponga que existen puntos racionales Q, P tales que G es equivalente a $(k-1)Q + P$ y $P, Q \notin D$, y $P, Q \notin \operatorname{supp}(D)$. Sea $G' = (k-1)Q + P$. Entonces los

códigos $C(X, D, G)$ y $C(X, D, G')$ son equivalentes en el sentido de la definición 4.2.6. Como códigos equivalentes tienen la misma distancia mínima, entonces basta considerar códigos de tipo $C(X, D, (k-1)Q + P)$.

Ejemplo 5.2.4. Sea X la curva elíptica de Fermat en $\mathbb{P}^2$ dada por $x^3 + y^3 + z^3 = 0$.

- Puntos sobre $\mathbb{F}_2$:

  $P_0 = (0 : 1 : 1)$, $P_1 = (1 : 1 : 0)$, $P_2 = (1 : 0 : 1)$.

- Puntos sobre $\mathbb{F}_4 = \frac{\mathbb{F}_2[z]}{(z^2+z+1)} = \mathbb{F}_2[\alpha] = \mathbb{F}_2(\alpha)$: con α raíz de $z^2 + z + 1$.

  $P_0 = (0 : 1 : 1)$, $P_1 = (1 : 1 : 0)$, $P_2 = (1 : 0 : 1)$,

  $P_3 = (\alpha : 1 : 0)$, $P_4 = (\alpha + 1 : 1 : 0)$, $P_5 = (\alpha : 0 : 1)$,

  $P_6 = (\alpha + 1 : 0 : 1)$, $P_7 = (0 : \alpha : 1)$, $P_8 = (0 : \alpha + 1 : 1)$.

- Puntos sobre $\mathbb{F}_8 = \frac{\mathbb{F}_2[z]}{(z^3+z^2+1)} = \mathbb{F}_2[\omega]$:

  $P_0 = (0 : 1 : 1)$, $P_1 = (1 : 1 : 0)$, $P_2 = (1 : 0 : 1)$,

  $Q_1 = (\omega : \omega^2 + 1 : 1)$, $Q_2 = (\omega^2 : \omega^2 + 1 : 1)$, $Q_3 = (\omega^2 + \omega + 1 : \omega + 1 : 1)$,

  $Q_4 = (\omega^2 + 1 : \omega : 1)$, $Q_5 = (\omega^2 + \omega : \omega^2 : 1)$, $Q_6 = (\omega + 1 : \omega^2 + \omega + 1 : 1)$.

La curva es nosingular si $\text{char}(\mathbb{F}_q) \neq 3$, ya que el sistema

$$\begin{aligned} x^3 + y^3 + z^3 &= 0 \\ 3x^2 &= 0 \\ 3z^2 &= 0 \end{aligned}$$

no tiene soluciones en $\mathbb{P}^2$. Por lo tanto, el género puede calcularse por la fórmula de Plücker [9, Pág. 169] y es igual a uno. Considere ahora el código $C^*(X, D, G)$, donde $D = P_1 + \cdots + P_8$ y $G = aP_0$ con $1 \leq a \leq 7$.

- La longitud es 8 por la definición de $C^*(X, D, G)$;

- la dimensión es $8-a$ por el Teorema 4.2.3;
- la distancia mínima es el menos a por el Teorema 4.2.3.

Por ejemplo, si $a=6$, $C^*(X,D,G)$ es un $[8,2,\geq 6]$-código; mientras que por el Teorema 4.1.2 $C(X,D,G)$ es un $[8,6,\geq 2]$-código.

Calculamos la distancia mínima si $a=6$. Primero discutimos la dimensión del espacio $L(aP_0)$ en algunos casos.

Caso $a=3$: En $P_0=(0:1:1)$, consideramos $t=x/z$ como un parámetro uniformizante. La expresión $x/(y+z)$ parece una función razonable en X (de hecho lo es casi en todo X). Sin embargo, en P_0 la fracción no tiene sentido. Así, conviene encontrar una forma equivalente para f alrededor de P_0. En X se tiene la expresión

$$\frac{x}{y+z}=\frac{x(y^2+yz+z^2)}{y^3+z^3}=t^{-2}\frac{y^2+yz+z^2}{z^2},$$

donde el segundo factor en la derecha es regular y no cero en P_0. Esto muestra que f tiene un polo de orden 2 en P_0. Similarmente $g=\frac{y}{y+z}$ tiene un polo de orden 3 en P_0. Según esto, las funciones $1,f,g$ tienen órdenes de polos mutuamente distintos y son elementos de $L(3P_0)$. Por lo tanto la dimensión es al menos 3. Ahora, si W es el divisor canónico de la curva X, entonces el grado del divisor $W-3P_0$ es negativo. El Teorema de Riemann-Roch implica que el espacio $L(3P_0)$ tiene dimensión 3.

Caso $a=6$: Se puede mostrar que el conjunto $\{1,\frac{x}{y+z},\frac{y}{y+z},\frac{x^2}{(y+z)^2},\frac{xy}{(x+y)^2},\frac{x^3}{(y+z)^3}\}$ es una base del espacio $L(6P_0)$ y las funciones de dicho conjunto tienen polos de orden $0,2,3,4,5$ y 6, respectivamente.

Por lo tanto, al evaluar las funciones en los puntos $P_1,\ldots,P_8$, encontramos una matriz generadora para $C(X,D,6P_0)$:

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

Se puede mostrar que existen 6 columnas de la matriz G que son linealmente independientes, lo que verifica que la dimensión de $C(X, D, G)$ es 6. La distancia mínima satisface $d \geq n - \deg(G) = 8 - 6 = 2$. ∎

Ejemplo 5.2.5. Considere la curva cúbica dada por $y^2 + y = x^3 + x$ sobre $\mathbb{F}_2$. Esta es una curva nosingular de género uno. Tiene cinco puntos sobre $\mathbb{F}_2$, junto con el punto al infinito:

$$P_\infty = (0:1:0), P_2 = (0:0:1), P_3 = (0:1:1), P_4 = (1:0:0), P_5 = (1:1:1).$$

Ya que $L(P_\infty)$ contiene sólo funciones constantes, entonces considere el divisor $G = 2P_\infty$. El espacio $L(G)$ está generado por $\{0, 1, x, x+1\}$, luego una base es $\{1, x\}$. Evaluando estas dos funciones en los 4 puntos racionales restantes obtenemos la matriz generadora asociada al código $C(X, D, G)$, donde $D = P_2 + \cdots + P_5$,

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ x(P_2) & x(P_3) & x(P_4) & x(P_5) \end{bmatrix}.$$

Es decir,

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

Podemos verificar que el peso mínimo es 2, por lo que este es un $[4, 2, 2]$-código.

Ejemplo 5.2.6. Sea $\mathbb{F}_4 = \{0, 1, \alpha, \overline{\alpha}\}$, donde $\overline{\alpha} = \alpha^2 = \alpha + 1$. Considere la curva X sobre $\mathbb{F}_q$ dada por la ecuación $x^2y + \alpha y^2 z + \overline{\alpha} z^2 x = 0$. Esta es una curva nosingular de género uno. Sus nueve puntos racionales son

$$P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1),$$

$$P_4 = (1:\alpha:\overline{\alpha}), P_5 = (1:\overline{\alpha}:\alpha), P_6 = (1:1:1),$$

$$Q_1 = (\alpha:1:1), Q_2 = (1:\alpha:1), Q_3 = (1:1:\alpha).$$

Sean $D = P_1 + \cdots + P_6$ y $G = 2Q_1 + Q_2$. Se puede mostrar que el conjunto

$$\{\frac{x}{x+y+\overline{\alpha}}, \frac{y}{x+y+\overline{\alpha}}, \frac{\overline{\alpha} z}{x+y+\overline{\alpha}}\}$$

es una base de $L(G)$.

- La matriz generadora del código $C(X, D, G)$ es

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

  que en este caso coincide con una matriz de chequeo de paridad H para el código.

- el código $C(X, D, G)$ tiene longitud 6; y por el Teorema 4.1.2 $C(X, D, G)$ tiene dimensión $k = \deg(G) + 1 - g = 3$;

- por el Teorema 4.1.2 la distancia mínima satisface $d \geq n - \deg(G) = 6 - 3 = 3$. Y como las ternas de vectores columna de H son linealmente independientes, y cualquiera cuatro de ellas son linealmente dependientes, se tiene que $d = 4$; ver [5, Cor. 1.4.14].

De hecho, el código anterior es MDS, ya que satisface que $d = n - k + 1$.

De manera similar, se puede ver que la curva $y^2z + yz^2 = x^3$ sobre $\mathbb{F}_4$ tiene el mismo número de puntos racionales y los mismos parámetros que la curva anterior.

El código del ejemplo anterior es peculiar en el sentido de que para códigos elípticos cuya longitud sea mayor a $q + 1$ se tiene que los parámetros son los mismos que en el ejemplo anterior. Este es un resultado debido a C. Munuera [11]. Enunciamos el resultado.

Proposición 5.2.7. [11, Prop. 3.4] *Sea X una curva elíptica sobre $\mathbb{F}_q$. Si el código $C(X, D, G)$ es MDS y su longitud es mayor que $q + 1$, entonces $C(X, D, G)$ es un $[6, 3, 4]$-código sobre $\mathbb{F}_4$ que proviene de una curva con nueve puntos racionales.*

5.3 Curvas hermitianas

Definición 5.3.1. Sea q una potencia prima. Definimos la *curva hermitiana*, $\mathcal{H}$, como la curva plana afín definida sobre $\mathbb{F}_{q^2}$ por el polinomio $u^{q+1} + v^{q+1} = 1$. Esta es una curva nosingular de género $g = (q^2 - q)/2$, con $q + 1$ puntos al infinito.

Considere la cerradura proyectiva de la curva hermitiana, $\overline{\mathcal{H}} : u^{q+1} + v^{q+1} = \omega^{q+1}$. Para las coordenadas $\omega = 0$, $v = 1$, tenemos que $u^{q+1} + 1 = 0$, y para esta última ecuación existen $q+1$ raíces. Estas raíces están en $\mathbb{F}_{q^2}$ ya que $u^{(q+1)(q-1)} = (-1)^{q-1} = 1$, para cualquier potencia de un primo. Así, $u^{q^2-1} = 1$, lo cual confirma que las raíces están en $\mathbb{F}_{q^2}$.

Escribiendo $\omega = 1$, tenemos que $u^{q+1} + v^{q+1} = 1$. Existen $q + 1$ valores para v tales que $v^{q+1} + 1 = 0$, así, existen $q + 1$ puntos de la forma $(0 : a : 1)$ que pertenecen a la curva. Ahora, si $\beta = v^{q+1} + 1 \neq 0$, entonces $u^{q+1} + \beta$ tiene $q + 1$ raíces distintas. El número de posibles v's que satisfacen lo anterior deben ser $q^2 - q - 1$, ya que, aparte de q^2 elementos de $\mathbb{F}_{q^2}$, $q + 1$ elementos satisfacen $v^{q+1} + 1 = 0$.

Por lo tanto, el número de puntos racionales de la curva hermitiana es

$$q + 1 + (q + 1) + (q^2 - q - 1)(q + 1) = q^3 + 1.$$

En resumen, si q es una potencia prima, entonces existen $q^3 + 1$ puntos racionales en la curva hermitiana definida sobre $\mathbb{F}_{q^2}$.

La curva $\mathcal{H}$ es uno de los mejores ejemplos de una curva maximal, i.e. con el número máximo de puntos $\mathbb{F}_{q^2}$-racionales asegurado por la cota de Hasse-Weil; ver Teorema 3.6.6. Eligiendo $a, b, c \in \mathbb{F}_{q^2}$ tales que

$$a^{q+1} = -1, \quad b^q + b = 1, \quad c = -ab^q;$$

se deduce que

$$ab^q + c = 0,$$

$$ac^q + a^q c = a(-a^q b) + a^q(-ab^q) = -a^{q+1}(b + b^q) = 1.$$

Sean

$$x = \frac{1}{u + av} \quad \text{y} \quad y = \frac{bu + cv}{u + av}.$$

Entonces se obtiene

$$(u + av)^{q+1} x^{q+1} = 1$$

y

$$\begin{aligned}(u + av)^{q+1}(y^q + y) &= (u + av)(bu + cv)^q + (u + av)^q(bu + cv) \\ &= (b^q + b)u^{q+1} + (b^q a + c)u^q v + (c^q + ba^q)uv^q + (ac^q + a^q c)v^{q+1}.\end{aligned}$$

De los cálculos anteriores podemos concluir que la curva $\mathcal{H}$ la podemos definir como los ceros del polinomio $y^q + y = x^{q+1}$, la cual es una curva con sólo un punto al infinito.

Ejemplo 5.3.2. Considere la cerradura proyectiva de la curva anterior con $q = 4$ dada por $\overline{\mathcal{H}} : x^5 + y^4 z + y z^4$ sobre $\mathbb{F}_{16}$. Es nosingular, ya que las ecuaciones de las derivadas parciales

$$5x^4 = 4y^3 z + z^4 = y^4 + z^3 y = 0,$$

lo cual se simplifica como

$$x^4 = z^4 = y^4 + z^3 y = 0.$$

Cualquier punto singular debe satisfacer $x = y = z = 0$. Es decir, la curva es nosingular. Sea $Q = (0 : 1 : 0)$ el único punto al infinito. Sean $x_y = x/y$ y $z_y = z/y$ y considere la curva plana afín definida por $f(x_y, 1, z_y)$. Al diferenciar se muestra que x_y es un parámetro uniformizante en Q, así, $\mathrm{ord}_Q(x_y) = 1$. Tenemos

$$\begin{aligned} x_y^5 + z_y^4 + z_y &= 0, \\ z_y^4 + z_y &= x_y^5, \\ z_y(z_y^3 + 1) &= x_y^5, \\ z_y &= \frac{x_y^5}{z_y^3 + 1}. \end{aligned}$$

Por otra parte, vemos que $\frac{1}{z_y^3+1}(0,0) = 1$, es decir, que $\frac{1}{z_y^3+1} \in \mathbb{F}_{16}[\overline{\mathcal{H}}]_Q^\times$. Por lo tanto, $\mathrm{ord}_Q(z_y) = \mathrm{ord}_Q(\frac{x_y^5}{z_y^3+1}) = 5 \cdot \mathrm{ord}_Q(x_y) = 5$. Se deduce que

$$\mathrm{ord}_Q(y/z) = \mathrm{ord}_Q(1/z_y) = -5,$$

y similarmente

$$\mathrm{ord}_Q(x/z) = \mathrm{ord}_Q(x_y/z_y) = \mathrm{ord}_Q(x_y) - \mathrm{ord}_Q(z_y) = 1 - 5 = -4.$$

Por la fórmula de Plücker, la curva tiene género 6 y el Teorema de Riemann-Roch implica que la dimensión de $L(11Q)$ es igual a $11 + 1 - 6 = 6$. Ya que tanto x/z y y/z tiene polos sólo en Q, entonces claramente se debe tener que $L(11Q)$ tiene por base al conjunto $\{1, x/z, y/z, x^2/z^2, xy/x^2, y^2/z^2\}$.

La representación de la curva hermitiana del ejemplo anterior es considerablemente más útil, porque se puede dar una descripción explícita del divisor canónico de la curva, de los espacios $L(rP_\infty)$ y de todos los puntos racionales. Para diversas aplicaciones enunciamos esos resultados en el lema siguiente.

Lema 5.3.3. [21, Lemma 6.4.4] *La curva hermitiana definida por* $y^q + y = x^{q+1}$ *tiene las siguientes propiedades:*

(*i*) *El género de la curva es* $g = \frac{q(q-1)}{2}$*;*

(*ii*) *La curva tiene* $q^3 + 1$ *puntos racionales sobre* $\mathbb{F}_{q^2}$*, a saber:*

  (*a*) *El punto al infinito* $Q = (0 : 1 : 0)$*;*

  (*b*) *Para cada* $\alpha \in \mathbb{F}_{q^2}$ *existen* q *elementos* $\beta \in \mathbb{F}_{q^2}$ *tales que* $\beta^q + \beta = \alpha^{q+1}$*.*

(*iii*) *Es una curva maximal, i.e. alcanza la cota de Hasse-Weil;*

(*iv*) *Para* $r \geq 0$*, los elementos* $x^i y^j$ *con* $0 \leq i;\ j \leq q-1$*; y* $iq + j(q-1) \leq r$*, forman una base del espacio* $L(rQ)$*.*

Ejemplo 5.3.4. (Códigos hermitianos) Considere la curva hermitiana, X, definida por $x^3+y^2z+yz^2 = 0$ sobre $\mathbb{F}_4$. Esta curva es nosingular de género uno. Tiene nueve puntos racionales y un punto al infinito, $Q = (0 : 1 : 0)$. Considere el código $C^*(X, D, aQ)$, donde D es la suma de los otros ocho puntos racionales, excepto Q.

- La distancia mínima satisface $a \leq d^* \leq a + 1$;
- si $\deg(G) < 8$, entonces el código tiene dimensión $k^* = 8-\deg(G)+1-g = 8-a$. Por ejemplo, si $a = 5$, entonces $k^* = 8 - a = 3$;
- Podemos suponer que $d^* = a$ ya que el caso $d^* = a + 1$ implica que el código $C^*(X, D, aQ)$ es MDS, lo cual se trata en la Proposición 5.2.7.

Por el Ejemplo 5.3.2, el espacio $L(5Q)$ tiene por base al conjunto $\{1, x' = x/z, y' = y/z, x'^2 = x^2/z^2, x'y' = xy/z^2\}$. Defina $\mathbb{F}_4 := \mathbb{F}[\omega]$, donde $\omega^2 + \omega + 1 = 0$. Sean

$$P_1 = (0 : 0 : 1), P_2 = (0 : 1 : 1), P_3 = (1 : \omega : 1), P_4 = (1 : \omega^2 : 1),$$

$$P_5 = (\omega, \omega, 1), P_6 = (\omega : \omega^2 : 1), P_7 = (\omega^2 : \omega : 1), P_8 = (\omega^2 : \omega^2 : 1).$$

El código $C^*(X, D, aQ)$ tiene matriz de chequeo de paridad

$$\begin{bmatrix} 1 & \cdots & 1 \\ x'(P_1) & \cdots & x'(P_8) \\ y'(P_1) & \cdots & y'(P_8) \\ x'^2(P_1) & \cdots & x'^2(P_8) \\ x'y'(P_1) & \cdots & x'y'(P_8) \end{bmatrix},$$

y al evaluar las funciones se tiene

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega^2 & \omega & \omega \\ 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & \omega \end{bmatrix}.$$

Observe que si $a > n + 2g - 2$, el Teorema de Riemann-Roch implica que

$$k = a - g + 1 - (a - n - g + 1) = n.$$

En este caso, $C(X, D, G) \sim \mathbb{F}_{q^2}$, i.e. el código trivial. Por lo tanto, sólo interesan códigos con $0 \leq a \leq n + 2g - 2$.

Para la curva hermitiana $X : y^q + y = x^{q+1}$ se tiene el código $C(X, D, G)$ con $D = P_1 + \cdots + P_n$, $n = q^3$, los P_i son los puntos racionales de la curva X, y $G = aQ_\infty$ es un múltiplo del único punto al infinito de la curva con $0 \leq a \leq n + 2g - 2$. El código $C(X, D, G)$ es dual a $C(X, D, bQ_\infty)$, con $b = n + 2g - 2 - a$.

Para encontrar la distancia mínima de códigos sobre curvas hermitianas primero necesitamos alguna notación.

El siguiente resultado nos da los parámetros principales de un código hermitiano, y generaliza al ejemplo anterior.

Proposición 5.3.5. *Suponga que* $0 \leq a \leq q^3 + (2g-2)$*, y sea* $b = q^3 + (2g-2) - 2 - m$*. Entonces la dimensión* k *de* $C(X, D, aQ_\infty)$ *viene dada por*

$$k = \begin{cases} \dim L(aQ_\infty), & 0 \leq a < q^3; \\ q^3 - \dim L(bQ_\infty), & q^3 \leq a \leq q^3 + (2g-2); \\ m - g + 1, & 2g - 2 < m < q^3, \end{cases}$$

y la distancia mínima satisface $d \geq q^3 - m$.

Prueba. Para $0 \leq a < q^3$ tenemos $k = \dim L(aQ_\infty)$. Para $q^3 \leq a \leq q^3 + (2g-2)$ y $b = q^3 + (2g-2) - 2 - m$ se tiene que $0 \leq b \leq q^3$, y entonces

$$k = q^3 - \dim C(X, D, bQ_\infty) = q^3 - \dim L(bQ_\infty).$$

Las afirmaciones restantes se siguen del Teorema 4.1.2. ∎

Definición 5.3.6. Sea X una curva sobre F_q de género $g \geq 2$. Sean $x \in X$ y $\alpha \geq 1$ un entero. Llamamos a α una *brecha* en x si $\dim L(\alpha x) = \dim L((\alpha - 1)x)$ y un *agujero* en caso contrario.

En otras palabras, α es un agujero en x si y sólo si existe una función $f \in F_q(X)$ teniendo un polo de orden α en x y siendo regular afuera de α, i.e. $(f)_\infty = \alpha x$. Si tal f no existe entonces α es una brecha en x.

La condición del género en la definición anterior es una condición técnica que permite mostrar la existencia de puntos importantes en la curva X llamados puntos de Weierstrass.

Considere el campo $\mathbb{F}_q^2$ y el conjunto $\mathcal{N}$ de agujeros en el punto $Q_\infty = (0:1:0)$, es decir,

$$\mathcal{N} := \{n \geq 0 : \text{existe } f \in \mathbb{F}_q^2(X) \text{ con } (f)_\infty = nQ_\infty\}.$$

Para $s \geq 0$, sea

$$\mathcal{N}_s = \{n \in \mathcal{N} : n \leq s\}.$$

Entonces $|\mathcal{N}_s| = \dim L(sQ_\infty)$ y para $s \geq 2g - 1 = q^2 - q - 1$, el Teorema de Riemann-Roch nos da que

$$|\mathcal{N}_s| = s + 1 - \frac{q^2 - q}{2}.$$

Ahora introducimos los principales parámetros de los códigos hermitianos y se generaliza el ejemplo anterior.

Definición 5.3.7. Para $r \in \mathbb{Z}$ definimos el código $C_r := C(X, D, rQ_\infty)$, donde $D := \sum_{i=1}^{q^3} P_i$ es la suma de todos los puntos racionales P_i (excepto $Q_\infty = (0:1:0)$) de la curva $y^q + y = x^{q+1}$ sobre F_{q^2}. Los códigos C_r son llamados códigos hermitinanos.

Para $r < 0$, $L(rQ_\infty) = 0$, por tanto $C_r = 0$. Si $r > q^3 + q^2 - q - 2$, el Teorema 4.1.2 implica que

$$\dim C_r = \dim L(rQ_\infty) - \dim L(rQ_\infty - D) = (r + 1 - g) - (r - q^3 + 1 - g) = q^3 = n.$$

Por lo tanto, C_r es el código trivial.

La dualidad de un código hermitiano viene dada en el siguiente resultado, tiene utilidad también para calcular los pesos generalizados de códigos hermitianos, lo cual hacemos en el siguiente capítulo.

Proposición 5.3.8. [21, Prop. 8.3.2] *El código dual de C_r es*

$$C_r^\perp = C_{q^3+q^2-q-2-r}.$$

Los casos no triviales de códigos hermitianos se tratan en el siguiente resultado.

Proposición 5.3.9. *Suponga que $0 \leq r \leq q^3 + q^2 - q - 2$. Entonces se satisface lo siguiente*

(*i*) *La dimensión k de $C_r = C(X, D, rQ_\infty)$ viene dada por*

$$k = \begin{cases} |\mathcal{N}_r|, & 0 \leq r < q^3; \\ q^3 - |\mathcal{N}_s|, & q^3 \leq r \leq q^3 + q^2 - q - 2, \end{cases}$$

donde $s := q^3 + q^2 - q - 2 - r$.

(*ii*) *Para $q^2 - q - 2 < r < q^3$ se tiene*

$$\dim C_r = r + 1 - \frac{q(q-1)}{2}.$$

(*iii*) *La distancia mínima satisface*

$$d \geq q^3 - r.$$

Si $0 \leq r < q^3$ y ambos números r y $q^3 - r$ son agujeros en Q_∞, entonces $d = q^3 - r$.

Prueba. (i): Para $0 \leq r < q^3$, el Teorema 4.1.2 implica que

$$k = \dim C_r = \dim L(rQ_\infty) = |\mathcal{N}_r|.$$

Para $q^3 \leq r \leq q^3 + q^2 - q - 2$ y $s = q^3 + q^2 - q - 2 - r$ se tiene que $0 \leq s \leq q^3$, y entonces

$$k = q^3 - \dim C(X, D, sQ_\infty) = q^3 - \dim L(sQ_\infty).$$

(ii): Para $q^2 - q - 2 = 2g - 2 < r < q^3$, el Teorema 4.1.2 nos da

$$\dim C_r = r + 1 - g = r + 1 - \frac{q(q-1)}{2}.$$

(iii): La desigualdad se deduce del Teorema 4.1.2. La igualdad se demuestra en el Teorema 6.5.5, junto con una generalización. ∎

Chapter 6

Pesos generalizados

El concepto de pesos generalizados fue introducido por Wei en [26]. Brevemente recordamos esta noción. Una referencia para códigos lineales es [5].

6.1 Definición

Sean $K = \mathbb{F}_q$ un campo finito y C un código lineal con *longitud* n y *dimension* k, esto es, C es un subespacio vectorial de K^n con $k = \dim C$.

Definición 6.1.1. Sean $1 \leq r \leq k$ un entero. Dado un subespacio vectorial D de C, el *soporte* de D es el conjunto

$$\operatorname{supp}(D) := \{i : \exists\, (a_1, \ldots, a_n) \in D,\, a_i \neq 0\}.$$

El r-ésimo *peso generalizado* de C, denotado $d_r(C)$, está dado por

$$d_r(C) := \min\{|\operatorname{supp}(D)| \colon D \text{ es un subespacio de } C \text{ con } \dim L(D) = r\}.$$

El conjunto $\{d_1(C), \ldots, d_k(C)\}$ se llama la *jerarquía de pesos* del código.

Observando que $d_1(C)$ es precisamente la distancia mínima del código, podemos considerar a la jerarquía de pesos como una generalización de la distancia mínima.

6.2 Algunas propiedades

Esta sección se presentan algunas generalizaciones de resultados dados en el primer capítulo acerca de la distancia mínima de un código.

Proposición 6.2.1. *Para un $[n, k, d]$-código C, los pesos generalizados satisfacen las desigualdades*

$$0 < d_1 < \cdots < d_k \leq n.$$

Prueba. La desigualdad $d_{r-1} \leq d_r$ se sigue de la definición; mostremos que es estricta. Sean D un subcódigo de C de dimensión r y $|\text{supp}(D)| = d_r(C)$. Sean $i \in \text{supp}(D)$ y $D_i := \{x \in D : x_i = 0\}$, donde x_i es la i-ésima coordenada de x. La dimensión de D_i es $r - 1$ y se tiene que $d_{r-1} \leq |\text{supp}(D)| \leq |\text{supp}(D)| - 1 = d_r(C) - 1$. ∎

El siguiente resultado generaliza la cota de Singleton.

Corolario 6.2.2. *Sea C un $[n, k, d]$-código. Entonces $k + d_r(C) \leq n + r$.*

Prueba. Por inducción en $k - r$. Si $k - r = 0$, entonces $d_r = d_k \leq n = n - k + r$ por el resultado anterior. Suponga que $d_r \leq n - k + r$ para algún $r \leq k$, por el mismo resultado, $d_{r-1} \leq d_r - 1 \leq n - k + r - 1$. ∎

La matriz de chequeo de paridad de un $[n, k, d]$-código lineal C es una matriz H de tamaño $(n-k) \times n$. Las palabras código son entonces vectores renglón x de longitud n tales que $Hx^T = 0$. El siguiente teorema da una manera alterna de calcular los pesos generalizados. Primero definimos $\langle H_i : i \in I\rangle$ como el espacio vectorial generado por las columnas de H, donde $I \subseteq \{1, \ldots, n\}$. ($H_i$ es la i-ésima columna de H.)

Teorema 6.2.3. *Sea C un $[n, k, d]$-código. Para todo $r \leq k$,*

$$d_r(C) = \min\{|I| : |I| - \dim\langle H_i : i \in I\rangle \geq r\}.$$

Prueba. Para cualquier $I \subseteq \{1, \ldots, n\}$, sea $V = \langle H_i : i \in I\rangle$. Sea

$$V^\circ := \{x \in V : x_i = 0 \text{ para todo } i \in I \text{ y } \sum_{i \in I} x_i H_i = 0\}.$$

Entonces $\dim V + \dim V^\circ = |I|$. Sea d igual al valor del lado derecho de la igualdad en la afirmación de este teorema. Sea $I \subseteq \{1, \ldots, n\}$ tal que $|I| - \dim V = r$ y $|I| = d$. Entonces $\dim V^\circ = r$, V° es un subcódigo de C, y $d_r(C) \leq |\mathrm{supp}(V^\circ)| \leq |I| = d$. Así, $d_r(C) \leq d$. Falta demostrar la desigualdad anterior en la otra dirección. Sea S un subcódigo de C con $\dim S = r$ y $|\mathrm{supp}(V)| = d_r(C)$. Sea $I \subseteq \mathrm{supp}(V)$, entonces $S \subseteq V^\circ$. Pero $\dim V = |I| - \dim V^\circ \leq |I| - r$, así, $|I| - \dim V \geq r$. Suponga $|I| - \dim V = r' > r$. Entonces $S \neq V^\circ$ y $d_r(C) \leq |\mathrm{supp}(V^\circ)| \geq |I|$, una contradicción. Por tanto $|I| - \dim V = r$ y $d \leq d_r(C)$. ∎

Proposición 6.2.4. (Dualidad de Wei)[26, Thm. 3] *Sean C un $[n, k, d]$-código y $C^\perp$ su código dual. Entonces se tiene que*

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

6.3 Sucesión de gonalidades

Ahora definimos la gonalidad de una curva y establecemos algunas de sus propiedades.

Definición 6.3.1. La *gonalidad* $\gamma(X)$ de una curva X sobre un campo K es el menor grado de un mapeo no constante racional de X a la línea proyectiva $\mathbb{P}^1$; cf. [14].

Lema 6.3.2. *Si D es un divisor de grado $\deg(D) < \gamma(X)$, entonces $\dim L(D) \leq 1$.*

Prueba. Si $\dim L(D) > 1$, entonces existe una función racional no constante f en X tal que $(f) \geq -D$, de donde se tiene que $(f)_\infty \geq D$. Podemos ver a f como un mapeo no constante, definido sobre el campo de constantes, de X a la línea proyectiva. El grado de este mapeo es igual a $\deg (f)_\infty \leq \deg(D) < \gamma(X)$, contradiciendo la definición de gonalidad. ∎

Lema 6.3.3. *Sea X una curva de género g definida sobre $\mathbb{F}_q$ y sea $N = |X(\mathbb{F}_q)|$ (número de puntos racionales de X), entonces $g + 1 \geq \gamma(X) \geq \frac{N}{q+1}$. Por otra parte, si $\gamma(X) = g + 1 > 3$, entonces $g \leq 10$ y $q \leq 31$.*

Prueba. Para el lado izquierdo de la desigualdad notar que sobre un campo finito siempre existe un divisor de grado $g + 1$ (ver [9]). Por el teorema de Riemann-Roch la

dimensión de tal divisor es al menos 2; ver [9, Thm. 3.2].

Para el lado derecho de la desigualdad notar que bajo un mapeo no constante de grado $\gamma(X)$ de una curva X a la línea proyectiva, los N puntos racionales de la curva son mapeados a uno de los $q+1$ puntos racionales de la línea proyectiva y la imagen inversa de un punto en la línea proyectiva contiene al menos $\gamma(X)$ puntos racionales.

Suponga ahora que $\gamma = g+1 > 3$. Primero mostramos que tal curva no tiene divisores efectivos de grado $g-2$. En efecto, si tal divisor existe considere el divisor canónico W, así, $\dim L(W-D) \geq \dim L(W) - \deg(D) = 2$ y $\deg(W-D) = g$. Por lo tanto $\deg(W-D) = g < g+1 = \gamma(X)$. Pero esto contradice el Lema 6.3.3. Ahora bien, la curva no tiene divisores efectivos de grado $g-2$, lo que implica que la curva sobre cualquier extensión de grado $g-2$ no tiene puntos racionales. Por la cota de Hasse-Weil, Teorema 3.6.6, tenemos que

$$q^{g-2} + 1 - 2gq^{\frac{g-2}{2}} \leq 0,$$

por tanto $g \leq 2\log_q(2g) + 1$. Esto implica que $g \leq 10$ y $q \leq 31$. ∎

Lema 6.3.4. *Sea X una curva de género g. Entonces*

(*i*) $\gamma(X) = 1$ *si y sólo si X es isomorfa a la línea proyectiva.*

(*ii*) $\gamma(X) = 2$ *si y sólo si X es una curva elíptica o hiperelíptica.*

Definición 6.3.5. Sea X una curva sobre $\mathbb{F}_q$. Para un entero positivo r, sea

$$\gamma_r = \gamma_r(X, \mathbb{F}_q) := \min\{\deg(A) : A \in \mathrm{Div}(X) \text{ y } \dim L(A) \geq r\}.$$

$GS(X, \mathbb{F}_q) := \{\gamma_r : r \in \mathbb{N}\}$ se llama la *sucesión de gonalidades* de X sobre $\mathbb{F}_q$.

Observese que el Teorema de Riemann-Roch implica $\gamma_1 = 0$. Enunciamos algunas propiedades de la sucesión $GS(X, \mathbb{F}_q)$ en el siguiente resultado.

Lema 6.3.6. [6, Prop. 11] *Sea g el género de X y suponga que $X(\mathbb{F}_q) \neq \emptyset$. Entonces*

(*i*) *La sucesión $GS(X, \mathbb{F}_q)$ es estrictamente creciente;*

(*ii*) $\gamma_r = g + r - 1$ *para* $r \geq g + 1$;

(*iii*) $\gamma_g = 2g - 2$;

(*iv*) $\gamma_r \geq 2r - 2$ *para* $0 \leq r \leq g - 1$.

Prueba. (i) Sea A un divisor con $\deg(A) = \gamma_r$ y $\dim L(A) \geq r$. Basta ver que existe un divisor A' con $\deg(A') < r$ y $\dim L(A') \geq r - 1$. Sea $A' := A - P$, donde P es un punto racional de la curva X. Tenemos que $\dim L(A) \leq \dim L(A') + \deg(P) = \dim L(A') + 1$. Por lo tanto $\dim L(A') \geq \dim L(A) - 1 \geq r - 1$.

(ii) Sea A un divisor de X con $\deg(A) = r + g - 1 > 2g - 1$. Por el Teorema de Riemann-Roch, $\dim L(A) = \deg(A) + 1 - g$, así, $\gamma_r \leq r + g - 1$. Considere cualquier divisor B de grado $< r + g - 1$. Entonces existe un divisor B' tal que $B \leq B'$ y $\deg(B') = r + g - 2 > 2g - 2$. Por lo que $\dim L(B) \leq \dim L(B')$ y $\dim L(B') = \deg(B') + 1 = g = r - 1$. De esto se sigue que $\gamma_r \geq r + g - 1$.

(iii)-(iv) Considere la clase del divisor canónico W de X. Entonces $\deg(W) = 2g - 2$ y $\dim L(W) = g$, luego $\gamma_g \leq 2g - 2$. Por definición de γ_r, tenemos que $0 \leq \gamma_r \leq 2g - 2$ para cualquier $1 \leq r \leq g$. Sea A un divisor con $\deg(A) = \gamma_r$ y $\dim L(A) \geq r$. Por el Teorema de Clifford 3.6.5, $\dim L(A) \leq (1/2)\deg(A) + 1 = 1 + \gamma_r/2$. Por lo tanto, $r \leq 1 + \gamma_r/2 = g$. Para $r = g$, $\gamma_g \leq 2(g - 1) = 2g - 2$. Esto muestra la igualdad en (iii) y la desigualdad en (iv). ∎

6.4 Cotas inferiores

El siguiente teorema muestra que la cota inferior dada en el Teorema 4.1.2, para la distancia mínima de un código de Goppa, admite una generalización para todos los pesos generalizados d_r, pero esta vez involucrando la sucesión de gonalidades $GS(X, \mathbb{F}_q)$.

Teorema 6.4.1. [6, Thm. 12] *Para el código de Goppa* $C = C(X, D, G)$*, con parámetros* $[n, k, d]$*, se tiene que*

$$d_r(C) \geq n - \deg(G) + \gamma_r \quad \textit{para todo} \quad 1 \leq r \leq k.$$

Prueba. Sea V_r un subcódigo r-dimensional de C tal que $d_r(C) = |\mathrm{supp}(V_r)|$. Sin pérdida de generalidad, podemos suponer que V_r está generado por r palabras código de la forma $\alpha(f_1), \ldots, \alpha(f_r)$, donde $f_1, \ldots, f_r \in L(G)$ son linealmente independientes y α es la aplicación dada en la Definición 4.1.1. Entonces, decir que $d_r(C) = |\mathrm{supp}(V_r)|$ es equivalente a decir que todas las palabras en la base $\{\alpha(f_1), \ldots, \alpha(f_r)\}$ comparten exactamente $n - d_r(C)$ lugares distintos donde todas las coordenadas son cero. Esto se puede establecer en término de divisores, a saber, que para cualquier $1 \leq i \leq r$ se tiene que

$$(f_i) = A + B_i - G,$$

donde $0 \leq A \leq D$, $\deg(A) = n - d_r(C)$ y $B_i \geq 0$ para $i = 1, \ldots, r$.

En efecto, como $f_i \in L(G)$, entonces $(f_i) \geq -G$. Podemos elegir un divisor $C_i \geq 0$ tal que $(f_i) = C_i - G$. Los Teoremas 4.1.2 y 6.2.1 implican que

$$\deg(G) \geq n - d_1 > n - d_r,$$

Así, $\deg(G) = b + n - d_r$. Por otra parte, $\deg(f) = 0 = \deg(C_i) - \deg(G)$. Estas dos observaciones implican que podemos escribir el divisor C_i como una suma de divisores $A + B_i$ con $\deg(A) = n - d_r$ y $\deg(B) = b \geq 0$.

La independencia lineal del conjunto $\{f_1, \ldots, f_r\}$ implica que el conjunto de funciones $\{f_1/f_1, \ldots, f_r/f_1\}$ es linealmente independiente y está contenido en $L(B_1)$ ya que

$$\left(\frac{f_i}{f_1}\right) = B_2 - B_1 \geq -B_1, \text{ para } i = 1, \ldots, r.$$

Esto implica que $\dim L(B_1) \geq r$ y por la definición de γ_r se tiene que $\deg(B_1) \geq \gamma_r$. Como $\deg(f_1) = 0 = \deg(B_1) + \deg(A) - \deg(G)$, entonces

$$\deg(G) - \deg(A) = \deg(G) - n + d_r(C) \geq \gamma_r,$$

lo que concluye la demostración. ∎

Corolario 6.4.2. *Para $n > \deg(G) > 2g - 2$, los pesos del código $C = C(X, D, G)$ satisfacen*

$$d_r(C) = n - k + r \quad \textit{para} \quad g + 1 \leq r \leq k,$$

donde k es la dimensión de C.

Prueba. La hipótesis inicial implica que $k = \dim L(G) = \deg(G) + 1 - g$, y

$$\begin{aligned} d_r(C) &\geq n - \deg(G) + \gamma_r \\ &= n - (\deg(G) + 1 - g) + r \\ &= n - k + r \end{aligned}$$

para cualquier r con $g + 1 \leq r \leq k$ por el Lema 6.3.6 y el Teorema 6.4.1. Por el Corolario 6.2.2 se tiene que $d_r(C) \leq n - k + r$. Por lo tanto, si $2g - 2 < \deg(G) < n$, entonces

$$d_r(C) = n - k + r,$$

para cualquier r con $g + 1 \leq r \leq k$. ∎

6.5 Curvas hermitianas

En esta sección se considera un caso más general de curvas hermitianas que las tratadas en el capítulo anterior, se establecen algunos resultados que complementan los resultados ya establecidos sobre códigos hermitianos.

Ejemplo 6.5.1. Considere la curva afín sobre $\mathbb{F}_{q^2}$ dada por

$$y^q + y = x^s, \quad s \text{ divide a } q + 1.$$

El género de la curva anterior es $g = \frac{(q-1)(s-1)}{2}$. Se afirma que tiene $N = 1 + q(1 + (q-1)s)$ puntos racionales. El punto $Q_\infty = (0 : 1 : 0)$ es uno de ellos. Sea $\alpha \in \mathbb{F}_{q^2}$. Contamos el número de elementos $\alpha \in \mathbb{F}_{q^2}$ tales que la ecuación $T^q + T = \alpha^s$ tiene una raíz $\beta \in \mathbb{F}_{q^2}$. La aplicación $\beta \mapsto \beta^q + \beta$ es la traza de la extensión de campos $\mathbb{F}_{q^2}/\mathbb{F}_q$, la cual es sobre. Por lo tanto, la ecuación anterior tiene una raíz en $\mathbb{F}_{q^2}$ si y sólo si $\alpha^s \in \mathbb{F}_q$. Sea $U \subseteq \mathbb{F}_{q^2}^\times$,

$$\alpha^s \in \mathbb{F}_q \Leftrightarrow \alpha \in U \cup \{0\}.$$

Por lo tanto, $N = q|U| + 1 = q(1 + (q-1)s) + 1$. Ya que $N = 1 + q^2 + 2gq = 1 + q^2 + q(q-1)(s-1)$, la curva $y^q + y = x^s$ sobre $\mathbb{F}_{q^2}$ es otro ejemplo de curva maximal.

Sea $m \geq 0$ un entero. Como en el Lema 5.3.3 se tiene que una base para el espacio $L(mQ_\infty)$ viene dada por

$$\{x^i y^j : 0 \leq i, 0 \leq j \leq q-1, iq + sj \leq m\}.$$

Ahora, basándose en el ejemplo anterior definimos el código más importante de la sección.

Definición 6.5.2. Sean $m \geq 0$ un entero, X la curva del ejemplo anterior y Q_∞ el punto al infinito. Definimos el código $C_m = C(X, D, mQ_\infty)$, donde $D := \sum_{i=1}^{N} P_i$ es la suma de todos los puntos racionales de X (excepto Q_∞). El código anterior es una generalización de los códigos hermitianos.

El código C_m es un código lineal de longitud $n = q(1+(q-1)s)$ y si $m_1 \leq m_2$, entonces $C_{m_1} \subseteq C_{m_2}$, y por lo tanto los pesos generalizados satisfacen $d_r(C_{m_1}) \geq d_r(C_{m_2})$ para todo r, con $1 \leq r \leq k_1$, donde k_1 es la dimensión de C_{m_1} sobre $\mathbb{F}_{q^2}$.

Proposición 6.5.3. *Sea p_r el r-ésimo agujero de Q_∞ y sea $\{\gamma_r : r \geq 1\}$ la sucesión de gonalidades de la curva hermitiana X definida por $y^q + y = x^{q+1}$. Entonces*

(i) $\gamma_1 = p_1 = 0$;

(ii) $\gamma_2 = p_2 = q$;

(iii) $\gamma_3 = p_3 = q + 1$.

Prueba. De las definiciones se sigue que $\gamma_1 = 0 = p_1$ y de la definición de γ_r se sigue que $\gamma_r \leq p_r$. Sea N el número de puntos racionales de X sobre $\mathbb{F}_{q^2}$. Suponga que $\gamma_2 < q$. Entonces los Lemas 6.3.6 y 6.3.3 implican que $N < (q^2+1)\gamma_2 \leq (q^2+1)(q-1)$. Así, $N < q^3+1$, lo cual es una contradicción al Lema 5.3.3(ii). Esto implica que $\gamma_2 = q$. El Lema 6.3.6 dice que $\gamma_3 > \gamma_2 = q \geq q+1$. Como $\gamma_3 \leq p_3 = q+1$, observando que $\gamma_r \leq p_r$, donde p_r es el r-ésimo agujero, se obtiene la igualdad. ∎

Respecto a una cota para los pesos generalizados en general se tiene:

Teorema 6.5.4. [1, Thm. 4.14] *Sean $s = q+1$ y p_r el r-ésimo agujero de Q_∞. Suponga que $2q^2 - q - 2 \leq m < q^3$ y que $q^3 - m$ es un agujero de Q_∞. Entonces, para todo $1 \leq r \leq g$, donde g es el género de la curva hermitiana, se tiene que*

$$d_r(C_m) \leq q^3 - m + p_r.$$

Ahora se da un resultado que muestra los primeros tres pesos generalizados.

Teorema 6.5.5. (Caso hermitiano) *Sea $s = q + 1$. Suponga que $2q^2 - q - 2 \leq m < q^3$ y que $q^3 - m$ es un agujero del punto Q_∞. Entonces se satisface*

(a) $d_1(C_m) = q^3 - m$;

(b) $d_2(C_m) = q^3 - m + q$;

(c) $d_3(C_m) = q^3 - m + q + 1$.

Prueba. Por la Proposición 6.5.3, $\gamma_1 = 0 = p_1$, $\gamma_2 = q = p_2$ y $\gamma_3 = q + 1 = p_3$. Con la observación previa, el Teorema 6.4.1 para $r = 1, 2, 3$, dice que en este caso $d_r(C_m) \geq q^3 - m + \gamma_r$ y por el Teorema anterior $d_r(C_m) \leq q^3 - m + \gamma_r$, lo que implica (a), (b) y (c). ∎

Ahora, la última parte del Teorema 5.3.9 es (a) en el resultado anterior.

De los primeros trabajos más relevantes en el área de códigos hermitianos se debe a Kyeongcheol Yang en su trabajo de tesis doctoral [28].

Enunciamos algunos de sus resultados en cuanto a pesos generalizados, la gran mayoría es para la distancia mínima y los pesos d_2 y d_3.

Teorema 6.5.6. [1, Thm. 4.16] *Suponga que $0 \leq m < q^2$ y que m es un agujero de Q_∞. Sea k la dimensión de C_m y escribamos $m = aq+$, con $0 \leq b \leq a \leq q - 1$. Sea p_r el r-ésimo agujero de Q_∞. Entonces*

(i) $d_1(C_m) = q^3 - m$;

(ii) $d_2(C_m) = q^3 - m + q$;

(*iii*) $d_3(C_m) = q^3 - m + q + 1$ *si* $b \neq 0$;

(*iv*) *Si* $b = a$, *entonces*

$$\begin{cases} d_{k-i}(C_m) = n - i, & 0 \leq i \leq a; \\ d_r(C_m) \leq q^3 - m + p_r, & 4 \leq r \leq k - a - 1. \end{cases}$$

(*v*) *Si* $b = a - 1$, *entonces*

$$\begin{cases} d_{k-i}(C_m) = n - i, & 0 \leq i \leq a - 1; \\ d_r(C_m) \leq q^3 - m + p_r, & 4 \leq r \leq k - a. \end{cases}$$

(*vi*) *Si* $0 \leq b \leq a - 2$, *entonces* $d_r(C_m) \leq q^3 - m + p_r$ *para todo* r *con* $1 \leq r \leq (b+2)(b+3)/2 - 1$.

Teorema 6.5.7. [1, Thm. 4.17] *Suponga que* $q^2 \leq m < 2q^2 - q - 2$. *Entonces*

(*i*) $d_1(C_m) = q^3 - m$;

(*ii*) $d_2(C_m) = q^3 - m + q$;

(*iii*) $d_3(C_m) = q^3 - m + q + 1$ *si* $m > q^2$.

(*iv*) *Si* $m = q^2 + aq + b$, *con* $0 \leq a \leq b \leq q - 3$, *entonces*

$$d_r(C_m) \leq q^3 - m + p_r, \quad 1 \leq r \leq (b+2)(b+3)/2 - 1,$$

donde p_r *es el* r*-ésimo agujero de* Q_∞. *En otro caso,* $d_r(C_m) \leq q^3 - m + p_r$, *para todo* $1 \leq r \leq g$, *y* p_r *es el* r*-ésimo agujero de* Q_∞.

Teorema 6.5.8. [1, Thm. 4.19] *Suponga que* $q^3 \leq m \leq q^3 + q^2 - q - 2$ *y escribimos* $m = q^3 + q^2 - q + a(q+1) + b$, *con* $0 \leq a$ *y* $0 \leq b \leq q$. *Entonces para todo* $1 \leq r \leq a + 1$ *tenemos*

$$d_r(C_m) = q - a + r + 1.$$

Los pesos generalizados de curvas hermitianas fueron determinados completamente por A. Barbero y C. Munuera en [1].

Referencias

[1] A.I. Barbero, C. Munuera, The weight hierarchy of hermitian codes. SIAM Discrete Mathematics 13(1) (1999), 79-104.

[2] H. Chen, H.S. Luk, S. Yau. Explicit computation of generalized Hamming weights for some algebraic geometric codes. Advances in Applied Mathematics 21 (1998), 124-145.

[3] V.D. Goppa. *Geometry and codes*. Kluwer Academic Publishers, 1998.

[4] R.W. Hamming. Error detecting and error correcting codes. Bell System Technical Journey 29 (1950), 147-160.

[5] W. Huffman, V. Pless. *Fundamentals of error correcting codes*. Cambridge University Press, 2003.

[6] P. Kumar, H. Stichtenoth, K. Yang. On the weight hierarchy of geometric Goppa codes. IEEE Transactions on Information Theory 40 (1994), 913-920.

[7] J. Li, D. Wan, J. Zhang, On the minimum distance of elliptic curve codes (2015). *arXiv:1501.01138*.

[8] S. Ling, C.Xing. *Coding theory a first course*. Cambridge University Press, 2004.

[9] C.J. Moreno. *Algebraic curves over finite fields*. Cambridge University Press, 1991.

[10] C. Munuera. The weight distribution of irreducible cyclic codes with block length $n((q^\ell - 1)/N)$. Discrete Mathematics 18 (1977), 179-211.

[11] C. Munuera. On MDS elliptic codes. Discrete Mathematics 117 (1993), 279-286.

[12] D. Nogin, M. Tsfasman, S. Vladut. *Algebraic geometric codes: Basic notions*. American Mathematical Society, 2007.

[13] R. Pellikaan, B.Z. Shen, G.J.M. van Wee, Which linear codes are algebraic geometric? Bell System Thechnical Journey 27 (1948), 379-423.

[14] R. Pellikaan. On the gonality of curves, abundant codes and decoding. Coding Theory and Algebraic Geometry 1518 (1992), 132-144.

[15] I.S. Reed, G. Solomon, Polynomial codes over certain finite fields. SIAM Journal of the Society for Industrial and Applied Mathematics 8 (1960, 300-304.

[16] C.E. Shannon. A mathematical theory of communications. Bell System Technical Journey 27 (1948), 379-423.

[17] J.H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics 106, 1991.

[18] T.A. Springer, J.H. van Lint. Generalized Reed-Solomon codes from algebraic geometry. IEEE Transactions of Information Theory 33 (1987), 305-309.

[19] H. Stichtenoth. Self-dual Goppa codes. Journal of Pure and Applied Algebra 55 (1988), 199-211.

[20] H. Stichtenoth, M. Tsfasman. *Coding theory and algebraic geometry*. Springer, 1992.

[21] H. Stichtenoth. *Algebraic function fields and codes*. Springer 2009.

[22] M. Tsfasman. Algebraic geometric codes and asymptotic problems. Discrete Applied Mathematics 33 (1991), 241-256.

[23] M. Tsfasman, S. Vladut. Geometric approach to higher weights. IEEE Transactions on Information Theory 41 (1995), 1564-1588.

[24] G. van der Geer, J.H. van Lint. *Introduction to coding theory and algebraic geometry*. Birkhauser, 1988.

[25] J.H. van Lint. *Introduction to coding theory*. Springer, 1998.

[26] V.K. Wei. Generalized Hamming weights for linear codes. IEEE Transactions of Information Theory 37 (1991), 1412-1418.

[27] S.B. Wicker, V.K. Bhargava, *Reed-Solomon codes and their applications*. IEEE Press, 1994.

[28] K. Yang, On the weight hierarchy of hermitian and other geometric Goppa codes. PhD Thesis, University of Southern California, 1992.