Códigos Goppa

Antonio Beato Caro

Códigos Goppa

Antonio Beato Caro

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Dr. Jose María Tornero Sánchez

Agradecimientos

A todos los profesores que he tenido en la carrera por haber conseguido fomentar mi curiosidad por las matemáticas. En especial a José María Tornero Sánchez por ese infinito (no numerable) de veces que ha leído este trabajo y haberme ayudado tanto a mejorarlo.

A todos los amigos que he hecho durante esta etapa porque son ellos los que harán que recuerde estos años como unos de los mejores de mi vida.

A mi familia por haberme dado esta oportunidad y por estar siempre ahí cuando me sentía frustrado (que no han sido pocas veces).

A Natalia porque no solo me he acompañado en este ciclo sino también lo hará en el que está por venir.

Listen to me, Morty. I know that new situations can be intimidating. You're lookin' around and it's all scary and different, but y'know … meeting them head-on, charging into 'em like a bull — that's how we grow as people.

Rick a Morty

Índice general

Resumen

El objetivo de este trabajo es servirnos de las herramientas impartidas en la asignatura de Álgebra Conmutativa y Geometría Algebraica para estudiar la teoría de códigos correctores de errores, presentada en la asignatura Teoría de Códigos y Criptografía. Esto servirá de pretexto para profundizar en temas importantes de la geometría algebraica como la teoría de divisores para curvas. Como principal aplicación para la teoría de códigos, definiremos los códigos Goppa, una familia de códigos de gran importancia histórica pues es la primera familia infinita de códigos en superar la cota de Gilbert-Varshamov.

En cuanto a la organización del trabajo, este se encuentra dividido en tres capítulos y un apéndice:

- El primer capítulo presenta, en sus tres primeras secciones un repaso de los conceptos básicos de la asignatura de Teoría de Códigos y Criptografía (Definición de código corrector de errores, corrección por mínima distancia, matrices de control, códigos cíclicos...). Las dos secciones siguientes están dedicadas a dos familias de códigos que fueron posteriormente generalizados por los códigos Goppa: los códigos BCH y los códigos de Goppa clásicos.

- En el segundo capítulo se desarrolla la geometría algebraica necesaria para definir los códigos de Goppa. El capítulo comienza exponer técnicas para describir curvas proyectivas sin puntos singulares sobre cuerpos algebraicamente cerrados a través de estudiar los llamados anillos de valoración de su cuerpo de funciones. Tras eso, se da una pequeña introducción a la teoría de divisores en dicho caso y se definen los espacios de Riemman-Roch, los cuales que serán la base de los códigos Goppa. En las últimas secciones del capítulo se define la noción de curva proyectiva abstracta que será de gran utilidad para extender la teoría a cuerpos arbitrarios.

- En el tercer y último capítulo se da la definición de la familia de los códigos Goppa así como la estimación de sus parámetros dimensión y distancia mínima. En la segunda sección, se motiva a través de la cota de Hasse-Weil, la elección de varias curvas como base para la construcción de códigos Goppa. Además, se dan las matrices generatrices de dichos códigos haciendo un análisis completo de dichos ejemplos. Por último en el resto del capítulo, se dedica una pequeña sección a hablar de la cota de Gilbert-Varshamov.

- Por último, el apéndice del trabajo elabora sobre asuntos que, aunque son de gran interés, no se han podido incluir en los capítulos principales del trabajo por falta de espacio. A pesar de ello, como estaban previstos en una primera planificación para ser estudiados, se añaden como complemento al texto principal siendo citados en repetidas ocasiones invitando al lector que ahonde en los temas expuestos. Se da una definición precisa de lo que se entiende por el género de una curva además de darse una prueba completa de la desigualdad de Riemman. Estas herramientas se utilizan para tratar la dualidad en códigos de Goppa. Para finalizar, hay una pequeña sección dedicada al estudio del grupo absoluto de Galois de un cuerpo finito.

Un último comentario en cuanto a la organización del contenido. El trabajo es extenso y largo de leer entero. Por ello, me gustaría recomendar que, en el caso de que el lector prefiera "ir al grano" y centrarse en lo importante (el último capítulo), las últimas 3 secciones de los capítulos 1 y 2 son de menor importancia que el resto del contenido para ese propósito. En especial las últimas secciones del capítulo segundo, son dedicadas a formalidades necesarias para ver que la teoría de las dos primeras secciones se extiende bien a cuerpos cualesquiera. Sin embargo la extensión es bastante natural y los resultados obtenidos son bastante parecidos a los obtenidos en la primera parte del capítulo.

Me gustaría terminar este pequeño resumen destacando un detalle. Algunos resultados que se presentan a lo largo del trabajo son muy profundos y por ello algunas demostraciones se omiten. En general, si la demostración puede seguirse pero se omite por motivos de longitud del trabajo, suelo dar una indicación de la idea de la prueba y de las herramientas que se utilizan en la misma. Por desgracia, será inevitable que a lo largo del trabajo nos encontremos unos pocos resultados que son imposibles de probar en tan solo unas pocas páginas de un trabajo de fin de grado y nos veremos obligados a asumir algunos teoremas. A pesar de todo esto, en cuanto a los resulta-

dos principales presentados en los tres primeros capítulos, todos están demostrados para el caso en el que estemos trabajando con curvas planas y, debido a que todos los ejemplos con los que construimos los códigos del capítulo 3 se basan en curvas planas, los resultados importantes del texto están todos demostrados. Hay una excepción a esto último: la fórmula de Plücker. Esta fórmula tiene una demostración un poco más compleja que el resto de resultados que precisa del teorema de Riemann-Roch en su versión completa. A pesar de ello, en el apéndice se indica una idea de cómo funcionaría la prueba conociendo el teorema de Riemann-Roch para no dejar al lector insatisfecho.

English Abstract

The goal of this project is to use the tools taught in the subject *Commutative Algebra and Algebraic Geometry* to study the theory of error-correcting codes presented in the subject Theory of Codes and Cryptography. This will serve as an excuse to delve into important topics in algebraic geometry such as the theory of divisors in curves. As the main application for the theory of codes, we will define the Goppa codes, a family of codes of historical value since it is the first infinite family of codes known to go beyond the Gilbert-Varshamov bound.

Regarding the memoir, it is divided into three chapters and an appendix:

- The first chapter presents, in its first three sections, a review of the basic concepts of the subject of Code Theory and Cryptography (definition of error–correcting code, minimum distance correction, control matrices, cyclic codes ...). The next two sections are devoted to two families of codes that were later generalized by Goppa codes: the BCH codes and the classic Goppa codes.

- In the second chapter the algebraic geometry we need to define the Goppa codes is developed. The chapter begins exposing techniques to describe projective curves without singular points on algebraically closed fields through studying the so-called evaluation rings of their body of functions. After that, a brief introduction is given to the theory of divisors in this case and the Riemman-Roch spaces are defined, which will be the basis of the Goppa codes. In the last sections of the chapter the notion of abstract projective curve is defined, which will be very useful to extend the theory to arbitrary fields.

- The third and last chapter gives the definition of the Goppa code family as well as the estimation of its dimension and minimum distance parameters. In the second section the choice of several curves as the basis for the construction of

Goppa codes is motivated through the Hasse-Weil bound. In addition, the generating matrices of those codes are given, making a complete analysis of the examples. Finally, in the rest of the chapter, a small section is devoted to discussing the Gilbert-Varshamov dimension.

- Finally, the appendix elaborates on topics that, being of great interest, have not been able to include in the main chapters of the work due to lack of space. Despite this, as they were foreseen to be studied in a first planning, they are added as a complement to the main text. A precise definition of what is meant by the genus of a curve is given in the appendix in addition to giving a complete proof of Riemman's inequality. These tools are used to deal with duality in Goppa codes. Finally, there is a small section dedicated to the study of the absolute Galois group of a finite field.

One last comment regarding the organization of the content. The work might seem long to read in its entirety. For this reason, I would like to recommend that if the reader prefers to "cut to the chase" and focus on what is important (the last chapter), the last 3 sections of the 1 and 2 chapters are less essential than the rest of the content for that purpose. Especially the last sections of the second chapter are devoted to the formalities necessary to see that the theory from the first two sections extends well to any field. However, the extension is quite natural and the results obtained are quite similar to those obtained in the first part of the chapter.

I would like to end this short summary by highlighting one detail. Some results that are presented throughout the work are very profound and therefore some proofs are omitted. In general, if the proof can be followed but it is omitted due to its length, I usually give an indication of the idea behind it and the tools used in it. Unfortunately, it will be inevitable that throughout the work we will find a few results that are impossible to prove in just a few pages of a dissertation and we will be forced to assume some theorems. Despite all this, as for the main results presented in the first three chapters, they are all proven for the case in which we are working with plane curves and, because all the examples with which we build the codes of chapter 3 are based on plane curves, the important results of the text are all proved. There is an exception to the latter: Plücker's formula. This formula has a proof a little more complex than the rest of the results required by the Riemann-Roch theorem in its complete version. Despite this, the appendix gives an idea of how the proof would work knowing the Riemann-Roch theorem so as not to leave the reader unsatisfied.

1 Conceptos generales

1.1 Introducción

Si uno ha rayado uno de los ya antiguos DVDs alguna vez en su vida, tal vez haya tenido la suerte de comprobar que, a no ser que el daño fuera demasiado grande, los lectores DVD eran capaces de acceder a su contenido sin perder nada de información, reproduciéndolo exactamente segundo a segundo como si no se hubiese rayado nunca. ¿Cómo es esto posible? El deterioro de la superficie definitivamente altera y hace que se pierda parte del contenido que el disco tuviese grabado. La respuesta a esta pregunta se halla en una manera muy precisa de almacenar la información: los códigos correctores de errores.

Planteemos el problema con antelación al incidente. Supongamos que como fabricantes de DVDs, sabemos que probablemente, tarde o temprano, nuestros discos pueden sufrir desperfectos y por tanto, decidimos utilizar parte de la capacidad de almacenamiento del DVD para, posiblemente, arreglar dichos desperfectos. Digamos que, como en última instancia es bien conocido que la información puede ser codificada de forma discreta en una sucesión de 1s y 0s, queremos almacenar un gran número escrito en código binario en nuestro DVD. Podríamos por ejemplo, almacenar el mismo número tres veces y así, cuando el lector examine la información, podría ir examinando el número cifra a cifra y en caso de que haya discordancia entre una cifra y sus dos supuestas copias, tomar como valor definitivo a leer del que haya mayor ocurrencia, como tenemos la información repetida tres veces, no es posible que haya empates. Este ejemplo es lo que se conoce como un código de repetición de longitud 3.

Esto parecería solucionar el problema. Sin embargo, el procedimiento antes descrito tiene notables desventajas, por ejemplo, a la hora de querer almacenar información,

solamente utilizamos un tercio de la capacidad disponible del disco, dejándose dos tercios de la misma como "datos redundantes". Además de esto, es sencillo darse cuenta de que este método no es capaz de lidiar con dos o más errores coincidiendo en la misma posición de una cifra en dos de las copias de los números. La teoría de códigos correctores de errores trata precisamente de generalizar esta idea a procedimientos que acaban siendo muchísimo más eficientes que el código de repetición. Por poner en perspectiva los números, el código de Hamming (cuyo creador, Richard Hamming, fue en 1950 un pionero en la materia) es, al igual que el código de repetición, un procedimiento para detectar y corregir un error que solamente usa 3/7 de la capacidad de almacenamiento para redundancia mejorando de entrada, notoriamente, los 2/3 del código anterior.

1.2 Preliminares sobre códigos correctores de errores

Para empezar el estudio de estos métodos, comencemos dando algunas definiciones. Como se ha dicho anteriormente, entendemos que a la hora de almacenar la información es posible tenerla en una forma discretizada, siendo así posible codificarla a través de una serie de caracteres (en el caso anterior, 1s y 0s). Por ello, empezamos con la siguiente definición.

Definición 1.1. *Un alfabeto Q es un conjunto no vacío de símbolos que no tienen significado individual. Una palabra o un bloque de longitud n es un elemento de Q^n.*

Ejemplo 1.1. Si entendemos que vamos a utilizar dos símbolos para transmitir información podemos asumir que $Q = \mathbb{F}_2$, el cuerpo de dos elementos, teniendo así los símbolos 0 y 1.

En este caso las n–uplas de elementos se pueden denotar indistintamente de la forma usual (por ejemplo $(0,0,0,1,1,1,0,1) \in \mathbb{F}_2^8$) o, usando una notación más compacta, yuxtaponiendo los elementos (en el ejemplo anterior 00011101).

Supondremos siempre que la información a codificar puede ser dividida en bloques de longitud n para ser descodificada de forma independiente. Esto es, que podemos dividir una larga cadena de símbolos en bloques de manera que el significado de cada palabra no depende del resto de palabras. Teniendo esto en cuenta, comencemos por los objetos con los que estudiaremos: los códigos.

Definición 1.2. *Un código C de longitud n es un conjunto no vacío de palabras, es decir es un subconjunto $C \subseteq Q^n$. Si C es finito, se llama tamaño del código a su cardinal, $\#(C)$.*

En cierto sentido, las palabras de C son las que se entienden como "palabras correctas". Es decir, de todas las posibles palabras de Q^n, nos restringiremos a almacenar la información solamente utilizando palabras de C. Así, si tenemos algún tipo de distorsión de la información y observamos palabras que no están en C, seremos capaces de detectar que ha habido un error.

Ejemplo 1.2. Si Q es un alfabeto cualquiera, el código de repetición de longitud n sobre el alfabeto Q es

$$C = \{(a, a, \dots, a) \mid a \in Q\} \subseteq Q^n$$

Para este código se suele tomar $Q = \mathbb{F}_2$ y $n = 8$.

En este caso, si en una transmisión de información en la que se usa este código, al recibir la palabra $\mathbf{c} = 00000001$ detectaríamos que ha habido un error en la transmisión ya que $\mathbf{c} \notin C$. Más aún, si la situación es adecuada, podríamos plantearnos incluso reemplazar la palabra errónea por aquella de C que "se le parezca más" (en este caso no es difícil adivinar que sería 00000000). Con este objetivo introducimos la siguiente definición.

Definición 1.3. *La distancia de Hamming en Q^n es la aplicación*

$$\begin{aligned} d : Q^n \times Q^n &\longrightarrow \mathbb{R}_{\geq 0} \\ (\mathbf{x}, \mathbf{y}) &\longmapsto \#\left\{i \mid x_i \neq y_i,\ i = 1, \dots, n\right\} \end{aligned}$$

Esto es, $d(\mathbf{x}, \mathbf{y})$ mide el número de coordenadas distintas de $\mathbf{x}$ e $\mathbf{y}$.

Proposición 1.1. La distancia de Hamming es una distancia (en el sentido topológico) sobre Q^n.

Demostración. Se dio en la asignatura de Teoría de Códigos y Criptografía. ∎

De esta forma, podemos al recibir una palabra $\mathbf{y} \in Q^n$, reemplazarla por alguna palabra de C que esté a distancia mínima:

Definición 1.4 (Descodificación por mínima distancia). *Si recibimos la palabra $\mathbf{y} \in Q^n$, se define su codificación por mínima distancia a la única palabra $\mathbf{x} \in C$ (caso de existir) que minimiza $d(\mathbf{x}, \mathbf{y})$.*

Por tanto, a la hora de descodificar por mínima distancia (la descodificación habitual en los códigos que vamos a estudiar[1]), nos interesará que las palabras del código disten entre sí lo máximo posible. En el ejemplo de antes, el código anterior tenía solamente dos palabras $C = \{00000000,\ 11111111\}$ y la distancia entre ellas es 8 por lo que si el emisor del mensaje envía una palabra del código y hay un fallo en la comunicación de esta, es necesario que se cometan 8 o más errores en la transmisión para que no se detecte el error. Se dice en este caso que C detecta 7 errores. Para medir las bondades de un código, definimos algunos parámetros de interés.

Definición 1.5. *Si $\#(Q) = q$ y dado un código $C \subseteq Q^n$, definimos:*

1. Distancia mínima del código al número

$$d(C) = \min\{d(\mathbf{x}, \mathbf{v}) \mid \mathbf{x}, \mathbf{v} \in C\}$$

2. Distancia mínima relativa del código al número

$$\delta(C) = \frac{d(C)}{n}$$

3. Tasa de transmisión de información del código al número

$$R(C) = \frac{\log_q\left(\#(C)\right)}{n}$$

4. Redundancia del código al número

$$n - \log_q\left(\#(C)\right)$$

Trataremos de construir códigos que tengan buenos parámetros concentrándonos especialmente en la distancia mínima del código y en su tasa de información ya que esta está directamente relacionada con el coste de transmisión de la información.

Observación 1.1 (Detección de errores). Si C es un código de longitud n y distancia mínima d y si $\mathbf{c} \in C$ y $\mathbf{x} \in Q^n$, se tiene que, si $d(\mathbf{c}, \mathbf{x}) < d$, entonces $\mathbf{x} \notin C$.

Decimos en este caso que el código detecta $d-1$ errores como vimos en el ejemplo anterior del código de repetición.

[1] En teoría de códigos se pueden considerar otros métodos de descodificación como los basados en métodos de máxima verosimilitud.

Observación 1.2 (Corrección de errores). Si $\mathcal{C}$ es un código de longitud n y distancia mínima d, para cualesquiera $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{C}$

$$\overline{B}\left(\mathbf{c}_1, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \cap \overline{B}\left(\mathbf{c}_2, \left\lfloor \frac{d-1}{2} \right\rfloor\right) = \varnothing$$

Dicho de otro modo, si $\mathbf{x} \in Q^n$ no es posible que:

$$d\left(\mathbf{c}_i, \mathbf{x}\right) \leq \left\lfloor \frac{d-1}{2} \right\rfloor, \quad i = 1, 2$$

Entonces si recibimos una palabra que no está en el código, $\mathbf{x} \notin \mathcal{C}$, y dista de alguna palabra de nuestro código $\mathbf{c} \in \mathcal{C}$ una cantidad menor o igual a $\lfloor (d-1)/2 \rfloor$ sabremos inmediatamente que su descodificación por mínima distancia (la palabra más cercana a $\mathbf{x}$ de nuestro código que supondremos que es la que se tenía intención de transmitir) es necesariamente la palabra $\mathbf{c}$.

Definición 1.6. *Diremos que un código $\mathcal{C}$ corrige $\lfloor (d-1)/2 \rfloor$ errores cuando se da esta situación.*

Evidentemente no tiene por qué ser siempre el caso de que cualquier palabra admita una decodificación por mínima distancia. Podríamos, a priori, recibir una palabra que no estuviera a distancia menor o igual a $\lfloor (d-1)/2 \rfloor$ de ninguna de $\mathcal{C}$ y ahí podrían surgir problemas. Existen códigos (que veremos luego) cuya construcción evita estos casos.

Los códigos en general, a nivel conjuntista, son objetos de difícil trato pues no es sencillo, en general, computar parámetros como la distancia mínima o la tasa de información de manera rápida. Por ello, vamos a dotar de un poco de estructura a los objetos con los que vamos a trabajar, introduciendo la familia de los códigos lineales.

Definición 1.7. *Un código lineal de longitud n sobre el alfabeto $Q = \mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$.*

Solemos decir que un código lineal $\mathcal{C}$ es de tipo (n, m, d) para decir que es de longitud n, tamaño m y distancia mínima d.

Observación 1.3. Si tenemos un código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$ con $\dim(\mathcal{C}) = k$, tenemos que $\mathcal{C}$ es un código de tipo (n, q^k, d) y por tanto su tasa de transmisión es $\mathcal{R}(\mathcal{C}) = k/n$.

Además, su redundancia sería $n - k$, esto es, de las n coordenadas, k son las que llevan la información lo cual es coherente con que el código sea de dimensión k.

Ejemplo 1.3 (Código del bit de paridad). Si nuestro alfabeto es $\mathcal{Q} = \mathbb{F}_q$, el código del bit de paridad de longitud n es el conjunto:

$$C = \left\{ (c_1, \dots, c_n) \in \mathbb{F}_q^n \;\middle|\; \sum_{k=1}^{n} c_k = 0 \right\}.$$

El nombre de este código está inspirado en el caso en el que $\mathcal{Q} = \mathbb{F}_2$ en cuyo caso, el último elemento de cada vector se conoce como bit de paridad y controla si la palabra que se transmite es de suma par o impar.

Está claro que entonces $n = q^n$, y $\dim(C) = q^{n-1}$ por venir el código dado por una ecuación implícita. Nos falta ver su distancia mínima. Pronto veremos que, gracias a que el sistema viene dado por una ecuación implícita, es fácil ver que $d = 2$. Para ello, hablemos un poco de la distancia mínima en un código lineal.

Proposición 1.2. En un código lineal $C \subseteq \mathbb{F}_q^n$ se tiene que

$$d(C) = \min \left\{ d(\mathbf{c}, \mathbf{0}) \mid \mathbf{c} \in C \setminus \{\mathbf{0}\} \right\}.$$

Demostración. Basta observar que si $\mathbf{x}, \mathbf{y} \in C$, entonces $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} - \mathbf{y}, \mathbf{0})$ pero como C es cerrado para la suma, $\mathbf{x} - \mathbf{y} \in C$.

A la cantidad $d(\mathbf{x}, \mathbf{0})$ para una palabra $\mathbf{x} \in \mathbb{F}_q^n$ se le denomina el peso de $\mathbf{x}$, se denotará por $w(\mathbf{x})$ y por tanto, con esta nomenclatura, la distancia mínima de un código C coincide con el mínimo peso de las palabras no nulas del código. Veamos que podemos caracterizar esta cantidad de manera algebraica. Para ello, usemos la estructura de espacio vectorial de dimensión finita de los códigos lineales.

Definición 1.8. *Sea $C \subset \mathbb{F}_q^n$ un código lineal. Si C viene expresado por un sistema de ecuaciones implícitas independientes,*

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{0} \in \mathcal{M}\left((n-k) \times 1, \mathbb{F}_q\right)$$

diremos que A es una matriz de control de C.

La existencia de una matriz de control ya proporciona una ventaja considerable de los códigos lineales frente a los que no lo son desde el punto de vista de la práctica pues en vez de tener que almacenar todas las palabras del código, basta con saber cuál

es la matriz de control para ir comprobando si las palabras recibidas pertenecen o no a $\mathcal{C}$. Además, esta matriz nos da una manera sencilla de calcular la distancia mínima de $\mathcal{C}$.

Teorema 1.1 (Distancia mínima mediante una matriz de control). *Si A es una matriz de control de un código lineal $\mathcal{C}$, la distancia mínima de $\mathcal{C}$ es la menor cantidad de columnas de A que necesitamos para formar un conjunto linealmente dependiente.*

Demostración. Probaremos que existe un vector de peso exactamente r en el código si y sólo si existe una combinación lineal de exactamente r columnas con coeficientes no nulos que da $\mathbf{0}$. Sea $\mathbf{x} \in \mathcal{C}$, con $w(\mathbf{x}) = r$. Entonces

$$\mathbf{x} \in \mathcal{C} \iff A\mathbf{x} = \mathbf{0} \iff x_1 C(A)_1 + \cdots + x_n C(A)_n = \mathbf{0} \in \mathbb{F}_q^{n-k}$$

donde exactamente r de las n coordenadas de $\mathbf{x}$ son no nulas. Por tanto, d es precisamente el cardinal del menor conjunto de columnas de A que formen un conjunto linealmente dependiente. ∎

Con esta proposición podemos hallar la distancia mínima de un código sin necesidad de conocer el peso de todas las palabras del código. Por ejemplo, ahora está claro que la distancia mínima del código del ejemplo 1.3 es $d = 2$. Veamos como aplicación adicional la distancia mínima del código de Hamming original, el primer ejemplo de códigos correctores de errores de la historia.

Ejemplo 1.4 (Código de Hamming original). El código de Hamming original puede ser introducido de una gran variedad de formas, cada una apoyándose y resaltando alguna de las muchas propiedades que este código posee. Nosotros lo veremos como las soluciones de un sistema de ecuaciones, es decir, por su matriz de control.

El código de Hamming original se construye sobre $\mathcal{Q} = \mathbb{F}_2$, como el conjunto de soluciones en $\mathbb{F}_2^7$ del sistema

$$\begin{cases} x_1 + x_3 + x_5 + x_7 = 0 \\ x_2 + x_3 + x_6 + x_7 = 0 \\ x_4 + x_5 + x_6 + x_7 = 0 \end{cases}$$

Esto es, una matriz de control del código es

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Es sencillo comprobar que la distancia mínima del código es 3 ya que dos a dos las columnas de A no son colineales y la primera y segunda columna suman la tercera.

Por tanto, en este caso diríamos que el código de Hamming es un código lineal $(n = 7, m = 2^4, d = 3)$. Esto quiere decir que el código de Hamming original es un código que detecta $d - 1 = 2$ errores y corrige $\lfloor (d-1)/2 \rfloor = 1$ error. Su tasa de transmisión sería $\mathcal{R}(\mathcal{C}) = k/n = 4/7$. En breve veremos qué hace al código de Hamming un código con tan buenas propiedades.

De la misma forma, podemos introducir un código lineal $\mathcal{C}$ a través de un sistema de generadores. Codificamos esta información en una matriz con la siguiente definición.

Definición 1.9. *Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal. Diremos que $\mathcal{M}$ es una matriz generatriz de $\mathcal{C}$ cuando las columnas de $\mathcal{M}$ formen una base de $\mathcal{C}$ como subespacio vectorial.*

Observación 1.4. De la propia definición se deduce que $\mathcal{M}$ es una matriz de rango la dimensión de $\mathcal{C}$ como espacio vectorial y que además verifica que, si A es una matriz de control de $\mathcal{C}$, entonces $A \cdot \mathcal{M} = 0$.

Por último, es importante si estamos tratando de optimizar ciertos parámetros de los códigos, estudiar las relaciones que hay entre ellos. A continuación haremos precisamente eso, veremos cotas asociadas a los códigos lineales que son de vital importancia a la hora de establecer si ciertas combinaciones de parámetros son óptimas o no.

Observación 1.5. Si $\mathcal{C}$ es un código lineal, debido a que la distancia de Hamming es invariante por traslación, se tiene que para todo $\mathbf{x} \in \mathcal{Q}^n$ y para todo $r \in \mathbb{Z}_{\geq 0}$,

$$\#\left(\overline{B}(\mathbf{x}, r)\right) = \#\left(\overline{B}(\mathbf{0}, r)\right)$$

por lo que designaremos a este número por $V(r)$.

Proposición 1.3. En las condiciones anteriores

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

Demostración. Basta observar que para cada j fijo existen

$$\binom{n}{j} (q-1)^j$$

vectores en Q^n de peso exactamente j, pues tenemos n posibles coordenadas de las cuales exactamente j son no nulas (de ahí el número combinatorio) y en cada una de las coordenadas no nulas escogidas tenemos $q-1$ posibilidades (de ahí el término $(q-1)^j$).

Teorema 1.2 (Cota de Hamming). *Si C es un código lineal de longitud n que corrige t errores (recordemos que $t = \lfloor (d-1)/2 \rfloor$) entonces*

$$mV(t) \leq q^n,$$

siendo m el tamaño de C.

Demostración. Como C corrige t errores, las bolas centradas en las palabras de C con radio t son disjuntas luego la suma de los cardinales de estas bolas es menor a la cantidad de palabras del espacio total, que es q^n.

A los códigos que alcanzan la igualdad en esta cota se les denomina *códigos perfectos* y son los códigos en los cuales las bolas centradas en las palabras de C y de radio la capacidad de corrección t recubren todo el espacio, luego la detección y la corrección de errores son equivalentes. No hay muchos códigos perfectos y su clasificación es un problema ya resuelto y bien conocido[2].

Veamos ahora que la dimensión del código (y por tanto la tasa de transmisión) y la distancia mínima de un código no pueden crecer demasiado al mismo tiempo.

Teorema 1.3 (Cota de Singleton). *Si C es un código lineal de tipo (n, q^k, d) sobre $\mathbb{F}_q$, entonces*

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

Demostración. Si A es una matriz de control de C, la distancia mínima de C es el mínimo número de columnas linealmente dependientes de A. Como el rango de A es $n-k$, este número es, a lo más, $n-k+1$ luego $d \leq n-k+1$.

A los códigos que alcanzan la igualdad se les llama códigos de máxima distancia de separación o MDS. La familia de códigos MDS, al contrario que los códigos perfectos, presentan problemas aún abiertos en teoría de códigos.

Por último, acabemos con una cota de existencia, es decir, una cota que debe superar al menos algún código lineal.

[2]Los únicos códigos perfectos son los de la familia de códigos de Hamming y los de la familia de códigos de Golay. Para más información ver [3].

Teorema 1.4 (Cota de Gilbert-Shannon-Varshamov). *Si se verifica que*

$$q^{n-k+1} > V(r-1),$$

entonces existe un código lineal de tipo (n, q^k, d) *con* $d \geq r$.

Demostración. La prueba se trata de dar una construcción inductiva. Sea $\mathbf{c}_1$ un vector de peso mayor o igual que r, $w(\mathbf{c}_1) \geq r$ y tomamos $C_1 = \langle \mathbf{c}_1 \rangle$.

En el paso de inducción seleccionados $\mathbf{c}_1, \ldots, \mathbf{c}_{i-1}$ independientes generadores de un código lineal C_{i-1} con parámetros (n, q^{i-1}, d), con $d \geq r$, por hipótesis de inducción se tiene que

$$q^{j-1}V(d-1) < q^n,$$

por lo que existe al menos un vector $\mathbf{c}_i \in \mathbb{F}_q^n$ que dista al menos r de todas las palabras de C_{i-1} entonces $C_i = \langle \mathbf{c}_1, \ldots, \mathbf{c}_i \rangle$ es el código buscado. ∎

La cota de Gilbert-Shannon-Varshamov tiene un gran valor histórico para la teoría de códigos pues el encontrar familias de códigos (no códigos individuales, que se pueden construir siguiendo la demostración) que superasen esta cota fue un reto para la disciplina.

Analicemos por último las cotas del ejemplo del código de Hamming original.

Ejemplo 1.5 (Cotas del código de Hamming original). Para empezar,

$$mV(t) = 2^4 V(1) = 2^4 \left[\binom{7}{0} + \binom{7}{1} \right] = 2^4 \cdot 8 = 2^7 = q^n,$$

luego el código de Hamming original es un código perfecto.

Por otro lado,

$$k + d = 4 + 3 = 7 < 8 = n + 1,$$

luego el código de Hamming original no es un código MDS.

Terminemos la sección con una manera de construir códigos a partir de otros que nos será de utilidad en capítulos posteriores. Consideremos un código lineal C de tipo (n, q^k, d) sobre un cuerpo de q elementos y con $q = r^m$ una potencia (donde r no es necesariamente un primo, lo importante es que es una potencia m-ésima). Supongamos que tenemos otro código lineal C' de tipo (n', r^m, d') sobre un cuerpo de r elementos.

Denotemos, abusando de la notación, por C y C' las aplicación lineales que consisten en multiplicar por las matrices generatrices de C y C' respectivamente a la izquierda. En tal caso, podemos componer los dos códigos C y C' como sigue:

$$\mathbb{F}_q^k \xrightarrow{C} \mathbb{F}_q^n \xrightarrow{\sim} \left(\mathbb{F}_r^m\right)^n \xrightarrow{(C',\dots,C')} \left(\mathbb{F}_r^{n'}\right)^n$$

Donde el isomorfismo entre $\mathbb{F}_q^n$ y $(\mathbb{F}_r^m)^n$ consiste en escribir cada elemento de $\mathbb{F}_q$ en una base de $\mathbb{F}_r^m$ y concatenar los n vectores resultantes en el mismo orden.

Definición 1.10. *La imagen de la composición anterior se denomina codigo lineal concatenación de C y C'.*

Calculemos los parámetros de este código.

Proposición 1.4. En las condiciones anteriores, la concatenación de C y C' es un código lineal de tipo $(n'n, r^{km}, D)$ con $D \geq d'd$.

Demostración. Que es un código lineal está claro por ser la imagen de un subespacio por una serie de aplicaciones lineales. Su primer parámetro es $n'n$ por la dimensión del espacio ambiente en el que está inmerso. Además, como el rango de una matriz generatriz es máximo, cada una de las aplicaciones que aparecen en el diagrama anterior es inyectiva luego la dimensión de la imagen es igual a la dimensión de la partida. Como nuestro espacio inicial es dimensión k sobre $\mathbb{F}_q$, tendrá dimensión mk sobre $\mathbb{F}_r$ (ya que $q = r^m$) luego se tiene el resultado para la dimensión. Veamos por último la cota inferior para la distancia mínima.

Sea $\mathbf{c} \in \mathrm{Im}(C)$. En tal caso $w(\mathbf{c}) \geq d$ por ser una palabra del código. Entonces escribiendo cada entrada de $\mathbb{F}_q^n$ como un vector de $\mathbb{F}_r^m$ (a través del isomorfismo del diagrama), los elementos no nulos de $\mathbb{F}_q$ serán no nulos en $\mathbb{F}_r^m$ luego tendremos al menos d vectores de tamaño m no nulos de los n posibles en $(\mathbb{F}_r^m)^n$. Al aplicar C' a cada uno de estos vectores de tamaño m no nulos, obtendremos una palabra no nula del segundo código luego su peso debe ser al menos d'. Por tanto, en total tendremos que una palabra en el código de concatenación deberá tener al menos peso dd' luego $D \geq dd'$.

Volveremos sobre los códigos concatenados en algunas construcciones que haremos en el último capítulo.

1.3 Códigos cíclicos

Los códigos cíclicos son una clase de familias de códigos lineales cuya relación con el anillo de polinomios en una variable con coeficientes en el cuerpo base es muy estrecha.

Definición 1.11. *Un código lineal $C \subset \mathbb{F}_q^n$ se dice que es cíclico si para toda palabra* $\mathbf{c}$ *se tiene que*

$$\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C \;\Rightarrow\; (c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

De ahora en adelante supondremos que $\mathrm{mcd}(n, q) = 1$ para el estudio de las propiedades de los códigos cíclicos.

La definición de los códigos cíclicos no parece encerrar la estructura algebraica prometida, ya que más bien parece una propiedad combinatoria y no algebraica. Sin embargo, identificando $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]$ de la forma usual

$$(a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n \;\longleftrightarrow\; a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x],$$

se tiene el siguiente resultado:

Teorema 1.5. *Un código C en $\mathbb{F}_q^n$ es cíclico si y solo si C visto en el anillo de polinomios es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.*

Demostración. Si C es un código cíclico, la suma es cerrada por ser un código lineal. Por tanto, solo habría que ver si multiplicando un elemento de C por cualquier elemento de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ nos quedamos en C. Sin embargo, al ser polinomios y ser la suma cerrada, en realidad basta ver que al multiplicar por $x \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ no nos salimos de C.

Pero eso está claro porque si tomamos el producto

$$(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \cdot x = a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}$$

que es un polinomio de C puesto que es un código cíclico.

Análogamente si tenemos un ideal del cociente, por ser el conjunto cerrado para el producto por x, el código correspondiente es cíclico. ∎

Recordemos que por ser $\mathbb{F}_q[x]$ un dominio de ideales principales, todos los ideales del cociente $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ estarán generados por un solo elemento $g(x) \in \mathbb{F}_q[x]$. Este

polinomio, si genera un ideal no trivial, podemos suponer sin pérdida de generalidad que será un divisor de $x^n - 1$. Por tanto. si tomamos la descomposición de $x^n - 1$ en sus factores irreducibles $x^n - 1 = f_1(x) \cdot \ldots \cdot f_r(x)$, podemos tomar $g(x)$ de 2^r maneras diferentes.

Definición 1.12. *En las condiciones anteriores a $g(x)$ se le llama un polinomio generador del código y al polinomio $h(x) = (x^n - 1)/g(x)$ un polinomio de control.*

Veamos que podemos dar la dimensión del código generado por $g(x)$ muy fácilmente.

Proposición 1.5. Sea $\mathcal{C} = \langle g(x) \rangle \subseteq \mathbb{F}_q[x]/\langle x^n - 1 \rangle$ un código cíclico, con $\deg(g) = n - k$. Entonces

$$\mathscr{B} = \left\{ g(x), xg(x), \ldots, x^{k-1}g(x) \right\}$$

es una base de $\mathcal{C}$ como espacio vectorial.

Demostración. Supongamos que tomamos un elemento genérico $f(x)g(x) \in \mathcal{C}$, para $f(x) \in \mathbb{F}_q[x]$ y sea $f_0(x)$ el resto de $f(x)$ módulo $h(x)$. Entonces

$$f(x)g(x) - f_0(x)g(x) = \big(f(x) - f_0(x)\big) \cdot g(x) = q(x)h(x)g(x) \in \langle x^n - 1 \rangle$$

con lo cual

$$f(x)g(x) = f_0(x)g(x) \pmod{x^n - 1}$$

Por tanto en vez de tomar fg podemos tomar $f_0 g$ y como f_0 tiene grado menor que k, está claro que $f_0 g$ se escribe como combinación lineal de los polinomios de $\mathscr{B}$.

Por otro lado, los elementos de $\mathscr{B}$ son linealmente independientes ya que cualquier combinación lineal de estos elementos se puede escribir como $g(x)f(x)$ para $f(x)$ de grado menor que $k-1$ por lo cual para que el producto sea 0 en $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ tenemos que $f(x)$ solo puede ser la combinación lineal trivial.

Corolario 1.1. Si $g(x) = g_0 + \ldots + g_{n-k}x^{n-k}$ es un polinomio generador del código $\mathcal{C}$ de grado $n - k$, entonces $\dim(\mathcal{C}) = k$ y una matriz generatriz del código es:

$$\mathcal{M} = \begin{pmatrix} g_0 & 0 & 0 & \cdots & 0 \\ g_1 & g_0 & 0 & \cdots & 0 \\ g_2 & g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ & & & & g_0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_{n-k} \end{pmatrix} \in \mathcal{M}\left(n \times k; F_q\right)$$

Corolario 1.2. Si $h(x) = h_0 + \ldots + h_k x^k$ es un polinomio de control del código $\mathcal{C}$ de grado k, entonces $\dim(\mathcal{C}) = k$ y una matriz de control del código es:

$$A = \begin{pmatrix} 0 & \ldots & & \ldots & h_2 & h_1 & h_0 \\ 0 & \ldots & & \ldots & h_1 & h_0 & 0 \\ 0 & \ldots & & \ldots & h_0 & 0 & 0 \\ \vdots & \iddots & & \iddots & \vdots & \vdots & \vdots \\ h_k & \ldots & h_0 & \ldots & 0 & 0 & 0 \end{pmatrix} \in M\left((n-k) \times n, \mathbb{F}_q\right)$$

La familia de códigos cíclicos más importante es la de los códigos BCH denominados así en honor a sus descubridores Bose, Chaudhuri y Hocquenghem.

1.4 Códigos BCH

Podríamos dedicar toda la extensión de este documento a hablar de los códigos BCH, puesto que el tema es muy amplio. Además no solo es de interés teórico, sino que presenta una variada gama de aplicaciones.[3] A pesar de esto, nos limitaremos solo a introducir su construcción para que nos sirva de motivación a la hora de persentar los objetos que nos van a interesar: los códigos de Goppa.

Consideremos en $\mathbb{F}_q[x]$ un polinomio $g(x) = f_1(x) \cdot \ldots \cdot f_r(x)$, con factores $f_i(x)$ que no se anulen en $x = 0$, que sean irreducibles y distintos dos a dos. Sea α_i un cero de $f_i(x)$ para $1 \leq i \leq r$, que se hallará en principio en una extensión algebraica de $\mathbb{F}_q$.

Proposición 1.6. En las condiciones anteriores, $g(x)$ divide a $x^n - 1$ para algún $n \in \mathbb{N}$.

Demostración. Como α_i son raíces de los polinomios $f_i(x)$, deben estar en alguna extensión finita de $\mathbb{F}_q$, digamos $\mathbb{F}_{q^{m_i}}$.

Sea entonces n_i el orden de estos α_i en $\mathbb{F}_{q^{m_i}}^*$. Esto es, $\alpha_i^{n_i} = 1$ y por tanto sus polinomios mínimos $f_i(x)$ dividen a los polinomios $x^{n_i} - 1$ Entonces, si tomamos $n = \text{mcm}(n_1, \ldots, n_r)$, está claro que todos los f_i dividen a $x^n - 1$. ∎

Si consideramos entonces el conjunto

$$\mathcal{C} = \left\{ c(x) \in \mathbb{F}_q[x]/\langle x^n - 1 \rangle \;\middle|\; c(\alpha_1) = \ldots = c(\alpha_r) = 0 \right\},$$

[3] Los códigos BCH son de los más utilizados en la tecnología actual a la hora de almacenar información.

tenemos entonces que $\mathcal{C}$ es un código cíclico de $\mathbb{F}_q^n$, que además verifica que $g(x) = f_1(x) \cdot \ldots \cdot f_r(x)$ es un polinomio generador del código.

Tratemos de dar una matriz de control para $\mathcal{C}$. Teniendo en cuenta que queremos que se verifique que $c(\alpha_1) = \cdots = c(\alpha_r) = 0$, podríamos proponer como matriz de control la matriz

$$A' = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \alpha_r^2 & \cdots & \alpha_r^{n-1} \end{pmatrix}$$

Sin embargo nótese que A' no es una matriz de control pues no tiene entradas en $\mathbb{F}_q$ sino en las extensiones $\mathbb{F}_{q^{m_i}}$. Sin embargo, podemos considerar estas extensiones como $\mathbb{F}_q$–espacios vectoriales y ver sus elementos como vectores columna en $(\mathbb{F}_q)^m$ donde m es tal que $\mathbb{F}_{q^m}$ contiene a todas las extensiones $\mathbb{F}_{q^{m_i}}$ y podemos sustituir cada elemento de la matriz A' por sus coordenadas (en $\mathbb{F}_q$) obteniéndose así una matriz con entradas en el cuerpo adecuado. Al hacer esto, es posible que hayamos creado algunas filas linealmente dependientes, dependiendo de cómo se escoja m, y por tanto tendríamos que eliminar estas filas para obtener una verdadera matriz de control de $\mathcal{C}$ (no se probará que el resultado es de hecho una matriz de control pero no es un resultado difícil de seguir).

Aunque A' no actúa como una verdadera matriz de control sí que nos sirve para medir la distancia mínima del código que, como sabemos, es el parámetro que más nos interesa controlar.

Proposición 1.7. La distancia mínima de $\mathcal{C}$ es mayor o igual que d si cualesquiera $d-1$ columnas de A' son linealmente independientes (sobre la mínima extensión que contenga a todos los α_i).

Demostración. Basta observar que si se verifica la proposición, el código lineal que da $\mathcal{C}$ sobre el cuerpo extendido tiene distancia mínima mayor o igual que d por lo que al restringirnos solo a las palabras que tengan coordenadas en $\mathbb{F}_q$ la distancia entre dos palabras dadas no puede disminuir. ∎

En general, esta distancia sigue siendo de difícil computación para una elección arbitraria de los α_i. Sin embargo si escogemos las raíces de una forma concreta, veremos que podremos obtener muy fácilmente una cota inferior para la distancia del código.

Definición 1.13. *Sea α una raíz n–ésima de la unidad en $\mathbb{F}_q$. Sea $g(x)$ el mínimo común múltiplo de los polinomios mínimos de*

$$\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\lambda-2}.$$

El código cíclico generado por $g(x)$ se denomina código BCH sobre $\mathbb{F}_q$ de longitud n y distancia mínima prevista λ.

Justifiquemos el nombre a través de la siguiente proposición.

Proposición 1.8 (Distancia mínima de los códigos BCH). Si C es un código BCH de distancia prevista λ, su distancia mínima d es mayor o igual que λ.

Demostración. Basta observar que en este caso la matriz A' tiene la forma

$$\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\lambda-2} & \alpha^{2(b+\lambda-2)} & \cdots & \alpha^{(n-1)(b+\lambda-2)} \end{pmatrix}$$

Y cualquier menor de tamaño $(\lambda-1)\times(\lambda-1)$ es un determinante de tipo Vandermonde que sabemos que es no nulo probándose así que cualesquiera $\lambda-1$ columnas son linealmente independientes y que por tanto la distancia mínima del código es mayor o igual que λ.

En general, la distancia mínima del código puede ser mayor estrictamente a λ como se ilustra en el siguiente ejemplo.

Ejemplo 1.6. Consideremos códigos BCH binarios ($q = 2$) para este ejemplo. Fijemos además parámetros $b = 1$ y $n = 2^m - 1$, para algún $m \in \mathbb{Z}$. Un código BCH de esta forma se llama un código BCH en sentido estricto ($b = 1$) y primitivo ($n = q^m - 1$).

Sea entonces $\alpha \in \mathbb{F}_{2^m}$ una raíz primitiva n-ésima de la unidad (esto es, un elemento que genera $\mathbb{F}_{2^m}^*$ como grupo cíclico).

Si tomamos $\lambda = 2$ obtenemos el conjunto

$$C_2 = \left\{ c(x) \in \mathbb{F}_2[x]/\langle x^n - 1\rangle \;\middle|\; c(\alpha) = 0 \right\}$$

Ahora bien, como estamos en un cuerpo de característica 2 y los coeficientes de los polinomios c están en $\mathbb{F}_2$ (y por tanto quedan invariantes al elevarlos al cuadrado),

si $c(\alpha) = 0$, entonces $c(\alpha^2) = 0$ y por tanto de hecho se tiene que

$$C_2 = C_3 = \left\{ c(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle \;\middle|\; c(\alpha) = c(\alpha^2) = 0 \right\}$$

Por lo que C_2 es un código de distancia mínima mayor o igual que 3 a pesar de que su distancia prevista fuera 2. De hecho, es posible comprobar que, salvo reordenación de las variables, este código coincide con el código original de Hamming presentado en el ejemplo 2.1 siendo su distancia mínima exactamente 3.

El estudio de la distancia real de los códigos BCH no es factible en general en la práctica por lo que se suele utilizar λ normalmente como sustituto. Existen algunos casos particulares en los que sí se puede averiguar con precisión esta distancia, y esta sería la discusión que vendría a continuación, de tratar este documento sobre códigos BCH. Sin embargo, como se ha dicho anteriormente, solo introducimos estos códigos para motivar los códigos de Goppa que vendrán a continuación por lo que nos limitaremos a dar una referencia donde se puede encontrar un tratamiento más extenso sobre este caso (puede verse en [4]).

1.5 Códigos de Goppa clásicos

Los códigos de Goppa[4] clásicos son una de las muchas generalizaciones de los códigos BCH. Para motivar su definición, recordemos que un código BCH (en sentido estricto, esto es $b = 1$) de longitud n y distancia prevista λ está definido como

$$C = \left\{ \left(c_0, \dots, c_{n-1}\right) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=0}^{n-1} c_i \left(\alpha^j\right)^i = 0,\ 1 \leq j \leq \lambda - 1 \right\}$$

Supongamos entonces la factorización de $x^n - 1$ en una extensión adecuada de $\mathbb{F}_q$ es

$$x^n - 1 = (x - \alpha) \cdots \left(x - \alpha^{-1}\right) \cdots (x - 1).$$

Dividiendo esta expresión por $x - \alpha^{-i}$ se obtiene que

$$\frac{x^n - 1}{x - \alpha^{-i}} = \sum_{k=0}^{n-1} (\alpha^{-i})^{n-1-k} x^k = \sum_{k=0}^{n-1} \alpha^{i(k+1)} x^k,$$

[4]En honor de Valery Denisovich Goppa, matemático ruso nacido en 1939 que los introdujo por primera vez.

donde simplemente hemos desarrollado el producto y agrupado términos. Ahora bien, si $(c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$, multiplicando por c_i y sumando en i se tiene que

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha^{-i}} = \frac{1}{x^n - 1} \sum_{i=0}^{n-1} c_i \sum_{k=0}^{n-1} \alpha^{i(k+1)} x^k$$

si $(c_0, \dots, c_{n-1})$ fuera una palabra del código, los términos de la derecha de grado menor o igual a $\lambda - 1$ se cancelarían obteniéndose así que lo restante es un múltiplo de $x^{\lambda-1}$ esto es:

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \alpha^{-i}} = \frac{x^{\lambda-1} p(x)}{x^n - 1}$$

para un cierto polinomio $p(x)$. Esto es, si la palabra está en el código, se tiene que $\sum_{i=0}^{n-1} c_i/(x - \alpha^{-i})$ escrita como función racional $p(x)/q(x)$ tiene numerador divisible por $x^{\lambda-1}$. Esto también funciona en la dirección contraria, pues caso de ser tener esta suma escrita como función racional denominador múltiplo de $x^{\lambda-1}$, observando el término de la derecha se tendría que los términos correspondientes a grado de x menor a $\lambda - 1$ se anularían lo que implica que la palabra está en el código. Generalizamos esta observación para introducir la definición de código de Goppa clásico:

Definición 1.14 (Código de Goppa clásico). *Sea $g(x)$ un polinomio mónico sobre $\mathbb{F}_{q^m}$ de grado t sin raíces dobles y $L = \{\gamma_0, \dots, \gamma_{n-1}\} \subseteq \mathbb{F}_{q^m}$ tal que $g(\gamma_i) \neq 0$, para cada $0 \leq i \leq n - 1$.*

El código de Goppa clásico de parámetros L y g (denotado como $\Gamma(L, g)$) es el conjunto de palabras $(c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$ tales que

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0 \qquad \text{mód } g(x).$$

Claramente así definidos, los códigos de Goppa clásicos son códigos lineales de longitud n. Además, por la condición de que $g(\gamma_i) \neq 0$, el elemento $x - \gamma_i$ será invertible en el anillo $\mathbb{F}_{q^m}[x]/\langle g(x) \rangle$. En concreto

$$\frac{1}{x - \gamma_i} = \frac{-1}{g(\gamma_i)} \left(\frac{g(x) - g(\gamma_i)}{x - \gamma_i} \right)$$

Por tanto, debemos entender $1/(x - \gamma_i)$ como la única clase del anillo $\mathbb{F}_{q^m}[x]/\langle g(x) \rangle$, pongamos $f(x)$, tal que $(x - \gamma_i) f(x) \equiv 1 \mod g(x)$.

Observación 1.6. En general los códigos de Goppa clásicos no son cíclicos. Sí lo son en el caso en el que $g(x) = x^{\lambda-1}$ y $L = \{\alpha^{-i} \mid 0 \leq i \leq n-1\}$ pues, como hemos observado anteriormente, coincide con un código BCH en sentido estricto.

Observación 1.7. Si $g(x)$ es un polinomio irreducible (o sea, $t > 1$), entonces la condición $g(\gamma_i) \neq 0$ se verifica siempre.

Tratemos de dar una matriz de control para un código de Goppa clásico. Digamos que $g(x) = g_0 + g_1 x + \ldots + g_t x^t$. Recordando que

$$\frac{1}{x-\gamma_i} = \frac{-1}{g(\gamma_i)}\left(\frac{g(x)-g(\gamma_i)}{x-\gamma_i}\right),$$

tenemos que

$$\frac{g(x)-g(\gamma_i)}{x-\gamma_i} = g_t\left(x^{t-1} + x^{t-2}\gamma_i + \ldots + \gamma_i^{t-1}\right) + \ldots + g_2\left(x+\gamma_i\right) + g_1$$

dividiendo por $-g(\gamma_i)$ para obtener la inversa de $x-\gamma_i$, podemos comprobar que una matriz de control para un código de Goppa clásico es:

$$A = \begin{pmatrix} \frac{-g_t}{g(\gamma_0)} & \cdots & \frac{-g_t}{g(\gamma_{n-1})} \\ \frac{-(g_{t-1}+g_t\gamma_0)}{g(\gamma_0)} & \cdots & \frac{-(g_{t-1}+g_t\gamma_{t-1})}{g(\gamma_{n-1})} \\ \vdots & & \vdots \\ \frac{-\left(g_1+g_2\gamma_0+\ldots+g_t\gamma_0^{t-1}\right)}{g(\gamma_0)} & \cdots & \frac{-\left(g_1+g_2\gamma_{n-1}+\ldots+g_t\gamma_{n-1}^{t-1}\right)}{g(\gamma_{n-1})} \end{pmatrix}$$

Observación 1.8. Al igual que pasaba en los códigos BCH, esta matriz no es una matriz de control en el sentido clásico pues no tiene coeficientes en $\mathbb{F}_q$ en general. Sin embargo, si se sustituye cada entrada de la matriz por un vector columna tomando coordenadas en el cuerpo base se obtendría, tras eliminar filas redundantes, una matriz de control real del código.

Además, esta matriz puede escribirse como el producto de las matrices

$$A = \begin{pmatrix} g_t & 0 & \cdots & 0 \\ g_{t-1} & g_t & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_0 & g_1 & \cdots & g_t \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \cdots & \gamma_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{t-1} & \gamma_1^{t-1} & \cdots & \gamma_{n-1}^{t-1} \end{pmatrix} \begin{pmatrix} g(\gamma_0)^{-1} & & & \\ & g(\gamma_1)^{-1} & & \\ & & \ddots & \\ & & & g(\gamma_{n-1})^{-1} \end{pmatrix}$$

Como la matriz de la izquierda es invertible ($g_t \neq 0$), podemos tomar el producto de las otras dos como matriz de control del código. Esto es, una matriz de control de un código de Goppa clásico sería:

$$H = \begin{pmatrix} g(\gamma_0)^{-1} & g(\gamma_1)^{-1} & \cdots & g(\gamma_{n-1})^{-1} \\ \gamma_0 g(\gamma_0)^{-1} & \gamma_1 g(\gamma_1)^{-1} & \cdots & \gamma_{n-1} g(\gamma_{n-1})^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{t-1} g(\gamma_0)^{-1} & \gamma_1^{t-1} g(\gamma_1)^{-1} & \cdots & \gamma_{n-1}^{t-1} g(\gamma_{n-1})^{-1} \end{pmatrix}$$

Gracias a esta matriz de control, podemos dar una cota de la distancia mínima y la dimensión de los códigos de Goppa clásicos.

Proposición 1.9 (Parámetros de los códigos de Goppa clásicos). Si C es un código de Goppa clásico $\Gamma(L, g)$, se tiene que:

1) $k = \dim_{\mathbb{F}_q}(C) \geq n - mt$,

2) $d = d(C) \geq t + 1$,

donde t es el grado de $g(x) \in \mathbb{F}_{q^m}[x]$.

Demostración. Si sustituimos en H cada término por un vector columna tomando coordenadas en una base de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial, obtenemos tras eliminar filas redundantes, una matriz de control en el sentido clásico de C. Esta matriz tendría dimensiones $p \times n$ con $p \leq mt$ lo que prueba el primer apartado (pues la dimensión sería $n - p \geq n - mt$).

La cota de la distancia mínima puede deducirse rápidamente de la definición ya que, como el código es lineal su distancia mínima coincide con el mínimo peso de las palabras del código. Por tanto, si $c \in C$ tiene peso w, en la expresión

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0 \mod g(x)$$

podemos tomar su expresión racional quedando así en el numerador un polinomio de grado a lo más $w-1$ (puesto que el el numerador aparecerían los productos de los c_i no nulos por el resto de los $x-\alpha_j$ correspondientes a c_j no nulos) y en el denominador un producto de polinomios de grado 1 que sabemos que no influyen para ver si el polinomio es 0 módulo $g(x)$. Por tanto, como g es mónico de grado t, la única manera de que un polinomio de grado $w-1$ sea 0 módulo $g(x)$ es que $w-1 \geq t$ probando así la desigualdad de la distancia.

En el caso en el que el cuerpo base es $\mathbb{F}_2$ se puede mejorar la cota de la distancia. Hemos de introducir un lema previo.

Lema 1.1. Sea $f(x) = \prod_{i=1}^{n}(x-a_i)^{b_i}$. Entonces el cociente de su derivada formal por sí mismo es

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^{n} \frac{b_i}{x-a_i}.$$

Demostración. Por la derivada del producto para n funciones se tiene que

$$f'(x) = \sum_{k=1}^{n} b_k(x-a_k)^{b_k-1} \prod_{i\neq k}(x-a_i)^{b_i}$$

Dividiendo esta expresión por $f(x)$ se cancelan todos los términos para cada k fijo menos los correspondientes al propio $x-a_k$ en el que queda $b_k/(x-a_k)$ probando así el resultado.

Proposición 1.10. Sea $\mathcal{C} = \Gamma(L,g)$ un código de Goppa clásico definido sobre $\mathbb{F}_2$. Entonces $d(\mathcal{C}) \geq 2t+1$ (luego su capacidad de corrección es, al menos, el grado de g).

Demostración. Sea $\mathbf{c} = (c_0, \ldots, c_{n-1})$ una palabra de $\mathcal{C}$ no nula. Sea así mismo $f(x) = \prod_{i=0}^{n-1}(x-\gamma_i)^{c_i}$. Por el lema anterior,

$$\sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} = \frac{f'(x)}{f(x)}$$

ahora bien, el polinomio $f'(x)$ solo posee monomios de potencias pares ya que el cuerpo base es de característica 2 (y por tanto la derivada de los monomios de exponente par se anula). Teniendo en cuenta que además en característica 2 se tiene que $(a+b)^2 = a^2+b^2$, podemos expresar $f'(x) = p^2(x)$ para algún polinomio p. Ahora bien, f es invertible módulo $g(x)$ y por tanto para que esta palabra esté en el código (y dado que no es nula) debe tenerse que $g(x)$ divide a $f'(x) = p^2(x)$. Ahora bien, g no tiene raíces múltiples y por tanto $g^2(x)$ divide a $f'(x)$, por lo que, por el mismo

razonamiento que hemos hecho en la prueba anterior para la distancia, $w(\mathbf{c}) - 1 \geq 2t$ lo que prueba el enunciado.

Terminemos la sección con un ejemplo de código de Goppa clásico. Será un ejemplo simple extraído de [5].

Ejemplo 1.7. Sea $\mathbb{F}_{2^4}$ el cuerpo representado por el cociente $\mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$. Denotemos por α el generador de $\mathbb{F}_{2^4}^*$. Queremos tener la máxima dimensión posible del código por tanto, en virtud de la proposición 1.9 escogemos tantas raíces como podamos. Por ejemplo sea $L = \{\alpha^i \mid 2 \leq i \leq 13\}$ y tomemos $g(x) = (x + \alpha)(x + \alpha^{14})$. En tal caso, como g no se anula en L, podemos considerar $C = \Gamma(L, g)$. Estimando sus parámetros con 1.9, tenemos que $k \geq 13 - 8 = 5$ y $d \geq 3$.

Si queremos obtener una matriz de control para C, tenemos que evaluar g en cada una de los elementos de L e ir calculando sus inversos. Por ejemplo, $g(\alpha^2)^{-1} = (\alpha^4 + \alpha^9 + 1)^{-1}$. Reduciendo módulo $\alpha^4 + \alpha + 1$ tenemos que

$$\alpha^4 + \alpha^9 + 1 = \alpha^9 + \alpha = \alpha(\alpha^4)^2 + \alpha = \alpha(\alpha + 1)^2 + \alpha = \alpha(\alpha^2 + 1) + \alpha = \alpha^3$$

por tanto obtenemos que $(\alpha^4 + \alpha^9 + 1)^{-1} = (\alpha^3)^{-1} = \alpha^{12}$.

Haciendo esto para todos los elementos de L obtenemos que una matriz de control sería

$$H = \begin{pmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha \end{pmatrix}$$

Por último, podemos hacer la identificación de estos elementos con la base $\{1, \alpha, \alpha^2, \alpha^3\}$ para obtener una matriz de control en el sentido clásico obteniendo:

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

2 | Preludio de curvas algebraicas

Para introducir los códigos de Goppa algebraico geométricos, es necesario utilizar resultados de geometría algebraica sobre cuerpos que no son algebraicamente cerrados. Introducir estos conceptos con generalidad ocuparía demasiada extensión y no es el onjetivo de este trabajo. Sin embargo, en el caso concreto del estudio de las curvas, es posible dar un enfoque particular mucho más sencillo que relaja los prerrequisitos para entender la materia. Nuestro objetivo será mostrar los conceptos con los que vamos a trabajar y tendremos que asumir, por desgracia, algunos resultados como ciertos para que la extensión del trabajo no sea excesiva.

En esta sección daremos por conocidos los resultados obtenidos sobre geometría algebraica en cuerpos algebraicamente cerrados de la asignatura *Álgebra Conmutativa y Geometría Algebraica* (ACGA en lo sucesivo) del grado en matemáticas.

2.1 Anillos de valoración

Veamos algunos resultados adicionales sobre variedades de dimensión uno que se obtienen directamente de los resultados ya conocidos de geometría algebraica, para el caso de cuerpos algebraicamente cerrados (por ahora, al menos). Comencemos caracterizando la singularidad para el caso particular de las curvas en función de su anillo local. Como ser regular es una propiedad local, podemos asumir en principio que nuestra curva es afín.

Proposición 2.1. Sea X una curva sobre un cuerpo algebraicamente cerrado k. Entonces un punto $P \in X$ es no singular si y solo si el único ideal maximal $\mathfrak{m}_P$ del anillo local de las funciones racionales definidas en P, $\mathcal{O}_P$, es principal.

Demostración. Basta recordar que el que P sea no singular es equivalente a que $\mathcal{O}_P$

sea un anillo regular, es decir, su ideal maximal puede ser generado con tantos elementos como su dimensión de Krull. Como X es de dimensión 1, significa que $\mathfrak{m}_P = t_p\mathcal{O}_P$ para algún $t_p \in \mathcal{O}_P$.

Definición 2.1. *En las condiciones anteriores, a un generador del ideal maximal t_p lo llamaremos un parámetro local (o parámetro de uniformización) de la curva en P.*

Ejemplo 2.1. Sea $X = \mathcal{V}(f)$, con $f \in k[x, y]$, una curva y, sin pérdida de generalidad, supongamos que $P = (0, 0) \in X$ es un punto no singular, sabemos entonces que

$$\mathcal{O}_P = \Big(k[x, y]/\langle f \rangle\Big)_{\langle x,y \rangle}$$

es el localizado del anillo de funciones regulares en el ideal maximal del punto P.

Ahora bien, decir que $P = (0, 0) \in X$ es equivalente a que f no tenga término constante. Como además es no singular, alguna de las derivadas parciales no se anula. Supongamos, de nuevo sin pérdida de generalidad, que $\partial f/\partial x \neq 0$, esto es, f tiene término lineal en x no nulo.

En tal caso, como $f = 0 \in k[x, y]/\langle f \rangle$, y por ser su término lineal no nulo, podemos expresar, a partir de $f = 0$ y, extrayendo factor común x si es necesario

$$x = u(x, y) \cdot g(x, y) \cdot y, \quad \text{para algunos } g(x, y) \in k[x, y] \text{ y } u(x, y) \in \mathcal{O}_P^*$$

y por tanto, en $\mathcal{O}_P$, $x \in \langle y \rangle$, lo que prueba que $\langle x, y \rangle = \langle y \rangle$ por lo que y es un parámetro local.

A partir de ahora supondremos que tratamos con un punto $P \in X$ no singular para hacer un estudio local.

Nuestro siguiente objetivo es ver que podemos expresar cualquier función regular en P en función de nuestro parámetro local t_p. Este resultado no es difícil de probar pero daremos antes una definición previa para mostrar que la razón de que esto sea así es debido a que $\mathcal{O}_P$ es un anillo de valoración (discreta, para ser precisos).

Definición 2.2. *Sea B un dominio de integridad y sea K su cuerpo de fracciones. B es un anillo de valoración de K si para cada $x \in K$ no nulo, se tiene que $x \in B$ o que $x^{-1} \in B$.*

Ejemplo 2.2. El anillo $\mathbb{Z}$ no es un anillo de valoración de $\mathbb{Q}$.

Observación 2.1. No es difícil ver entonces que $\mathcal{O}_P$ es un anillo de valoración ya que su cuerpo de fracciones es el cuerpo de funciones racionales $\mathcal{K}(X)$. Esto se debe a

que $\mathcal{O}_P$ contiene al anillo de funciones regulares $\mathcal{A}(X)$ y el cuerpo de fracciones de este es $\mathcal{K}(X)$, que contiene a $\mathcal{O}_P$. Además sabemos que $\mathcal{O}_P$ es el localizado de $\mathcal{A}(X)$ en el ideal maximal asociado a P, $\mathfrak{m}_p$, luego una función racional de $\mathcal{K}(X)$ o está bien definida en P o su inversa se anula en P (y por tanto está bien definida) por la definición de localizado.

Además, como se vio en ACGA (ejercicio 9.7), todo anillo de valoración es un anillo local lo cual ya sabíamos en el caso particular de $\mathcal{O}_P$.

Podemos ahora probar con mayor fluidez el siguiente resultado:

Proposición 2.2. Sea $f \in \mathcal{K}(X)$. Entonces f tiene una única representación de la forma $f = t^r u$ para $r \in \mathbb{Z}$ y $u \in \mathcal{O}_P^*$.

Demostración. Para la existencia, como $\mathcal{O}_P$ contiene a f o a f^{-1} y $r \in \mathbb{Z}$, asumamos, sin pérdida de generalidad que $f \in \mathcal{O}_P$.

Si $f \in \mathcal{O}_P^*$, $f = t^0 f$. En caso contrario, existe un máximo $m \geq 1$ tal que $f \in t^m \mathcal{O}_P$ ya que f puede representarse localmente como un cociente de polinomios. Escribiendo $f = t^m u$ con $u \in \mathcal{O}_P$, u debe ser una unidad ya que en caso de no serlo estaría en $\mathfrak{m}_p = t\mathcal{O}_P$ contradiciendo a que m sea máximo.

La unicidad está clara, usando que u es una unidad. ∎

En esta prueba hemos visto que a cualquier función racional en la curva, le podemos asociar un único número entero directamente asociado con un parámetro local de la curva en P. Es decir, que tenemos una aplicación que identifica a nuestras funciones definidas en P salvo unidad asociándoles un número entero. Esto motiva la siguiente definición [1].

Definición 2.3. *Sea R una k-álgebra. Una valoración discreta (o valuación discreta) sobre R es una aplicación $v : R \to \mathbb{Z} \cup \{\infty\}$ que verifica:*

- $v(x) = \infty \iff x = 0$.
- $v(xy) = v(x) + v(y) \quad \forall x, y \in R$.
- $v(x + y) \geq \min\{v(x), v(y)\} \quad \forall x, y \in R$ *(Desigualdad triangular).*
- *Existe un elemento $z \in R$ con $v(z) = 1$.*
- $v(a) = 0, \quad \forall a \in k$.

[1] Pueden encontrarse otras definiciones similares pero no exactamente iguales de valoración discreta; esta será la que usemos en esta memoria

En este contexto, ∞ es un elemento que verifica que $\infty+\infty = \infty+n = n+\infty = \infty$ y $\infty > m$ para todos $m, n \in \mathbb{Z}$. De la segunda y la cuarta propiedad se sigue que $v : F \to \mathbb{Z} \cup \{\infty\}$ es sobreyectiva.

Con esta terminología, si a cada función racional en nuestra curva le asociamos el entero correspondiente a su representación en función de un parámetro local, tenemos una valoración discreta en $\mathcal{K}(X)$. Al número entero m que le asociamos le llamamos orden de la función en P. Si $m > 0$ diremos que P es un cero de f, y si $m < 0$ diremos que es un polo. Los nombres están justificados ya que si $f = t^m u$ con $t \in m_p$ y $u \in \mathcal{O}_P$, como u es invertible localmente en P, es el parámetro local t lo que marca si f es un cero o un polo dependiendo del signo de m.

Además notemos que este número m no depende del parámetro local escogido ya que si t' es otro parámetro local con $t\mathcal{O} = t'\mathcal{O}$, entonces deben diferenciarse en una unidad y por tanto la valoración de una función arbitraria f no cambia.

Para hablar de la valoración de una función racional f en un punto $P \in X$, se usarán indistintamente las notaciones $v_P(f)$ u $\mathrm{ord}_P(f)$.

Ejemplo 2.3. Consideremos la curva dada por $X = \mathcal{V}(h)$ con $h = x^3y + y^3 + x$ conocida como cuártica de Klein afín. Como la parcial con respecto a x es no nula, y es un parámetro local de la curva en $P = (0,0)$. Calculemos la valoración de la función $f = x^3 + y^3$ en P.

Procediendo como en el ejemplo anterior, $x = y(-x^3-y^2)$ y por tanto sustituyendo en nuestra función regular:

$$f = x^3 + y^3 = y^3\big(-x^3 - y^2\big)^3 + y^3 = y^3\Big(\big(-x^3 - y^2\big)^3 + 1\Big)$$

Como $(-x^3 - y^2)^3 + 1$ no se anula en P, es una unidad en nuestro anillo local y por tanto la valoración de f en P, es $v_P(f) = 3$.

Las valoraciones discretas nos ayudan a describir una biyección que será en la que nos basaremos para extender nuestro entendimiento de curvas sobre cuerpos algebraicamente cerrados a cuerpos arbitrarios. En concreto, notemos que que podemos describir el anillo local $\mathcal{O}_P$ en función de la valoración como:

$$\mathcal{O}_P = \Big\{ f \in \mathcal{K}(X) \mid v(f) \in \mathbb{Z}_{\geq 0} \cup \{\infty\} \Big\}.$$

Observación 2.2. Es fácil comprobar que de hecho los elementos de valoración mayor o igual a cero forman un anillo de valoración dando sentido a la terminología del anillo. A este anillo lo llamaremos anillo de valoración asociado a v.

Finalmente, damos el teorema que nos permitirá trabajar con curvas en cuerpos arbitrarios:

Teorema 2.1. *Sea X una curva proyectiva sin puntos singulares. Entonces existe una correspondencia biunívoca entre los puntos $P \in X$ y el conjunto de anillos de valoración en $\mathcal{K}(X)$. En concreto, a cada punto $P \in X$ se le asocia el anillo de valoración asociada a su valoración discreta v.*

Demostración. Una prueba elemental puede encontrarse en [1]. ∎

Volveremos sobre este resultado en una sección posterior.

2.2 Divisores

Sea X una curva proyectiva completa sin puntos singulares sobre un cuerpo algebraicamente cerrado k.

Definición 2.4. *Un divisor D en X es una suma formal finita de la forma $D = \sum_{P \in X} a_p P$ donde P son puntos de la curva y los a_p son enteros. En tal caso, el soporte de D es el conjunto de puntos de la curva cuyo coeficiente a_p es no nulo.*

El conjunto de los divisores de una curva X se denota como $Div(X)$ y es un grupo abeliano para la suma definida para $D = \sum_{P \in X} a_p P$ y $E = \sum_{P \in X} b_p P$ como $D + E = \sum_{P \in X} (a_p + b_p) P$.

Definición 2.5. *El grado de un divisor $D = \sum_{P \in X} a_p P$ se define como $\sum_{P \in X} a_p$.*

Con esta definición, es inmediato comprobar que la aplicación que a cada elemento de $Div(X)$ le asocia su grado en $\mathbb{Z}$ es un homomorfismo de grupos sobreyectivo. A su núcleo se le denotará por $Div^0(X)$ y es el conjunto de divisores de grado 0.

Si para un divisor $D = \sum_{P \in X} a_p P$ todos los a_p son no negativos, diremos que D es un divisor efectivo. Si además D es no nulo diremos que es positivo. Al conjunto de los divisores efectivos lo denotaremos por $Div^+(X)$ y podemos inducir en $Div(X)$ un orden parcial basado en él:

$$D \geq E \iff D - E \in Div^+(X).$$

Definición 2.6. *Sea $f \in \mathcal{K}(X)^*$ una función racional. Definimos el divisor de la función f como*

$$(f) = \sum_{P \in X} \mathrm{ord}_P(f) P$$

donde $\mathrm{ord}_P(f)$ *denota el orden de* f *por la valoración discreta en* P *esto es, esencialmente, el orden del cero o el polo de la función en el punto* P.

Observación 2.3. Nótese que con esta definición, (f) es un divisor ya que f tiene un número finito de polos y ceros en X. Además, tenemos la descomposición

$$(f) = (f)_0 - (f)_\infty$$

donde

$$(f)_0 = \sum_{\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f)P \qquad y \qquad (f)_\infty = \sum_{\mathrm{ord}_P(f)<0} -\mathrm{ord}_P(f)P$$

A $(f)_0$ se le llama el divisor de ceros de f y a $(f)_\infty$ el divisor de polos. Notemos que ambos divisores son, de hecho, efectivos.

Ejemplo 2.4. Sea $F = x^3y + y^3z + xz^3$ y consideremos $X = \mathcal{V}(F) \subseteq \mathbb{P}^2(k)$ la cuártica de Klein. Se puede comprobar, por el criterio usual, que esta curva no tiene puntos singulares independientemente de la característica del cuerpo. Sea $f = (y^3 + xz^2)/z^3$ la función racional representada por este cociente. Entonces mirando por cartas:

- Si $z = 1$, estamos en el caso afín. Para ver los ceros de f, usamos que $f = 0$ sustituido en la ecuación de p nos da que $x^3y = 0$. Tanto como si x o y son cero, sustituyendo de nuevo en p vemos que la otra variable también tiene que ser 0. Por tanto, el único punto que es un cero es el $P = (0, 0)$. Para calcular la valoración de f en el punto, recordemos que en el ejemplo 2.3 vimos que un parámetro local en $P = (0, 0)$ es y así que debemos expresar f como $y^n u$ con u una unidad. Para ello, de la expresión de f multiplicando por z en numerador y denominador
$$f = \frac{zy^3 + xz^3}{z^4},$$
luego despejando de F se tiene que
$$f = \frac{-(x^3y)}{z^4} = -y\left(\frac{x}{z}\right)^3\left(\frac{1}{z}\right).$$
La función $(1/z)$ es una unidad localmente en P luego podemos olvidarnos de ella. Ahora bien, de la ecuación de X podemos expresar x/z como
$$\frac{x}{z} = -\left(\frac{y}{z}\right)^3 \cdot \frac{z^3}{x^2y + z^3}.$$
Esto se puede comprobar escribiendo la ecuación de X como $y^3z = -x(x^2y + xz^2)$ y simplificando. Por tanto, deducimos que x/z tiene valoración en P de 3 y por tanto $v_P(f) = v_P(y) + 3v_P(x/z) = 1 + 9 = 10$.

- Veamos cómo se comporta la función en sus punto del infinito para $z = 0$. Si tomamos $z = 0$ comprobamos que los puntos del infinito para la carta dada por la variable z de la cuártica son el $Q = (1 : 0 : 0)$ y el $R = (0 : 1 : 0)$. En ambos casos la función g tiene un polo.
  Calculemos exactamente el orden de g en R. Para ello, lo más sencillo tomar la carta $y = 1$ y trabajar afínmente en $(0,0)$ para la curva $\mathcal{V}(\tilde{F})$, con $\tilde{F} = x^3 + z + xz^3$. Como tenemos término lineal en z en la curva, un parámetro local para el $(0,0)$ es x. Podemos expresar ahora f como $f = (y/z)^3 + x/z$ por lo que basta calcular la valoración de la función (y/z) en este punto. En este caso podemos expresar esta función como $y/z = -(y/x)^3((y^3+xz^2)/y^3)$ en virtud de nuevo de la ecuación de X. Entonces y/z tiene valoración -3 luego deducimos que $v_R(f) = -9$ que es el polo de orden 9 que aporta $(y/z)^3$.
  Por último, en Q tomamos la carta $x = 1$ y un parámetro local sería z teniéndose que $y = -z(y^3 + z^2)$. Sustituyendo esta expresión en f obtenemos que $f = -(y^3 + z^2)^3 + (x/z)$ luego f solo tiene un polo de orden 1 que es el que aporta x/z.

Por tanto, podemos escribir el divisor de g como

$$(f) = 10\,(0 : 0 : 1) - 9\,(0 : 1 : 0) - 1\,(1 : 0 : 0)$$

Su grado es $\deg(f) = 10 - 9 - 1 = 0$. Es decir, los ceros de f compensan, contando multiplicidades, a sus polos. Esto, como veremos en breves instantes, no es casualidad.

Los divisores de las funciones racionales serán esenciales para construir los códigos algebraico geométricos. Les damos un nombre especial.

Definición 2.7. *Sea $D \in Div(X)$. Si $D = (f)$ para algún $f \in \mathcal{K}(X)^*$, diremos que D es un divisor principal de la curva. Al conjunto de divisores principales lo denotaremos por $P(X)$.*

Observación 2.4. Si $f, g \in \mathcal{K}(X)^*$, entonces

$$(f \cdot g) = (f) + (g), \quad \left(\frac{f}{g}\right) = (f) - (g),$$

lo cual se puede ver trivialmente expresando cada función en su forma dependiente del parámetro local en cada punto. Esto prueba entonces que $P(X)$ es un subgrupo de $Div(X)$. Diremos que D y E son divisores equivalentes si están en la misma clase de equivalencia en el cociente $Cl(X) = Div(X)/P(X)$.

No podremos probar el teorema que viene a continuación puesto que alargaría demasiado la exposición de los contenidos, a pesar de ello, no debe subestimarse la importancia de este resultado pues es sobre el que se cimenta toda la teoría de divisores de curvas que nos proporcionarán herramientas muy potentes para estudiar las curvas.

Teorema 2.2. *Con las notaciones anteriores, $P(X) \subseteq Div^0(X)$. Esto es, el grado de un divisor principal es cero.*

Observación 2.5. En el caso de que estemos tratando con curvas planas, esto es, en $\mathbb{P}^2(k)$, el teorema no es más que un corolario del teorema de Bézout visto en ACGA ya que entonces si $X = \mathcal{V}(F)$ y $f \in \mathcal{K}(X)$ se puede representar localmente como $f = g/h$ con $g, h \in k[x_0, x_1, x_2]$ del mismo grado. Bézout nos dice que, contando multiplicidades, el número de ceros de h y de g en X son los mismos. En general, el teorema de Bézout que se vio solo para curvas planas vale para cualquier par de curvas en posición general. Un poco de trabajo para extender el teorema valdría para probar el caso general que da el teorema.

Estamos ahora en condiciones de introducir el espacio vectorial sobre el que construiremos los códigos algebraico-geométricos.

Definición 2.8. *Sea $D \in Div(X)$. Se llama el espacio asociado a D al conjunto*

$$L(D) = \left\{ f \in \mathcal{K}(X) \mid (f) + D \geq 0 \right\} \cup \{0\}.$$

Podemos entender con esta definición que $L(D)$ son las funciones racionales cuyos ceros *compensan* los puntos de D con coeficiente negativo, y cuyos polos se ven compensados por la parte efectiva de D.

Observación 2.6. Así definido, $L(D)$ tiene estructura de k-espacio vectorial. A su dimensión la denotaremos por $l(D)$.

Ejemplo 2.5. Si $X = \mathbb{P}^1(k)$, $P = (0 : 1)$ es su punto del infinito y $D = n\,(0 : 1)$ para $n \in \mathbb{Z}_{\geq 0}$, $L(D)$ son funciones racionales a las que les permitimos tener un polo de hasta orden n en el infinito pero que no pueden tener un polo en ningún otro punto. Como la recta proyectiva es bien conocida, no es difícil comprobar que entonces $L(D)$ consta de funciones de la forma $p(x_0, x_1)/x_0^q$ de manera que $q \leq n$ y x_0 no divide al polinomio homogéneo $p(x_0, x_1)$.

Entonces podemos identificar los elementos de $L(D)$ con polinomios en x_1 de grado a lo más n puesto que su función racional que coincidirá con esta función regular sería precisamente el cociente que acabamos de describir. Por tanto, en este caso, $L(D) = \langle 1, x_1, \ldots, x_1^n \rangle$ como $k-$espacio vectorial por lo que $l(D) = n + 1$.

Este resultado es más general. Veamos que de hecho $l(D)$ es siempre finito y está acotado.

Lema 2.1. Si $\deg(D) < 0$, entonces $l(D) = 0$.

Demostración. Si $\deg(D) < 0$, entonces para cualquier $f \in \mathcal{K}(X)^*$,

$$\deg((f) + D) = \deg((f)) + \deg(D) = 0 + \deg(D) < 0$$

por el teorema 2.2. Luego $L(D) = \{0\}$.

Lema 2.2. $l(D)$ solo depende de la clase de equivalencia de D.

Demostración. Si $D - E = (f)$ para algún $f \in \mathcal{K}(X)^*$ con $D = \sum_{P \in X} a_p P$ y $E = \sum_{P \in X} b_p P$. Definamos la aplicación

$$\begin{aligned} \phi_f : L(D) &\longrightarrow L(E) \\ g &\mapsto \phi_f(g) = fg \end{aligned}$$

Debido a que $D - E = (f)$, se tiene que para todo $P \in X$,

$$\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g) \geq \operatorname{ord}_P(f) - a_p = -b_p.$$

Por tanto la aplicación está bien definida y es de hecho homomorfismo de $k-$espacios vectoriales cuya inversa es el producto por f^{-1}, luego $L(D)$ y $L(E)$ son isomorfos.

Teorema 2.3. *La dimensión de $L(D)$, $l(D)$, es finita para todo $D \in Div(X)$.*

Demostración. Si $f \neq 0 \in L(D)$ entonces $D' = (f) + D \geq 0$ es efectivo y $L(D')$ es isomorfo a $L(D)$ por el lema 2.2 luego basta probar que $L(D')$ es de dimensión finita. Digamos que $D' = \sum_{P \in X} a_P P$ con $a_P > 0$. Asumamos que $g \in L(D')$ y fijemos un punto $P \in X$. Consideremos entonces la aplicación lineal $\phi_P : L(D') \to k$ de manera que:

$$\phi_P(f) = t_P^{a_P} f(P)$$

con t_P un parámetro local en el punto P. Para que una función esté en $\ker \phi_P$, debe tener un polo de orden hasta $a_P - 1$, esto es, el núcleo está contenido en $L(D' - P)$. Por tanto, $l(D') \leq 1 + l(D' - P)$. Como $a_P > 0$, $D_1 = D - P$ vuelve a ser efectivo por lo que podemos proceder inductivamente hasta que $D_{\deg(D)} = 0$ y utilizando el lema 2.1, llegamos a que $l(D)$ es de dimensión finita.

Corolario 2.1. De la construcción por inducción anterior se deduce que, si $D \geq 0$:

$$l(D) \leq \deg(D) + 1,$$

donde $\deg(D)$ es el grado del divisor D.

2.3 Lugares

Hasta ahora hemos supuesto que k es algebraicamente cerrado. Como sabemos, esto no será suficiente para desarrollar teoría de códigos puesto que esta se hace sobre cuerpos finitos. Por ello, en esta sección extenderemos el concepto de curva algebraica a un cuerpo k que no sea necesariamente algebraicamente cerrado. Veremos que podremos hacer esto trabajando con cuerpos K de grado de trascendencia 1 sobre k de manera completamente algebraica. Durante toda la subsección, es importante tener en mente que este cuerpo K representaría, en el caso en el que k fuese algebraicamente cerrado, el cuerpo de las funciones racionales sobre una curva proyectiva. De esta forma, los resultados serán mucho más naturales de asimilar que si se entienden como resultados de álgebra conmutativa pura.

La única restricción que le impondremos a nuestro cuerpo base k es que sea un cuerpo perfecto, esto es, que sea de característica cero o que sea de característica $p > 0$ debiéndose cumplir adicionalmente en este caso que el endomorfismo de Frobenius ϕ (dado por $\phi(x) = x^p$), sea un automorfismo. Con esta definición, los cuerpos finitos son perfectos.

Definición 2.9. *Un cuerpo de funciones algebraicas K de una variable sobre k es cualquier cuerpo K que contenga a k que tenga grado de trascendencia 1 sobre k o, equivalentemente, una extensión finita de $k(x)$.*

Ejemplo 2.6. Si X es una curva proyectiva sobre un cuerpo algebraicamente cerrado k, $\mathcal{K}(X)$ es un cuerpo de funciones algebraicas sobre k.

Como sabemos, el conjunto de los elementos de K algebraicos sobre k forman un cuerpo al que llamaremos el cuerpo de las constantes K y al que denotaremos por $\tilde{k}$. En general a los elementos de K los llamaremos funciones, nombre que se justificará en breves instantes.

Ejemplo 2.7. Si $K = k(x)$, el cuerpo de las constantes de K es el propio k ya que ningún polinomio con coeficientes en k puede ser algebraico sobre k.

La idea de cómo vamos a extender la construcción de las curvas está basada en extender la biyección entre los puntos de una curva y los anillos de valoración de su cuerpo de funciones dada por el teorema 2.1. Para ello, veamos que muchas de las propiedades que tenían los anillos de valoración de $\mathcal{K}(X)$ son las mismas que para K.

Proposición 2.3. Sea $\mathcal{O}$ un anillo de valoración de un cuerpo de funciones K sobre k y sea $P \subseteq \mathcal{O}$ su único ideal maximal (recordemos que $\mathcal{O}$ siempre es local). Entonces:

(a) $\tilde{k} \subseteq \mathcal{O}$ y $\tilde{k} \cap P = \{0\}$.
(b) P es un ideal principal.
(c) Si $P = t\mathcal{O}$, entonces cualquier elemento $f \in K$ tiene una única representación de la forma $f = t^n u$ con $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$. En particular, el entero n no depende de la elección de t.

Demostración. (a) Si $x \in \tilde{k}$ pero $x \notin \mathcal{O}$, entonces $x^{-1} \in \mathcal{O}$ por ser $\mathcal{O}$ local. Como x^{-1} es algebraico sobre k, existen $a_0, a_1, \dots, a_n \in k$ tales que $a_0 + a_1 x^{-1} + \dots a_n x^{-n} = 0$ por lo que

$$z = \frac{-a_n (x^{-1})^{n-1} - \dots - a_1}{a_0} \in \mathcal{O},$$

donde hemos usado que $a_0 \neq 0$ puesto que el polinomio lo podemos tomar irreducible. Como P no puede contener unidades se tiene que $\tilde{k} \cup P = \{0\}$.

(b) Si P no es principal, existen elementos no nulos $x_1, x_2 \in P$ con $P \neq x_1\mathcal{O}$ y $x_2 \in P \setminus x_1\mathcal{O}$. En tal caso, $x_2 x_1^{-1} \notin \mathcal{O}$ y por tanto $x_2^{-1} x_1 \in P$ por ser un elemento no invertible en $\mathcal{O}$. Obtendríamos por tanto que $x_1 \in x_2 P$. Podemos por tanto hacer un proceso inductivo en el que encontraríamos una sucesión infinita $\{x_i \mid i \in \mathbb{N}\}$ tales que $x_i \in x_{i+1} P$ para todo i. La demostración de que esto no puede ocurrir se da a través de un lema técnico que vendrá a continuación que nos limitamos a citar ya que no es de mayor interés salvo para esta prueba.

(c) La prueba de este punto es parecida a la del caso en el que el cuerpo k es algebraicamente cerrado (ver proposición 2.2) pero hay que justificar que existe un máximo $m \geq 1$ tal que cualquier $f \in K$ verifica que $f \in t^m \mathcal{O}$ en el caso que nos ocupa. Esto se hace a través del lema técnico siguiente que cierra la prueba.

Lema 2.3. Sea $\mathcal{O}$ un anillo de valoración de un cuerpo de funciones algebraicas K. Sea P su ideal maximal y sea $x \neq 0 \in P$. Sean $x_1, \dots, x_n \in P$ que verifiquen que $x_1 = x$ y $x_i \in x_{i+1} P$, entonces $n \leq [K : k(x)] < \infty$.

Demostración. La prueba puede encontrarse en [6] o en [7].

Introducimos ahora el concepto de lugar, el cual hará el papel de los puntos en el caso en el que k no sea algebraicamente cerrado.

Definición 2.10. *Un lugar P de un cuerpo de funciones K sobre k es el ideal maximal de cualquier anillo de valoración de K. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ se dice que es un parámetro local (o parámetro de uniformización) en P. El conjunto de todos los lugares de K se denotará[2] por $\mathbb{P}^n(K)$.*

[2] No confundir con la notación de espacio proyectivo, $\mathbb{P}_K$.

Observación 2.7. El punto (c) del teorema 3.8 prueba que todo anillo de valoración $\mathcal{O} \subseteq K$ es de hecho un anillo de valoración discreta. A la valoración discreta que arroja (c) en el punto P la denotaremos por v_P igual que en la sección anterior.

Observación 2.8. Un anillo de valoración queda unívocamente determinado por su ideal maximal P, en concreto, $\mathcal{O} = \{f \in K \mid f^{-1} \notin P\}$. A este anillo se le denotará por $\mathcal{O}_P$ y le llamaremos el anillo de valoración en el lugar P.

Ejemplo 2.8. Si $p(x) \in k[x]$ es un polinomio irreducible y consideramos la aplicación $v_{p(x)} : k(x) \to \mathbb{Z} \cup \{\infty\}$ definida como:

- Si $f(x) \in k[x]$ es no nulo, $v_{p(x)}(f) = m$, donde m es la mayor potencia de $p(x)$ que divide a $f(x)$.
- Si $f(x)/g(x) \in k(x)$, $v_{p(x)}(f/g) = v_{p(x)}(f) - v_{p(x)}(g)$.
- $v_{p(x)}(0) = \infty$.

Entonces $v_{p(x)}$ es una valoración discreta que define un lugar P que es el conjunto de todas las funciones racionales $f(x)/g(x) \in k(x)$ tales que $p(x)$ divide a $f(x)$ pero $p(x)$ no divide a $g(x)$.

Observación 2.9. Si k es algebraicamente cerrado y X es una curva proyectiva sin puntos singulares, el teorema 2.1 dice que existe una correspondencia biyectiva entre los puntos $P \in X$ y los lugares de $K = \mathcal{K}(X)$.

Al igual que en el caso de tratar con curvas proyectivas, diremos que una función $f \in K$ tiene un cero en P si la valoración en P es positiva y diremos que tiene un polo en P si la valoración en P es negativa. Por último, diremos que f está definida en P si su valoración es no negativa. En términos de la valoración podemos describir los conjuntos:

$$P = \{f \in K \mid v_P(f) > 0\}, \quad \mathcal{O}_P = \{f \in K \mid v_P(f) \geq 0\}.$$

Como veremos en la siguiente sección, a la hora de tratar con una curva no singular sobre un cuerpo cualquiera, es conveniente pensar en sus puntos como los anillos de valoración de su cuerpo de funciones. En virtud de la observación 2.9, esta definición es equivalente a la que se da en geometría algebraica clásica.

Definición 2.11 (Curva proyectiva no singular). *Sea k un cuerpo y sea K un cuerpo de funciones sobre k. Una curva proyectiva no singular es un conjunto X que está en biyección con el conjunto de los anillos de valoración de K, $\mathrm{Val}(K/k)$, tal que la intersección $\cap_{\mathcal{O}_P \in \mathrm{Val}(K/k)} \mathcal{O}_P = k$.*

La condición de que la intersección de los anillos de valoración del cuerpo de funciones sea el cuerpo base refleja la idea de que cualquier función racional definida en cualquier punto de una curva proyectiva debe ser constante. Esta definición da además sentido a la notación de los lugares por P puesto que estos están en correspondencia con los puntos de la curva que representa el cuerpo de funciones K.

Hablemos por último de los cuerpos residuales de los anillos de valoración de K. Como sabemos, en el caso de que $K = \mathcal{K}(X)$ sea el cuerpo de funciones racionales de una curva proyectiva no singular sobre un cuerpo algebraicamente cerrado se estudió en ACGA que el cuerpo residual de cada uno de los anillos de valoración de K son isomorfos al cuerpo base k. En general, sin embargo, este cuerpo residual no tiene por qué coincidir con el cuerpo base sino que puede ser una extensión finita de este. Un ejemplo claro puede encontrarse fácilmente tomando $k = \mathbb{R}$, $K = k(x)$ y considerando la valoración del ejemplo 2.8 con $p(x) = x^2 + 1$. En tal caso, el cuerpo residual del anillo de valoración asociado a $v_{p(x)}$ es isomorfo a

$$\frac{\mathbb{R}[x]_{x^2+1}}{\langle x^2+1\rangle \mathbb{R}[x]_{x^2+1}} \cong \frac{\mathbb{R}[x]}{\langle x^2+1\rangle} \cong \mathbb{C}.$$

Al cuerpo residual del anillo de valoración $\mathcal{O}_P$ lo denotaremos por k_P.

Proposición 2.4. La extensión $k \subseteq k_P$ es finita y su grado está acotado por el grado de la extensión de K sobre $k(x)$.

Demostración. La prueba es una consecuencia del lema 2.3. Puede encontrarse en detalle en [7]. ∎

Definición 2.12. *Al grado de la extensión* $[k : k_P]$ *lo llamaremos el grado del lugar* P. *Lo denotaremos por* $\deg(P)$.

Por tanto, en el caso en el que k es algebraicamente cerrado, como $k \subseteq k_P$ es finita, $k_P = k$ para cualquier P, es decir el grado de cada lugar es 1.

2.4 Puntos racionales de una curva

Cabe ahora considerar una pregunta que es natural plantearse a la hora de estudiar curvas algebraicas sobre cuerpos que no son algebraicamente cerrados. Digamos que k es un cuerpo cualquiera. Entonces podríamos haber considerado las curvas

$$X = \mathcal{V}(h_1, \dots, h_r), \text{ con } h_1, \dots, h_r \in k[x_0, \dots, x_n]$$

de k como las curvas X definidas por las mismas ecuaciones que en su cierre algebraico $\overline{k}$, pero cuyos puntos tengan todas las coordenadas en k. A estos puntos se les suele llamar **puntos racionales** de la curva $X \subseteq \mathbb{P}^n(\overline{k})$ (sobrentendiendo quién es el cuerpo k, evidentemente). Teniendo en cuenta esta manera de extender los conceptos tan natural cabe preguntarse si existe alguna relación con la manera puramente algebraica de tratar con curvas que hemos visto en esta sección.

La respuesta a esto es afirmativa. Recordemos que el teorema 2.1 nos decía que existía una correspondencia biyectiva entre los puntos de una curva y los lugares de su cuerpo de funciones cuando trabajamos sobre un cuerpo algebraicamente cerrado. En el caso en el que nuestro cuerpo k no sea algebraicamente cerrado tendremos que pedirle a k que sea un cuerpo perfecto, o equivalentemente, que toda extensión algebraica suya sea separable (cosa que sabemos que verifican los cuerpos finitos). En tal caso, los anillos de valoración de lo que definiremos como el cuerpo de funciones asociada a la curva, se corresponderán en este caso, no con un punto de la curva sino con un conjunto de puntos conjugados por la acción del grupo de Galois de la extensión $k \subseteq \overline{k}$ de la curva considerada sobre $\overline{k}$.

A partir de ahora supondremos que nuestras curvas son planas por simplicidad.

Definición 2.13. *Sea k un cuerpo. Una variedad proyectiva $\overline{X}$ sobre el cuerpo k o más brevemente, una $k-$variedad, $\overline{X} \subseteq \mathbb{P}^n(\overline{k})$ es el conjunto de ceros comunes de un conjunto de polinomios con coeficientes en k.*

En tal caso, dado un cuerpo k' tal que $k \subseteq k' \subseteq \overline{k}$, denotamos por $X(k')$ el conjunto de puntos racionales de la $k-$variedad $\overline{X}$ sobre el cuerpo k'. Esto es, el conjunto de puntos que admiten una representación[3] con todas las coordenadas en k' de la variedad $\overline{X} \subseteq \mathbb{P}^n(\overline{k})$. Dado un punto $P \in \overline{X}$, el cuerpo de definición de P sobre k es el menor cuerpo intermedio k' generado por unas coordenadas de P. En otras palabras, es el menor cuerpo k' en el que P es un punto racional.

Ejemplo 2.9. La cuártica de Klein dada por $\mathcal{V}(F) \subset \mathbb{P}^2$ con $F = x^3y + y^3z + z^3x$ es una $k-$variedad para cualquier cuerpo base k. Tomemos $k = k' = \mathbb{F}_2$, entonces $X(k')$ consta de solamente 3 puntos: $(0 : 0 : 1)$, $(0 : 1 : 0)$ y $(1 : 0 : 0)$.

Definición 2.14. *Sean $k \subseteq \overline{k}$ en las condiciones anteriores. Definimos el grupo de Galois,* $\mathrm{Gal}(\overline{k}/k)$ *(también conocido como el grupo absoluto de Galois) como el conjunto de los automorfismos de $\overline{k}$ que dejan invariante a k.*

[3] Dado que un punto proyectivo puede venir dado por varias $(n+1)$-uplas de coordenadas proyectivas.

En el caso de que $k = \mathbb{F}_q$ sea un cuerpo finito, el grupo absoluto de Galois se puede describir explícitamente, esto se hace con detalle en el material adicional (ver 4.4).

El grupo de Galois actúa de manera natural sobre el espacio $\mathbb{P}^2(\overline{k})$ de manera que

$$\sigma\big(p_0 : p_1 : p_2\big) = \big(\sigma(p_0) : \sigma(p_1) : \sigma(p_2)\big).$$

En tal caso, está claro que, por construcción,

$$X(k') = \left\{x \in \overline{X} \mid \sigma(x) = x, \ \ \forall \sigma \in \mathrm{Gal}(\overline{k}/k')\right\}$$

y que además, si $P \in \overline{X}$, el cuerpo de definición de P es precisamente $\overline{k}^{G_P}$ donde $G_P = \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid \sigma(P) = P\}$ es el subgrupo denominado *estabilizador de* P. Utilizando teoría de Galois se puede deducir entonces que si k es un cuerpo perfecto, entonces la órbita de cada punto $P \in \overline{X}$ tiene exactamente $\left[\overline{k}^{G_P} : k\right]$ puntos distintos.

Digamos ahora que tenemos una curva plana sobre un cuerpo arbitrario k descrita por $F \in k[x_0, x_1, x_2]$ homogéneo. Esto es, $\overline{X} = \mathcal{V}(F)$. A partir de ahora supondremos que F es **totalmente irreducible**, es decir, no solo F es irreducible en k sino también en $\overline{k}$ lo cual hará que podamos trabajar con su cuerpo de funciones sobre $\overline{k}$.

Así definida, la acción del grupo de Galois sobre $\mathbb{P}^2(\overline{k})$ se restringe a una acción sobre la curva $\overline{X}$ ya que F tiene coeficientes en k luego $F(\sigma(P)) = \sigma(F(P)) = \sigma(0) = 0$ para cualquier $P \in \overline{X}$. Como además F es totalmente irreducible, podemos considerar $\mathcal{K}(\overline{X})$ su cuerpo de funciones y denotaremos análogamente por $\mathcal{K}(X)$ al conjunto de cocientes de polinomios homogéneos del mismo grado con coeficientes en k. Exactamente igual que en el caso en el que k es algebraicamente cerrado, $\mathcal{K}(X)$ es un cuerpo de grado de trascendencia 1 sobre k y además $\mathcal{K}(X) \subseteq \mathcal{K}(\overline{X})$. Si denotamos por $\mathrm{Val}(\mathcal{K}/k)$ el conjunto de anillos de valoración de un cuerpo de funciones algebraicas $\mathcal{K}$ sobre k, entonces podemos obtener los anillos de valoración de $\mathcal{K}(X)$ a través de los anillos de valoración de $\mathcal{K}(\overline{X})$ como:

$$\begin{aligned} I_{val} : \mathrm{Val}\left(\mathcal{K}(\overline{X})/\overline{k}\right) &\longrightarrow \mathrm{Val}(\mathcal{K}(X)/k) \\ \overline{\mathcal{O}} &\mapsto \overline{\mathcal{O}} \cap k(X_F). \end{aligned}$$

Además, siguiendo la analogía que teníamos para un cuerpo algebraicamente cerrado, la aplicación $P \to \mathcal{O}_P$ de $\overline{X}$ en $\mathrm{Val}(\mathcal{K}(X)/\overline{k})$ es una biyección según el teorema 2.1. Es decir, teníamos una biyección entre los anillos de valoración del cuerpo de funciones de la curva y los puntos de la misma. Llamaremos a esta aplicación biyectiva

$I_{\overline{k}}$. En el caso en el que k no sea algebraicamente cerrado, tenemos que esta biyección es entre los anillos de valoración de su cuerpo de funciones y **las órbitas de cada punto** según $\mathrm{Gal}(\overline{k}/k)$. Es decir, hay una biyección:

$$\begin{array}{rccc} I_k : & \overline{X}/\mathrm{Gal}(\overline{k}/k) & \longrightarrow & \mathrm{Val}(\mathcal{K}(X)/k) \\ & \text{órbita de } P & \mapsto & \mathcal{O}_P \cap \mathcal{K}(X) \end{array}$$

Todo esto se resume en este teorema:

Teorema 2.4 (Correspondencia entre puntos conjugados y anillos de valoración). *Sea k un cuerpo y $F \in k[x_0, x_1, x_2]$ un polinomio homogéneo. Supongamos que $\overline{X} = \mathcal{V}(F) \subseteq \mathbb{P}^2(\overline{k})$ es una curva no singular. Entonces I_k está bien definido, es biyectivo y el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} \overline{X} & \xrightarrow{I_{\overline{k}}} & \mathrm{Val}(\mathcal{K}(\overline{X}/\overline{k})) \\ \downarrow & & \downarrow{\scriptstyle I_{val}} \\ \overline{X}/\mathrm{Gal}(\overline{k}/k) & \xrightarrow[I_k]{} & \mathrm{Val}(\mathcal{K}(X/k)) \end{array}$$

Además, el cuerpo de definición de $P \in \overline{X}$ es precisamente el dado por I_k, esto es $\mathcal{O}_P \cap \mathcal{K}(X)$.

Demostración. La prueba, aunque no es difícil y solo requiere algunas comprobaciones, no la daremos y nos limitaremos a citarla ya que no es el tema principal del trabajo. Aún así, una pequeña idea de cómo iría es que, dado que sabemos que $I_{\overline{k}}$ es isomorfismo e I_{val} es sobreyectivo, se sigue que I_k es sobreyectivo y por tanto solo habría que probar que es inyectivo. Esto requeriría de estudiar previamente los ideales maximales del anillos $k[x, y]$ y comprobar que puntos conjugados dan lugar al mismo anillo de valoración. Una demostración de este hecho con detalle puede encontrarse en [1].

Corolario 2.2. En virtud del teorema anterior, el conjunto de puntos conjugados de $\overline{X}$ por la acción de $\mathrm{Gal}(\overline{k}/k)$ es una curva proyectiva no singular sobre k en el sentido de la definición 2.11 siendo su cuerpo de funciones $K = \mathcal{K}(X)$.

Corolario 2.3. Si k es un cuerpo perfecto y dado $P \in \overline{X}$, el cuerpo de definición de P tiene grado sobre k exactamente $[k_P : k]$, a lo que llamamos $\deg(P)$ en la definición 2.12 que a su vez coincide con el número de elementos en la órbita de P.

Observación 2.10. Como para cada cuerpo finito $k = \mathbb{F}_q$ solo existe una única extensión de cada grado, el corolario anterior nos dice que si tengo $\deg(P)$ puntos conjugados a un punto P, todos estos puntos tienen como cuerpo de definición a $k' = \mathbb{F}_{q^{\deg(P)}}$.

Ejemplo 2.10 (La cuártica de Klein). Sea $k = \mathbb{F}_2$ y sea $F = x^3y+y^3z+z^3x \in \mathbb{F}_2[x, y, z]$. Entonces ya vimos que $X = \mathcal{V}(F)$ tiene 3 puntos en k. Esto es, 3 puntos de grado 1. Para *ver* sus puntos de grado 2 debemos tomar una extensión la extensión de grado 2 de k, por ejemplo $k' = \mathbb{F}_4 = \mathbb{F}_2[a]/\langle a^2 + a + 1\rangle$. En tal caso en $X(k')$ aparecen dos puntos de grado 1 conjugados: $(1 : a : 1 + a)$ y $(1 : 1 + a : a)$. Este par de puntos define un punto de grado 2 sobre k. En particular, esto nos dice que el cuerpo de funciones racionales de X sobre $\mathbb{F}_2$ solo tiene un lugar de grado 2.

Si quisiéramos ver los puntos de grado 3, tomaríamos $k' = \mathbb{F}_8$. Como sabemos, existe un generador de la extensión $\mathbb{F}_8 = \mathbb{F}_2(\xi)$. Resulta que una posible elección de generador es un elemento que cumpla $\xi^3 = \xi + 1$. Si alguna de las coordenadas del punto es cero, recuperamos los puntos de grado 1 de $\mathbb{F}_2$. En caso contrario tomamos sin pérdida de generalidad $z = 1$ y obtenemos que poniendo $y = \xi^m$ y $x = \xi^p$ y sustituyendo en la ecuación, obtenemos que los puntos de la forma $(\xi^{3m}\eta : \xi^m : 1)$ con $\eta = \xi, \xi^2, \xi^4$ son soluciones. Reordenando todos las posibles combinaciones obtenemos un total de 24 puntos de grado 1 sobre $\mathbb{F}_8$ lo cual nos dice que, quitando los 3 que había sobre $\mathbb{F}_2$ de grado 1, tenemos 7 puntos de grado 3 que deben ser conjugados sobre $\mathbb{F}_2$.

2.5 Divisores en cuerpos arbitrarios y la desigualdad de Riemann

Podemos ahora introducir el concepto de divisores que será con el que construiremos los espacios $L(D)$ sobre los cuales construiremos los códigos Goppa. Lo que veremos a continuación puede generalizarse para un cuerpo de funciones algebraicas cualquiera pero por simplicidad, supondremos que $K = \mathcal{K}(X)$ es el cuerpo de funciones de una curva plana, proyectiva sin puntos singulares sobre un cuerpo perfecto k.

Definición 2.15. *El grupo de los divisores de $\mathcal{K}(X)$, $Div(\mathcal{K}(X))$ es el grupo abeliano libre generado por sumas de la forma*

$$D = \sum_{P \in \mathbb{P}_{\mathcal{K}(X)}} a_P P$$

donde a_P son todos nulos salvo un número finito.

La suma se toma sobre todos los lugares de $\mathcal{K}(X)$ o, dicho de otro modo, en virtud

del teorema 2.4, la suma es sobre conjuntos de puntos conjugados por la acción del grupo de Galois.

Definición 2.16. *El grado del divisor* $D = \sum_{P \in \mathbb{P}_K} a_P P$ *es*

$$\deg(D) = \sum_{P \in \mathbb{P}_K} a_p \deg(P).$$

Observación 2.11. Esta definición del grado es compatible con la que se dio para cuando k es algebraicamente cerrado ya que en ese caso, el grado de cada punto es 1.

Esto refleja el hecho de que, según el teorema 2.4, si tomamos el lugar P con coeficiente a_P en nuestro divisor, como P puede entenderse como $\deg(P)$ puntos de $\overline{X}$ conjugados, tenemos que contar el lugar P tantas veces como indique el grado de su cuerpo residual.

Definición 2.17. *Si* $f \in K$ *se define el divisor de* f, (f) *como*

$$(f) = \sum_{P \in \mathbb{P}_K} v_P(f) P$$

A los divisores que son divisores de alguna función les llamaremos divisores principales.

Al igual que en el caso proyectivo habitual se tiene este importante resultado.

Teorema 2.5. *El grado de un divisor principal es cero.*

Demostración. Como $f \in \mathcal{K}(X)$, f es cociente de dos polinomios $f = g/h$ con $g, h \in k[x_0, x_1, x_2]$ homogéneos del mismo grado. Entonces por tener g y h coeficientes en k, g y h tienen, respectivamente, la misma valoración para puntos conjugados por la acción del grupo de Galois por estar estos puntos asociados al mismo lugar de $\mathcal{K}(X)$ en virtud del teorema 2.4.

Así podemos asociar, a cada divisor D de $Div(\mathcal{K}(X))$, un divisor en $Div(\mathcal{K}(\overline{X}))$, descomponiendo cada lugar P en la suma de los puntos que conforman su órbita. Dado que la valoración de f en cada punto conjugado es la misma, está claro que $\deg(D)$ visto en $Div(\mathcal{K}(X))$ coincide con $\deg(D)$ visto en $Div(\mathcal{K}(\overline{X}))$ luego por el teorema 2.2 se sigue el resultado. ∎

Por último, hemos de introducir la desigualdad de Riemann, la cual es un caso particular del teorema de Riemann-Roch original. Tratar con este teorema en su forma completa requeriría previamente introducir el concepto de formas diferenciales lo

cual va más allá del objetivo del capítulo. Por ello, hablaremos simplemente de la desigualdad de Riemann, utilizada por este mismo y más tarde completada con el teorema de Gustav Roch. Aún así, un tratamiento un poco más exhaustivo se puede encontrar en el apéndice del trabajo, en la sección 4.2.

Para introducir la desigualdad de Riemann es preciso dar la definición de **género de una curva**. Para no extender demasiado la exposición del trabajo, solamente diremos que el género de una curva es un invariante por morfismo birracionales que se le asocia a curvas proyectivas sobre un cuerpo k. Una definición precisa y puramente algebraica puede encontrarse en el apéndice del trabajo. En el caso de que estemos en $\mathbb{P}^2$ y la curva sea plana, no singular, dada por $F = 0$ con F de grado d, el género g puede ser calculado según la **fórmula de Plücker**[4]:

$$g = \frac{1}{2}(d-1)(d-2).$$

Teorema 2.6 (Desigualdad de Riemann). *Sea X una curva proyectiva de género g sobre un cuerpo k y sea $D \in Div(K(X))$. Entonces:*

$$l(D) \geq \deg(D) - g + 1.$$

Además, si $\deg(D) > 2g - 2$, *se tiene la igualdad.*

Demostración. No la damos aquí. Se puede encontrar en la sección 4.2 del apéndice del trabajo.

[4]Una indicación de en qué se basa la prueba de esta fórmula puede encontrarse en el apéndice del trabajo (ver sección 4.3)

3 | Códigos Algebraico-Geométricos

Volvamos al mundo de la teoría de códigos. A la hora de encontrar familias de códigos con buenos parámetros, una idea es encontrar una familia de espacios vectoriales de dimensión finita sobre $\mathbb{F}_q$ que tengan una estructura muy variada pero que a su vez seamos capaces de entender. Resulta que los espacios $L(D)$ de Riemann verifican estas dos condiciones. Goppa construyó los códigos algebraico-geométricos basándose en estos espacios vectoriales creando un puente entre la geometría algebraica y la teoría de códigos correctores de errores.

3.1 Definición

Sea X una curva no singular sobre un cuerpo finito $\mathbb{F}_q$ de manera que $X(\mathbb{F}_q) \neq \emptyset$ y sean $P_1, \dots, P_n \in X(\mathbb{F}_q)$, esto es, puntos racionales de X sobre $\mathbb{F}_q$. Sea $D = P_1 + \dots + P_n$ y sea $G = \sum_{P \in \mathbb{P}_{K(X)}} a_P P$ un divisor cualquiera disjunto con D, esto es, que $a_{P_i} = 0$ para todos los i.

En estas condiciones podemos evaluar cada función de $L(G)$ en los puntos P_i y crear la aplicación lineal $\alpha : L(G) \to \mathbb{F}_q^n$ definida por:

$$f \to \big(f(P_1), \dots, f(P_n)\big)$$

Definición 3.1 (Código Goppa). *La imagen de la aplicación α anterior se denomina código algebraico geométrico (o Código Goppa) y se denota por $C(D, G)$.*

Teorema 3.1 (Parámetros de los códigos Goppa). *Si $C(D, G)$ es un código Goppa, sus parámetros verifican:*

$$k = \dim C(D, G) = l(G) - l(G - D), \quad d \geq n - \deg(G).$$

Demostración. La dimensión del código viene dada, como sabemos por álgebra lineal básica, por $l(G) - \dim \ker(\alpha)$. Ahora bien, para que f se anule en todos los P_i, $a_{P_i} \geq 1$. Además como G y D son disjuntos y $f \in L(G)$, debe tenerse que $f \in L(G - D)$.

Vayamos con la distancia mínima. Digamos que $\alpha(f)$ tiene peso d. En tal caso, f se anula en $n - d$ puntos de los P_i, digamos, los $n - d$ primeros sin pérdida de generalidad. En tal caso, $(f) + G - P_1 - \ldots - P_{n-d} \geq 0$ por ser $f \in L(G)$. Tomando grados, se tiene que, como todo divisor principal es de grado 0, $\deg(G) - n + d \geq 0$ lo que finaliza la prueba. ∎

Ejemplo 3.1. Tomemos $X = \mathbb{P}^1$ sobre $\mathbb{F}_q$, sea $r < q - 1$ un natural y escojamos $P_1, \ldots, P_{q-1}$ los $\mathbb{F}_q$−puntos afines excepto el origen. Tomando entonces $G = r \cdot P_\infty$ el divisor que es el punto del infinito con multiplicidad r con $r < q - 1$. Obtenemos que, según el ejemplo 2.5, una base para $L(G)$ puede verse como las funciones afines $\{1, x, \ldots, x^r\}$.

Para estudiar la imagen de α, tomemos un generador del grupo multiplicativo $\mathbb{F}_q^* = \langle \beta \rangle$. En tal caso, podemos tomar, sin pérdida de generalidad los P_i tales que $P_i = \beta^i$ con i variando en $\{1, \ldots, q - 1\}$. Para hallar la imagen de α hallemos un sistema generador viendo la imagen de un sistema generador de $L(G)$

$$\mathrm{Im}(\alpha) = \left\langle \left(f(\beta), \ldots, f(\beta^{q-1}) \right) \mid f \in \{1, x, \ldots, x^r\} \right\rangle,$$

por lo que obtenemos un sistema generador del código que sería

$$\left\{ (1, \ldots, 1),\ (\beta, \beta^2, \ldots, \beta^{q-1}),\ (\beta^2, \beta^4, \ldots, \beta^{2(q-1)}),\ \ldots,\ (\beta^r, \beta^{2r}, \ldots, \beta^{r(q-1)}) \right\}.$$

La dimensión del código será como máximo $r + 1$ pues $L(G)$ tenía esta dimensión. Podemos entonces dar un sistema de $q - 1 - (r + 1)$ ecuaciones independientes y ver que el código tiene dimensión máxima. En concreto estas ecuaciones serían:

$$\left(c_1, \ldots, c_{q-1}\right) \in \mathrm{Im}(\alpha) \iff \sum_{i=1}^{q-1} c_i (\beta^l)^i = 0, \quad 1 \leq l \leq q - 1 - (r + 1).$$

Escribamos la matriz de control que codifica a estas ecuaciones (lo que al mismo tiempo dejará claro por qué estas ecuaciones son independientes). Para ello, tengamos en cuenta que $\beta^{q-1} = 1$. Entonces la matriz de control sería:

$$\begin{pmatrix} \beta & \beta^2 & \beta^3 & \cdots & 1 \\ \beta^2 & \beta^4 & \beta^6 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ \beta^{q-r-2} & \beta^{2(q-r-2)} & \beta^{3(q-r-2)} & \cdots & 1 \end{pmatrix},$$

la cual es una matriz de rango máximo pues corresponde a un determinante de tipo Vandermonde.

En concreto, podemos observar que la matriz es la de un código BCH (ver sección 1.4) con una permutación de la primera y la última coordenada. Los parámetros longitud n y b de este código BCH son $n = q - 1$ y $b = 1$. A este tipo de códigos se les denomina códigos de tipo Reed-Solomon y son una familia de códigos MDS (lo cual justificaremos a continuación) que, vistos como códigos algebraico-geométricos, son resultado del caso particular en el que la curva escogida es la recta proyectiva.

Los códigos Reed-Solomon son la familia de códigos correctores más utilizada a día de hoy estando implementados en diversos dispositivos como códigos QR, tecnología tipo Blu-ray y muchísimos tipos de canales relacionados con comunicaciones. Estos códigos surgieron en los años 60 como un caso particular de los códigos BCH que vimos en el primer capítulo. Veremos pronto que seremos capaces de mejorar por mucho esta familia de códigos gracias a los códigos algebraico-geométricos.

Analicemos los parámetros del código usando los teoremas anteriores y veamos lo rápido que somos capaces de calcular la dimensión y la distancia mínima a través de ellos. Por el corolario 2.1 y por la desigualdad de Riemann, podemos concluir que, como $\mathbb{P}^1$ es de género 0, $l(D) = \deg(D) + 1$ para cualquier divisor D efectivo. En tal caso, por el teorema 3.1, se tiene que

$$k = \dim C(D, G) = r + 1 - l(G - D) = r + 1,$$

donde hemos usado que como $\deg(G-D) = r-(q-1) < 0$, tenemos que $l(G-D) = 0$. Por otro lado, $d \geq q - 1 - \deg(G) = q - 1 - r$. Por tanto,

$$k + d \geq r + 1 + q - 1 - r = q = n + 1,$$

con n la dimensión del espacio ambiente que es $q - 1$. Es decir la desigualdad de Singleton se alcanza y por tanto este código es MDS [1].

El que utilicemos $\mathbb{P}^1$ u otra curva de género 0 es irrelevante para los cálculos de la dimensión como veremos derivado de esta proposición:

Proposición 3.1. Si $2g - 2 < \deg(G) < n$ entonces $k = \deg(G) + 1 - g$.

Demostración. Si $\deg(G) < n$ entonces $\deg(G-D) < 0$ luego $l(G-D) = 0$ y además, dado que $\deg(G) > 2g - 2$, por el teorema 2.6 se tiene que $l(G) = \deg(G) - g + 1$ y por tanto $k = l(G) - l(G - D) = \deg(G) - g + 1$.

[1] Un argumento muy similar a este prueba que todo códigos Reed-Solomon es MDS.

Los códigos $C(D, G)$ con G verificando la proposición anterior se suelen llamar códigos **fuertemente algebraico-geométricos** y son la familia de códigos de este tipo que mejor conocemos puesto que somos capaces de saber exactamente su dimensión y, como veremos en un momento, su distancia mínima.

En principio, no existe ninguna manera general a través de G y D de conocer directamente la distancia mínima del código. Por eso normalmente se trabaja con la cantidad $d^* = n - \deg(G)$ como una primera aproximación a d. Sin embargo, si se puede encontrar un divisor efectivo equivalente a G acotado por D, podemos calcular exactamente d.

Proposición 3.2. Si $\deg(G) < n$, $d = d^*$ si y solo si existe un divisor D' tal que $0 \leq D' \leq D$ que sea equivalente a G.

Demostración. Según la prueba del teorema 3.1, la distancia mínima es d si y solo si hay $n - d$ puntos $P_1, \ldots, P_{n-d}$ tales que $l(G - P_1 - \ldots - P_{n-d}) > 0$.

Si $d = d^*$ entonces $n - d = \deg(G)$ por lo que $\deg(G) = \deg(P_1 - \ldots - P_{n-d})$. Como $l(G - P_1 - \ldots - P_{n-d}) > 0$, cualquier función en este espacio da la equivalencia entre estos dos divisores.

Veamos por último cómo se comportan los códigos fuertemente algebraico-geométricos en cuanto a la cota de Singleton.

Proposición 3.3. Si $2g - 2 < \deg(G) < n$, se tiene que $n + 1 - g \leq k + d \leq n + 1$.

Demostración. Es una consecuencia directa de la cota de la distancia del teorema 3.1 y la dimensión para estos códigos de la proposición 3.1.

Corolario 3.1. Si $C(G, D)$ es un códigos fuertemente algebraico-geométrico sobre una curva de género 0 entonces $C(G, D)$ es un código MDS.

3.2 Generalizaciones y ejemplos

La gran variedad de formas que puede tomar el espacio $L(G)$ en función del divisor y de la curva que escojamos hace que los códigos Goppa sean una familia muy general y la mayoría de los códigos que vimos en el capítulo introductorio de teoría de códigos pueden verse como casos particulares de la familia de códigos algebraico-geométricos.

En el ejemplo 3.1 ya vimos que los códigos Goppa en la recta proyectiva dan lugar a los códigos Reed-Solomon que no son más que, a su vez, un caso particular

de los códigos BCH. De la misma forma, podemos ver los códigos de Goppa clásicos (ver sección 1.5) como un código algebraico-geométrico para un cierto divisor. Sin embargo, la construcción explícita de este divisor no es posible darla sin hablar del teorema de Riemman-Roch. Por no extender demasiado el texto, esto se trata con más detenimiento en una sección del apéndice dedicado este tema (ver sección 4.3) donde además se expone este ejemplo. Aquí daremos de forma simplemente una explicación más vaga solo para ilustrar que, efectivamente, los códigos Goppa generalizan a los códigos de Goppa clásicos.

Sea $L = \{\gamma_0, \dots, \gamma_{n-1}\} \subseteq \mathbb{F}_{q^m}$ puntos diferentes y sea $g(x) \in \mathbb{F}_{q^m}[x]$ que no se anula en ningún γ_i. Entonces el código de Goppa clásico está definido como:

$$\Gamma(L, g) = \left\{ (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0 \mod g(x) \right\}.$$

Resulta que si tomamos Z el divisor de ceros de g en la recta proyectiva y los puntos $P_i = (\gamma_i : 1), Q = (1 : 0)$ y tomamos $D = P_0 + \dots + P_{n-1}$ entonces el conjunto $\Gamma(L, g)$ no es más que el dual del código $C(D, Z - Q)$. El concepto de dualidad también se explica en el apéndice pero puede entenderse como el espacio ortogonal clásico de álgebra lineal del código $C(D, Z - Q)$.

En general, ocurre que el código dual de un código Goppa vuelve a ser un código Goppa para un divisor especial. En concreto, el código dual de $C(D, G)$ coincide con el espacio $C(D, K + D - G)$ donde K es un divisor de una forma diferencial con polos simples los P_i y residuo 1. Más allá de esto, existen cuatro formas clásicas de construir códigos Goppa asociados a un mismo divisor G ,todas ellas teniendo fuertes relaciones entre sí y derivadas de la geometría algebraica.

Una vez hemos visto que los códigos Goppa constituyen una de las familia amplia en teoría de códigos, pasemos a construir algunos ejemplos un poco más complejos.

Ejemplo 3.2 (La cuártica de Klein). Sea $F = x^3y + y^3z + xz^3$ y consideremos $X = \mathcal{V}(F) \subseteq \mathbb{P}_k^2$ la cuártica de Klein. Como ya vimos en el ejemplo 2.10, uno puede comprobar (ya sea probando todas las combinaciones o bien utilizando argumentos más finos basándose en la teoría de Galois vista en el capítulo anterior) que sobre $k = \mathbb{F}_8$ esta curva tiene un total de 24 puntos de grado 1.

Si tomamos entonces $Q = (0 : 0 : 1)$, D la suma de los otros 23 puntos restantes y tomamos $G = mQ$ para $4 \leq m \leq n = 23$, obtenemos que $C(D, G)$ es fuertemente algebraico-geométrico luego por la proposición 3.1 se tiene que $k = \deg(G) + 1 - g$ y $d \geq n - \deg(G)$. Pasemos a ver cuáles son los posibles valores de k y d.

Por la fórmula de Plücker, $g = 3$ y $\deg(G) = m$. Sustituyendo, obtenemos que:

$$k = m - 2, \qquad d \geq 23 - m.$$

En concreto, para $m = 10$, uno obtiene un código de parámetros $(23, 8, 13)$ siendo pesimista para la distancia mínima.

Lo habitual en teoría de códigos es utilizar el alfabeto $\mathbb{F}_2$. Esto se suele hacer a través de un código de paridad (ver ejemplo 1.3). Podemos entonces concatenar estos dos códigos como estudiamos en la definición 1.10: viendo cada elemento de $\mathbb{F}_8$ como un vector de longitud 4 de $\mathbb{F}_2$, podemos construir un código de paridad $(4, 3, 2)$. Interpretando los elementos de $\mathbb{F}_8$ de $C(G, D)$ de esta manera y reemplazando cada elemento por su correspondiente vector de $\mathbb{F}_2^4$ bajo la aplicación lineal definida por el código de paridad $(4, 3, 2)$, uno obtiene un código $(23 \cdot 4, 8 \cdot 3, 13 \cdot 2) = (92, 24, 26)$ lo cual estableció en su momento un récord para la tasa de transmisión en códigos de esta longitud y distancia.

Cabe preguntarse qué es lo que hace a la cuártica de Klein una curva apropiada para construir un código de Goppa. La respuesta está en que es una curva con muchos puntos de grado 1 (los que hemos denominado puntos racionales). Gracias a esto, podemos tomar D compuesto por muchos puntos de grado 1 haciendo que el código pueda transmitir mucha más información puesto que la elección de D afecta directamente a la dimensión de nuestro espacio ambiente. Por otro lado, la elección de G se hace de manera que la dimensión del código y la distancia mínima lleguen a un punto medio que nos interese ya que sabemos que no podemos aumentar ambas cantidades a la vez según la desigualdad de Singleton. En resumen, las curvas con muchos puntos racionales son ideales para construir códigos Goppa sobre ellas.

Debido a esto, deberíamos preguntarnos si somos capaces de estimar el número de puntos racionales que va a tener una curva sobre un cuerpo finito. Resulta que esta pregunta es interesante por muchísimas más razones que las que estamos aquí tratando y es un tema ya muy estudiado. Tradicionalmente estimar estas cantidades involucra el uso de lo que se llaman funciones zeta sobre cuerpos finitos, unas funciones de variable compleja que tienen estructura de series de Dirichlet al igual que la función zeta de Riemann. Uno de los teoremas principales que se acaba deduciendo de este estudio es la **cota de Hasse[2]-Weil[3]** la cual enunciamos sin dar la prueba.

[2]Helmut Hasse, matemático alemán nacido en 1898 y fallecido en 1979 con grandes aportaciones a la teoría de números algebraica.

[3]André Weil fue un matemático francés nacido en 1906 y fallecido en 1998. Conocido por las pro-

Teorema 3.2 (Cota de Hasse-Weil). *Sea X una curva de género g sobre $\mathbb{F}_q$. Si denotamos por $N_q(X)$ el número de puntos racionales de X, se tiene que:*

$$\left|N_q(X) - (q+1)\right| \leq 2g\sqrt{q}.$$

Demostración. Una demostración que sigue la línea de la teoría desarrollada en el apéndice puede encontrarse en [1].

Gracias a este resultado podemos buscar las curvas que tengan el máximo número de puntos racionales según esta cota y construir códigos Goppa sobre ellas.

Ejemplo 3.3 (Curvas Hermitianas). Consideremos la curva $X = \mathcal{V}(F) \subseteq \mathbb{P}^2(\mathbb{F}_q)$ con $F = x^{r+1}+y^{r+1}+z^{r+1} \in k[x,y,z]$. Estas curvas (variando r) forman la familia conocida como curvas hermitianas.

Consideremos el caso particular $q = r^2 = 2^l$. Por la fórmula de Plücker,

$$g = \frac{r(r-1)}{2} = \frac{1}{2}\left(q - \sqrt{q}\right).$$

Veamos que estas curvas tienen el máximo número de puntos racionales. Esto es, por la cota de Hasse-Weil, un máximo de $N_q(X) = 1 + q\sqrt{q}$ puntos de grado 1.

Pongamos que una de las tres variables es nula, $xyz = 0$, entonces, sin pérdida de generalidad, la otra es 1 y tenemos que $x^{r+1} = 1$ ya que estamos en un cuerpo de característica 2. Como nuestro cuerpo tiene r^2 elementos, su grupo multiplicativo tiene $r^2 - 1 = (r+1)(r-1)$ elementos. Usando además que sabemos que el grupo multiplicativo es cíclico, digamos $\mathbb{F}_q^* = \langle\beta\rangle$, tenemos que las soluciones son explícitamente $\{\beta^{r-1}, \beta^{2(r-1)}, \ldots, \beta^{(r-1)(r+1)}\}$ por lo que llegamos a que en el cuerpo están todas las $r+1$ soluciones de $x^{r+1} = 1$. Permutando, tenemos que hay $3(r+1)$ puntos racionales con $xyz = 0$.

Digamos ahora que $xyz \neq 0$ y razonemos de forma similar. Sin pérdida de generalidad, $z = 1$ y despejando se tiene que $x^{r+1} = 1 + y^{r+1}$. Si $y^{r+1} \neq 1$, entonces $1 + y^{r+1} \neq 0$ y, dado que β genera $\mathbb{F}_q^*$, β^{r+1} genera $\mathbb{F}_r$ (ya que $\mathbb{F}_q^*$ tiene $(r+1)(r-1)$ elementos) lo cual nos dice que $y^{r+1} \in \mathbb{F}_r$ y por tanto que $1 + y^{r+1} \in \mathbb{F}_r$ luego este elemento se puede poner como una potencia $(r+1)$-ésima de β y por tanto tiene una raíz $(r+1)$-ésima. Esto, junto con que $x^{r+1} = 1$ tiene las $r+1$ soluciones, prueba

fundas conexiones que descubrió entre la teoría de números y la geometría algebraica, es una de las figuras más destacadas del siglo XX en ambos campos.

que tenemos $r+1$ soluciones para x para cada elección de y. Como para y tenemos $r^2-1-(r+1) = (r+1)(r-1-1) = (r+1)(r-2)$ opciones, esto nos da $(r-2)(r+1)^2$ valores para x e y. Se tiene por tanto que X tiene

$$3(r+1) + (r-2)(r+1)^2 = 3(r+1) + r^3 - 3r - 2 = r^3 + 1 = 1 + q\sqrt{q}$$

puntos racionales, que, por el teorema 3.2, es el máximo número de puntos racionales posibles para este cuerpo y este género.

Procedemos como siempre y tomamos $G = mQ$ con Q un punto que puede ser arbitrario, digamos por fijar, $Q = (0 : 1 : 1)$ y pongamos $q - \sqrt{q} < m < q\sqrt{q}$ para obtener un código fuertemente algebraico geométrico. Tomemos por último D como la suma del resto de puntos racionales. Entonces, por la proposición 3.1, se tiene que $k = m + 1 - g$ y la distancia d es por el teorema 3.1, $d \geq d^* = n - m$.

Veamos lo buenos que son estos códigos. Tomemos $q = 16$ y $m = 37$. Entonces $k = 32$ y $d \geq d^* = 27$. Comparando esto con los códigos tipo Reed-Solomon del ejemplo 3.1 (que son los códigos más utilizados a día de hoy) sobre el mismo alfabeto, $\mathbb{F}_{16}$ y tomemos $r = 8$. Con esta elección de r hacemos que ambos códigos tengan el ratio tasa de transmisión, $1/2$. Obtenemos entonces que el código Reed-Solomon puede transmitir palabras de tamaño 15 con una distancia mínima de 7 unidades.

Para un canal con el que la probabilidad de transmitir mal un caracter sea de $p = 0.01$ y asumiendo que recibimos una palabra equivocada, obtenemos que el código Reed-Solomon tiene una probabilidad de aún tener una palabra incorrecta de alrededor de $3 \cdot 10^{-4}$ lo cual es muy bueno. Sin embargo, $C(G, D)$ tiene un probabilidad de fallar menor a $2 \cdot 10^{-7}$ que es una mejora de 3 órdenes de magnitud.

Observación 3.1. Según el teorema 3.2, la cuártica de Klein del ejemplo 3.2 puede tener hasta 25 puntos racionales y ya vimos en el ejemplo 2.10 que tenía 24. Al tener casi todos sus puntos racionales posibles, es una curva idónea para la construcción de códigos Goppa.

Solo tenemos una cosa pendiente: hemos de construir explícitamente los códigos de los que hemos estado hablando de forma teórica todo este tiempo. Para ello, es necesario hallar o bien una matriz generatriz, o bien una matriz de control de estos códigos la que nos sirve además para los algoritmos de decodificación que precisan de ella. Encontrar una de estas matrices se basa en conocer bien el espacio $L(G)$ en los ejemplos anteriores y será la geometría, por tanto, la que nos permita resolver este problema.

Ejemplo 3.4 (Matriz generatriz para la cuártica de Klein). Sea X la cuártica de Klein dada en el ejemplo 3.2 sobre $\mathbb{F}_8$. Ya vimos en el ejemplo 2.3 que y/z es un parámetro local en el $Q = (0 : 0 : 1)$. De forma totalmente análoga se prueba que las funciones z/x y x/y son parámetros locales en $P_1 = (1 : 0 : 0)$ y $P_2 = (0 : 1 : 0)$ respectivamente.

Vamos a ver cómo se comporta y/z en estos dos puntos. De la ecuación de X en P_1 obtenemos despejando que

$$\frac{y}{z} = \left(\frac{z}{x}\right)^2 \frac{x^3}{x^3 + y^2 z}$$

Como $x^3 + y^2 z$ no se anula en P_1, y/z tiene un cero de multiplicidad 2. De forma análoga, en P_2 tenemos que

$$\frac{y}{z} = \left(\frac{y}{x}\right)^3 \frac{y^3 + z^2 x}{y^3},$$

por lo que tenemos un polo de multiplicidad 3. Estos son todos los posibles ceros y polos de y/z, de donde

$$\left(\frac{y}{z}\right) = 2P_1 - 3P_2 + Q.$$

Con razonamientos similares se acaba deduciendo que

$$\left(\frac{x}{y}\right) = -3P_1 + P_2 + 2Q, \quad \left(\frac{z}{x}\right) = P_1 + 2P_2 - 3Q.$$

La observación fundamental para acabar calculando $L(G) = L(10\,Q)$ es que

$$\left(\frac{z}{x}\right)^a \left(\frac{y}{x}\right)^b \in L(10\,Q), \quad \text{para } 0 \leq 3a + 2b \leq 10, \;\; 0 \leq b \leq 2a,$$

que es una mera comprobación después de haber ajustado los valores de a y b para que estas funciones estén en el espacio.

Esto nos da un total de 8 funciones que están en $L(10\,Q)$ que coincide con la dimensión del espacio $l(10\,Q) = \deg(10\,Q) + 1 - g = 8$. Falta comprobar que son independientes pero esto se tiene debido a que cada una de estas 8 funciones tiene un polo de orden distinto en Q, haciendo las cuentas (órdenes $0, 2, 5, 6, 7, 8, 9, 10$ respectivamente).

Ya solamente falta sustituir las coordenadas de los puntos racionales de X para conseguir una matriz generatriz. El resultado es una matriz 23×8 que, desgraciadamente, es demasiado grande para que quepa en una hoja. No debemos aún así preocuparnos pues existen librerías de Sage con estos códigos ya implementados.

Ejemplo 3.5 (Matriz generatriz para curvas hermitianas). Ya vimos en el ejemplo 3.3 que para la curva hermitiana sobre $\mathbb{F}_{16}$ con $q - \sqrt{q} < m < q\sqrt{q}$ se tenía que $l(G) = l(mQ) = m + 1 - g$ siendo $Q = (0 : 1 : 1)$.

Al igual que en el ejemplo anterior, vamos a dar una base de $L(G)$ explícitamente. Estas serán las funciones:

$$f(a, b; x, y, z) = \frac{x^a y^b}{(y+z)^{a+b}}; \quad 0 \leq a \leq 4, \quad 4a + 5b \leq m \quad a, b \in \mathbb{Z}$$

Esto nos da, efectivamente, un total de $m - 5 = m + 1 - g$ funciones diferentes. Veamos que todas estas están en $L(G)$ y que son independientes.

Considerando la carta afín $z = 1$, tenemos que Q se corresponde con el punto afín $(0, 1)$. En tal caso, la función x/z parece una elección muy razonable para ser un parámetro local en Q. En efecto, haciendo el cambio para trabajar con el origen, uno comprueba que $\partial f/\partial y(0, 1) = r + 1 \neq 0$ puesto que $r + 1$ es impar por ser r^2 una potencia de 2. Por tanto, x/z es un parámetro local en Q. Análogamente, otro parámetro local de la curva en Q sería x/y. Teniendo esto en cuenta podemos observar que en la curva:

$$\frac{x}{(y+z)} = \frac{x\left(\sum_{i+k=r} y^i z^j\right)}{y^{r+1} + z^{r+1}} = \left(\frac{z}{x}\right)^r \frac{\sum_{i+k=r} y^i z^j}{z^r},$$

donde hemos usado la identidad clásica

$$(a+b)^n = (a+b)\left(\sum_{i+k=n} a^i b^j\right),$$

que se da en cuerpos de característica 2. De igual forma, aplicando esta misma identidad a $y/(y+z)$ obtenemos que

$$\frac{y}{y+z} = \frac{y\left(\sum_{i+k=r} y^i z^j\right)}{y^{r+1} + z^{r+1}} = \left(\frac{y}{x}\right)^{r+1} \frac{\left(\sum_{i+k=r} y^i z^j\right)}{y^r}$$

En conclusión, la función $x/(y+z)$ tiene un polo de orden r en Q y la función $y/(y+z)$ tiene un polo de orden $r+1$ en Q. En el caso que nos concierne, $r = 4$ y por

tanto podemos concluir que la función

$$f(a,b;x,y,z) = \frac{x^a y^b}{(y+z)^{a+b}}$$

tiene un polo en Q de orden $4a+5b$ y por tanto todas estas funciones son independientes. Por último, las condiciones impuestas sobre a y b hacen que las funciones $f(a,b;x,y,z)$ estén en $L(G)$ por definición. La matriz generatriz del código se podría obtener por tanto, sustituyendo estas funciones en cada uno de los puntos racionales de nuestra curva.

Observación 3.2. La construcción anterior es válida para cualquier q en las condiciones del ejemplo 3.3. Hemos tomado $q = 16$ por ser el ejemplo más conocido históricamente sobre este tipo de códigos.

3.3 Mejora de la cota de Gilbert-Varshamov

Los códigos algebraico-geométricos presentan una de las familias de códigos lineales más generales que existen. En función de la curva que escojamos y de los puntos racionales de esta, podemos construir códigos con una cantidad muy diversa de parámetros. Además cuanta más información tengamos sobre la curva, más información podemos obtener sobre los códigos algebraico-geométricos que podemos construir sobre ella. Un ejemplo de esto lo hemos visto al tratar de acercarnos a la cota de Hasse-Weil en la sección anterior. El gran desarrollo de la geometría algebraica en cuerpos finitos por André Weil y más tarde las técnicas creadas por Alexander Grothendieck[4] para atacar estos problemas, arrojan una cantidad de resultados sorprendentes sobre los códigos algebraico-geométricos. En particular cabe resaltar que existe una familia infinita de códigos algebraico-geométricos que se hallan por encima de la cota de Gilbert-Varshamov. Hasta ese entonces, se conocía que si entre todos los códigos conocidos se toma una sucesión "al azar" una restricción sobre la distancia mínima relativa al código, entonces su tasa de transmisión converge a cero casi seguro, lo cual implicaría que se superaba la cota de Gilbert-Varshamov. Sin embargo ninguna familia infinita de códigos conocidos hasta la fecha verificaba tal propiedad. Los códigos Goppa rompieron con esta tendencia teniéndose este teorema, probado por Tsfasman, Vlăduţ y Zink:

[4]Matemático franco–alemán nacido en 1928 y fallecido en 2014. Uno de los fundadores de la geometría algebraica moderna y uno de los matemáticos más influyentes del siglo XX.

Teorema 3.3 (Tsfasman, Vlăduţ y Zink). *Si q es una potencia par de un primo, existe una familia infinita de curvas $\mathcal{X}_i$ ($i \in \mathbb{N}$), tal que $\mathcal{X}_i$ tiene $n_i + 1$ puntos racionales y género g_i teniéndose que n_i tiende a infinito cuando lo hace i y tal que*

$$\frac{g_i}{n_i} \longrightarrow \left(q^{\frac{1}{2}} - 1\right)^{-1}, \qquad \text{cuando } i \to \infty.$$

Demostración. La prueba se encuentra en el libro de Tsfasman, Vlăduţ y Zink en [8].

Como se puede deducir del teorema 3.1, esto implica que el código fuertemente algebraico-geométrico correspondiente a esta curva con $G = m_i Q$ y $D = \sum_{k=1}^{n_i} P_k$ tiene ratio $(m_i - g_i + 1)/n_i$ y distancia mínima $d_i \geq n_i - m_i$ luego asintóticamente estos códigos superan la cota de Gilbert-Varshamov.

En concreto, uno encuentra una mejora estricta de la cota para $q \geq 49$ marcando un antes y un después para la rama de teoría de códigos.

4 Apéndice

4.1 Dualidad en códigos correctores

Veremos en esta breve sección que dado un código lineal C, podemos construir un código asociado a él al que denominaremos el dual de C cuyos parámetros y propiedades pueden ser deducidas en su mayoría, a través del estudio del código C.

Sea por tanto $C \subset \mathbb{F}_q^n$ un código lineal y sea A una matriz de control de este. Como A es de rango máximo, A^t puede ser interpretada como una matriz generatriz de otro código sobre $\mathbb{F}_q$.

Definición 4.1. *En las condiciones anteriores, tal código es llamado el código dual de C y se denotará como $C^\perp$.*

Por construcción, si C es de dimensión k, $C^\perp$ es de dimensión $n-k$. Si además $\mathcal{M}$ es una matriz generatriz de C, sabemos que $A \cdot \mathcal{M} = \mathbf{0}$ lo que implica que $\mathcal{M}^t \cdot A^t = \mathbf{0}$ y $\mathcal{M}^t$ es de rango máximo luego es una matriz de control para $C^\perp$.

Para entender la relación entre estos dos códigos, introducimos una forma bilineal que imita al producto escalar de $\mathbb{R}$. Consideramos la forma bilineal definida como sigue: si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$,

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

a la que llamaremos producto escalar, igual que en $\mathbb{R}$. Esta nomenclatura no es precisa, ya que la operación anterior no es un producto escalar en el sentido estricto de la palabra. Por ejemplo, en $\mathbb{F}_2^4$, $1100 \cdot 1100 = 0$.

Sin embargo, sí que es una operación simétrica y lineal en cada uno de los factores. Utilizando estas propiedades y el mismo argumento que en $\mathbb{R}$ o en $\mathbb{C}$, puede demos-

trarse que la dimensión del ortogonal de un subespacio vectorial C de dimensión k es de dimensión $n-k$ (pues es el conjunto de soluciones de un sistema lineal homogéneo de k ecuaciones).

La única diferencia principal con un producto escalar propiamente dicho es pues la existencia de vectores ortogonales a sí mismo y por tanto, el hecho de que la intersección de C y su ortogonal puede ser no nula.

Proposición 4.1. Si C es un código lineal, su dual, $C^{\perp}$, es el ortogonal de C.

Demostración. Se deduce directamente de que el producto de la matriz generatriz de C por la matriz generatriz de $C^{\perp}$ es nula como hemos visto antes. Por tanto el código generado por las filas de la matriz generatriz está contenido en $C^{\perp}$. Al tener la misma dimensión, se prueba que este código es, de hecho, el código ortogonal.

Para finalizar esta sección, enunciaremos un teorema que no se probará relativo al cálculo de la distancia mínima del código $C^{\perp}$.

Definición 4.2. *Si $C \subset \mathbb{F}_q^n$ es un código lineal, se define el polinomio de pesos*

$$W(x) = \sum_{i=0}^{n} a_i x^i,$$

donde a_i es el número de elementos de C de peso exactamente i. Se define el polinomio de pesos homogeneizado $W(x, y)$ como el homogeneizado de $W(x)$ a grado n mediante la variable y.

Observación 4.1. Con la definición anterior, está claro que la distancia mínima de C coincide con el primer índice no nulo cuyo coeficiente a_i tiene un valor distinto de cero.

La ventaja de introducir este polinomio que recoge la distribución de pesos es que muchas veces en teoría de códigos, si C es un código de tamaño muy elevado, su dual $C^{\perp}$ será pequeño por lo que su polinomio de pesos será de cómputo más sencillo y podemos relacionar estos dos a través del siguiente resultado:

Teorema 4.1 (Identidad de MacWilliams). *Si C es un código de longitud n y dimensión k sobre $\mathbb{F}_q$ y $W(x, y)$ y $W^{\perp}(x, y)$ son los polinomios de pesos homogeneizados de C y $C^{\perp}$ respectivamente, se tiene que*

$$W^{\perp}\big(x, y\big) = q^{-k} W\big(y - x,\ y + (q-1)x\big).$$

Demostración. Puede encontrarse en [2].

4.2 Género de una curva proyectiva sin puntos singulares

Tradicionalmente al estudiar códigos algebraico-geométricos es necesario pasar por estudiar formas diferenciales sobre curvas. Esto implica tener que alejarse de una perspectiva puramente algebraica del tema para introducirse en el estudio de unos objetos más relacionados con la teoría de la integración. Por eso, proponemos aquí un enfoque canalizado a través de la aritmética geométrica que no precisa de la mención de 1-formas.

Para esta sección, cambiaremos la notación habitual de $L(D)$ para el espacio de Riemman-Roch asociado al divisor D por la notación[1] $H^0(D)$ y su dimensión la denotaremos por $h^0(D)$ en vez de $l(D)$. El objetivo de esta sección será describir el género de una curva de manera algebraica.

Definición 4.3. *Sea X una curva proyectiva no singular sobre un cuerpo k. Para cada $P \in X$ definimos $H^0(D)_P$ como:*

$$H^0(D)_P = \left\{ f \in \mathcal{K}(X) \mid \operatorname{ord}_P(f) + \operatorname{ord}_P(D) \geq 0 \right\}.$$

Consideremos el siguiente homomorfismo de k-espacios vectoriales:

$$\begin{array}{rcl} \varphi_D : \mathcal{K}(X) & \longrightarrow & \bigoplus_{P \in X} \left(\mathcal{K}(X)/H^0(D)_P \right) \\ f & \mapsto & \bigoplus_{P \in X} \left(f \mod H^0(D)_P \right) \end{array}$$

Por definición, $\ker(\varphi_D) = H^0(D)$.

Definición 4.4. *El espacio $H^1(D)$ se define[2] como el conúcleo de la aplicación anterior, $H^1(D) = \operatorname{coker}(\varphi_D)$.*

Con esta definición, está claro que, por construcción, la siguiente sucesión es exacta:

$$0 \to H^0(D) \to \mathcal{K}(X) \xrightarrow{\varphi_D} \bigoplus_{P \in X} \left(\mathcal{K}(X)/H^0(D)_P \right) \to H^1(D) \to 0$$

[1] Esta notación tan sugerente se debe a que este espacio es isomorfo al grupo 0-ésimo de una cierta cohomología que se asigna a una curva no singular y al divisor D.

[2] Como el lector puede imaginarse, este espacio es isomorfo al primer grupo de la cohomología de la que se habló en el anterior pie de página.

Es decir, $H^1(D)$ mide la diferencia entre el espacio "global" $H^0(D)$ y el espacio "local" $\bigoplus_{P\in X}\left(f \mod H^0(D)_P\right)$. Esta diferencia es precisamente lo que trata de medir el género de una curva. Para ver la definición en concreto, tenemos que hablar un poco del espacio $H^1(D)$.

Teorema 4.2. *$H^1(D)$ es de dimensión finita para cualquier divisor.*

Demostración. La prueba es bastante técnica y se apoya en el uso de la estructura de los anillos de funciones regulares para abiertos en la curva, los cuales son dominios de Dedekind. La demostración completa puede encontrarse en [1]. ∎

A la dimensión del espacio $H^1(D)$ la denotaremos por $h^1(D)$. Vamos por último a ver en detalle la prueba de que el número entero $h^0(D)-h^1(D)-\deg(D)$ es una constante que no depende del divisor D escogido. Para ello, vamos primero a establecer la situación general con la que vamos a trabajar y después veremos un par de lemas previos a la prueba.

Sean $D \geq E$ dos divisores. Entonces por definición, $H^0(E) \subseteq H^0(D)$. Sea φ_1 la inclusión entre estos dos espacios. Denotemos por φ_2 la identidad en $\mathcal{K}(X)$ y sea

$$\varphi_3 : \bigoplus_P \mathcal{K}(X)/H^0(E)_P \to \bigoplus_P \mathcal{K}(X)/H^0(D)_P$$

la aplicación sobreyectiva que se obtiene como la suma directa de las aplicaciones

$$\varphi_{3,P} : \mathcal{K}(X)/H^0(E)_P \to \mathcal{K}(X)/H^0(D)_P$$

que induce la inclusión $H^0(E)_P \subseteq H^0(D)_P$. Entonces se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(E) & \longrightarrow & \mathcal{K}(X) & \xrightarrow{\varphi_D} & \bigoplus_{P\in X}\left(\mathcal{K}(X)/H^0(E)_P\right) & \longrightarrow & H^1(E) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_{E,D}} & & \\
0 & \longrightarrow & H^0(D) & \longrightarrow & \mathcal{K}(X) & \longrightarrow & \bigoplus_{P\in X}\left(\mathcal{K}(X)/H^0(D)_P\right) & \longrightarrow & H^1(D) & \longrightarrow & 0
\end{array} \tag{4.1}$$

donde $\varphi_{E,D}$ es la aplicación inducida por φ_3 entre los conúcleos de φ_E y φ_D. Nuestro objetivo es probar que $\ker(\varphi_3)$ es de dimensión finita y hallar su dimensión. Para ello, usaremos algunos lemas.

Observación 4.2. Si k es un cuerpo y tenemos unas inclusiones de k-espacios vectoriales de la forma:

$$0 = V_0 \subset V_1 \subset \ldots \subset V_{q-1} \subset V_q = V,$$

de manera que la dimensión de V_i/V_{i-1} es finita, entonces la dimensión de V es $\dim(V) = \sum_{i=1}^{q} \dim(V_i/V_{i-1})$, simplemente utilizando que la dimensión del cociente es la diferencia de las dimensiones.

Lema 4.1. Sea t_P un parámetro local en $P \in X$. Entonces si $q \leq r$ se tiene que $t_P^r\mathcal{O}_P \subseteq t_P^q\mathcal{O}_P$ y el cociente $t_P^q\mathcal{O}_P/t_P^r\mathcal{O}_P$ es un $k-$espacio vectorial de dimensión finita de dimensión $(t-s)\deg(P)$.

Demostración. Como $k \subseteq \mathcal{O}_P$, estos espacios son claramente $k-$espacios vectoriales. Se tiene la cadena de inclusiones:

$$t_P^r\mathcal{O}_P \subset t_P^{r-1}\mathcal{O}_P \subset \ldots \subset t_P^{q+1}\mathcal{O}_P \subset t_P^q\mathcal{O}_P.$$

La observación anterior nos dice que solo tenemos que probar que la dimensión del espacio $t_P^m\mathcal{O}_P/t_P^{m+1}\mathcal{O}_P$ es $\deg(P)$. Esto se sigue de que sabemos que la dimensión de $\mathcal{O}_P/\langle t_P\rangle$ es $\deg(P)$ por definición y podemos establecer un isomorfismo entre $\mathcal{O}_P$ y $t_P^m\mathcal{O}_P$ de manera que a cada $f \in \mathcal{O}_P$ le asociamos $t_P^m f$. Por transitividad, esto prueba que los espacios $\mathcal{O}_P/t_P\mathcal{O}_P$ y $t_P^m\mathcal{O}_P/t_P^{m+1}\mathcal{O}_P$ son isomorfos lo que finaliza la prueba. ∎

Lema 4.2. Si $D \geq E$ entonces $\dim\left(\bigoplus_P H_P^0(D)/H_P^0(E)\right) = \deg(D) - \deg(E)$.

Demostración. El lema anterior prueba que cada espacio vectorial $H_P^0(D)/H_P^0(E)$ tiene dimensión $(\mathrm{ord}_P(D) - \mathrm{ord}_P(E))\deg(P)$. Los órdenes de D y E en cada punto $P \in X$ son nulos salvo para un número finito de puntos luego este espacio es de dimensión

$$\sum_P \left(\mathrm{ord}_P(D) - \mathrm{ord}_P(E)\right)\deg(P) = \deg(D) - \deg(E).$$

∎

Volviendo al diagrama 4.1, el lema anterior prueba que el núcleo de φ_3 es un $k-$espacio vectorial de dimensión $\deg(D) - \deg(E)$. Esto, junto al siguiente lema nos dará las herramientas necesarias para probar el resultado que queremos.

Lema 4.3. Consideremos el siguiente diagrama conmutativo de filas exactas:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & V_1 & \xrightarrow{a} & V_2 & \xrightarrow{b} & V_3 & \xrightarrow{c} & V_4 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \\
0 & \longrightarrow & W_1 & \xrightarrow{\alpha} & W_2 & \xrightarrow{\beta} & W_3 & \xrightarrow{\gamma} & W_4 & \longrightarrow & 0
\end{array}$$

Si φ_2 es un isomorfismo, existe una sucesión exacta

$$0 \to W_1/\varphi(V_1) \longrightarrow \ker(\varphi_3) \longrightarrow \ker(\varphi_4) \to 0$$

Demostración. Del diagrama podemos obtener las sucesiones cortas siguientes conectadas por homomorfismos inducidos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V_2/\ker(b) & \xrightarrow{b} & V_3 & \xrightarrow{c} & \mathrm{Im}(c) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\varphi}_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4 \restriction_{\mathrm{Im}(c)}} & & \\ 0 & \longrightarrow & W_2/\ker(\beta) & \xrightarrow{\beta} & W_3 & \xrightarrow{\gamma} & \mathrm{Im}(\gamma) & \longrightarrow & 0 \end{array}$$

Que se obtiene separando las sucesiones exactas largas por separado y conectándolas con homomorfismos como ahora indicaremos. Sustituyamos antes que, por exactitud, $\ker(b) = \mathrm{Im}(a) = V_1$, $\mathrm{Im}(c) = V_4$,$\ker(\beta) = \mathrm{Im}(\alpha) = W_1$, $\mathrm{Im}(\gamma) = W_4$ e identifiquemos V_1 con $a(V_1)$ y W_1 con $\alpha(W_1)$ (ambas son aplicaciones inyectivas por exactitud) para que el isomorfismo sea natural en cuanto al primer diagrama. Entonces obtenemos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V_2/a(V_1) & \xrightarrow{b} & V_3 & \xrightarrow{c} & V_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\varphi}_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \\ 0 & \longrightarrow & W_2/\alpha(W_1) & \xrightarrow{\beta} & W_3 & \xrightarrow{\gamma} & W_4 & \longrightarrow & 0 \end{array}$$

En cuanto a los homomorfismos que conectan las filas, $\tilde{\varphi}_2$ es la aplicación que a $v_2 + a(V_1) \in V_2/a(V_1)$ le asocia $\varphi_2(v_2) + \alpha(W_1) \in W_2/\alpha(W_1)$ que está bien definida pues si $v_1 \in V_1$, $\varphi_2(a(v_1)) = \alpha(\varphi_1(v_1))$ por conmutatividad del diagrama. Por tanto $\varphi_2(a(v_1))$ cae en $\alpha(W_1)$ luego es cero en $W_2/\alpha(W_1)$.

Las otras dos aplicaciones φ_3 y φ_4 son las mismas que en el primer diagrama.

Estamos ahora en condiciones de aplicar el lema de la serpiente (más conocido como *snake lemma* en inglés) que forma parte de la asignatura de Homología Simplicial. Este nos dice que existe una sucesión exacta corta:

$$0 \to \ker(\tilde{\varphi}_2) \to \ker(\varphi_3) \to \ker(\varphi_4) \to \mathrm{coker}(\tilde{\varphi}_2) \to \mathrm{coker}(\varphi_3) \to \mathrm{coker}(\varphi_4) \to 0$$

Veamos que $\ker(\tilde{\varphi}_2) \simeq W_1/\varphi_1(V_1)$. Vamos a comprobarlo sin mucho detalle y dando una pequeña idea de porqué es así ya que, aunque no es difícil probar que hay un isomorfismo natural en el diagrama, es técnico y haría la prueba innecesariamente tediosa. Teniendo esto en mente, usemos que a, α y φ_2 son inyectivas (a y α por exactitud y φ_2 por hipótesis) luego si $\tilde{\varphi}_2(v_2+a(V_1)) = 0+\alpha(W_1)$, tenemos que $\varphi_2(v_2) \in$

$\alpha(W_1)$ luego por la inyectividad, concluimos que viendo a W_1 como subespacio de V_2 por la inclusión de α y φ_2^{-1}, tenemos que todo W_1 va a 0 por φ_2. Por estar operando no en V_2 sino en $V_2/a(V_1)$, tenemos que este núcleo es salvo V_1. Como vemos por el diagrama la inclusión por φ_1 $V_1 \subseteq W_1$, comprobamos entonces que $\ker(\tilde{\varphi}_2) \simeq W_1/\varphi_1(V_1)$.

Por último, el lema de la serpiente nos daría el resultado que buscamos si vemos que $\operatorname{coker}(\tilde{\varphi}_2) = 0$. Esto se tiene por el teorema de rango-nulidad ya que

$$\dim(V_2/V_1) = \dim(\operatorname{Im}(\tilde{\varphi}_2)) + \dim(W_1/\varphi_1(V_1))$$

luego obtenemos que $\dim(\operatorname{Im}(\tilde{\varphi}_2)) = \dim(V_2) - \dim(W_1) = \dim(W_2) - \dim(W_1)$ por lo que el cociente dado por el $\operatorname{coker}(\tilde{\varphi}_2)$ tiene dimensión cero.

Teorema 4.3. *El entero* $\deg(D) - h^0(D) + h^1(D)$ *no depende de la elección del divisor* D.

Demostración. El lema anterior nos dice que, separando la sucesión exacta corta y tomando dimensiones,

$$\dim\left(\ker(\varphi_{E,D})\right) = \deg(D) - \deg(E) - \dim\left(H^0(D)/H^0(E)\right).$$

Por otro lado, como $\varphi_{E,D}$ es sobreyectiva (pues φ_3 lo es y el diagrama es de filas exactas), se tiene que, por álgebra lineal básica:

$$\dim\left(\ker(\varphi_{E,D})\right) = h^1(E) - h^1(D).$$

Estas dos expresiones juntas hacen que si $D \geq E$ se tenga el resultado. Para obtener el teorema completo para cualesquiera divisores D y E, simplemente tomamos otro divisor $M \geq D, E$ y aplicamos el teorema para la desigualdad $M \geq D$ y $M \geq E$ lo que da la igualdad

$$\deg(D) - h^0(D) + h^1(D) = \deg(M) - h^0(M) + h^1(M) = \deg(E) - h^0(E) + h^1(E),$$

y esto finaliza la prueba.

Este sorprendente resultado es de increíble utilidad para estimar la dimensión de $h^0(D)$. Como es lógico, escogeremos para ello en el teorema anterior, un divisor E lo más simple posible para hacer los cálculos. Teniendo esto en mente, la definición de género de una curva es muy natural.

Definición 4.5 (Género de una curva). *Si X es una curva proyectiva sin puntos singulares, el género de la curva g es el entero $h^1(O)$ donde O denota al divisor nulo.*

Corolario 4.1 (Desigualdad de Riemann). Se tiene que para cualquier divisor D:

$$h^0(D) = \deg(D) - g + 1 + h^1(D)$$

En particular, $h^0(D) \geq \deg(D) - g + 1$.

Demostración. El teorema 4.3 aplicado a D y O nos da que:

$$h^0(D) + h^1(D) - \deg(D) = h^0(O) + h^1(O) - \deg(O).$$

Usando que $\deg(O) = 0$, que $h^0(O) = 1$ (las funciones constantes son las únicas que están en este espacio) y que $h^1(O) = g$ se sigue el resultado.

4.3 El teorema de Riemann-Roch. Dualidad en códigos de Goppa.

El teorema de Riemann-Roch es uno de los resultados más potentes de la teoría de divisores para curvas algebraicas. De él pueden deducirse resultados fundamentales para otros campos como que toda curva elíptica puede escribirse en forma de Weierstrass o incluso la cota de Hasse-Weil (teorema 3.2) aunque esta segunda demostración no fue la que originalmente de propuso y se tardaron varios años hasta que se encontró una demostración más elegante que involucraba el teorema de Riemann-Roch[3]. La teoría de códigos no escapa a ser influenciada por este teorema pues permite conectar los códigos algebraico-geométricos con sus duales demostrando que el dual de un código Goppa vuelve a ser un código Goppa para otra elección de divisores.

No seremos capaces de proporcionar las herramientas necesarias para demostrar este profundo teorema. Aún así, una prueba que sigue los pasos que hemos dado hasta ahora puede encontrarse en [1] donde se demuestra el teorema de una manera puramente algebraica, sin tener que pasar por el espacio de las formas diferenciales como precisaba la prueba original. Sin más dilación, pasemos a ver el enunciado del teorema.

[3]La cota de Hasse-Weil se deduce de la que se conoce como la hipótesis de Riemann para curvas algebraicas, una de las conjeturas de Weil sobre funciones Zeta para curvas que fue la única, en su momento, que parecía no deducirse de forma directa del teorema de Riemman-Roch.

En la sección anterior, vimos que $H^1(D)$ era un espacio vectorial de dimensión finita. Nos interesa comprobar si podemos entender este espacio a través de un espacio de funciones del tipo H^0 independientemente del divisor escogido. Sorprendentemente, la respuesta es afirmativa y es precisamente sobre esto sobre lo que habla el teorema de Riemman-Roch.

Teorema 4.4 (Teorema de Riemman-Roch). *Sea X una curva proyectiva sin puntos singulares sobre un cuerpo k. Entonces existe un divisor $K \in Div(X)$ tal que para cualquier $D \in Div(X)$, el espacio $H^1(D)$*[4] *es isomorfo de manera natural al espacio $H^0(K - D)$. En particular, $h^1(D) = h^0(K - D)$ y, utilizando la fórmula que relaciona $h^1(D)$ con $h^0(D)$ y g de la sección anterior, se tiene que:*

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

Demostración. Puede encontrarse en [1]. ∎

Definición 4.6. *A cualquier divisor K verificando el teorema anterior se le llama un divisor de clase canónica.*

Tomemos un momento para comprobar la fuerza de este teorema viendo alguna de sus consecuencias inmediatas.

Corolario 4.2. Se tiene que:

$$h^0(K) = g, \qquad h^1(K) = 1, \qquad \deg(K) = 2g - 2.$$

Demostración. Basta utilizar el teorema de Riemman-Roch con $D = O$, $D = K$ y sustituir $D = K$ en la fórmula $h^0(D) = \deg(D) + 1 - g + h^0(K - D)$ respectivamente para cada expresión. ∎

Corolario 4.3 (Segunda parte de la desigualdad de Riemman). Si $\deg(D) \geq 2g - 1$, entonces $h^0(D) = \deg(D) + 1 - g$, es decir, la desigualdad de Riemman de da con igualdad.

Demostración. Basta sustituir en la fórmula dada por el teorema de Riemman-Roch y tener en cuenta que $h^1(D) = h^0(K - D)$ pero $\deg(K - D) < 0$ según el corolario anterior luego $h^0(K - D) = 0$. ∎

Este corolario es de suma importancia ya que nos dice que si tomamos un divisor de grado lo suficientemente alto, los espacios $H^0(D)$ se hacen "regulares" en el sentido de que su dimensión no depende del divisor concreto que tomemos sino solo de

[4] Si V es un espacio de dimensión finita, V^* denota su dual, esto es, el espacio de los homomorfismo de V en su cuerpo base.

su grado. Este resultado es de inmensa utilidad por tanto para calcular por ejemplo, géneros de curvas ya que basta con que seamos capaces de encontrar familias de divisores de grados altos para los cuales sepamos calcular explícitamente $h^0(D)$ lo cual nos permitirá despejar de la expresión dada por Riemman-Roch el género. Veamos una aplicación en este corolario.

Corolario 4.4. La recta proyectiva es de género 0.

Demostración. Vimos en el ejemplo 2.5 que si tomamos $D = n(0 : 1)$, se tiene que $h^0(D) = n + 1$ luego si tomamos n lo suficientemente grande se tiene que $h^0(D) = n + 1 - g$ luego $g = 0$.

La misma idea es la que se utiliza para otro gran teorema fundamental de esta disciplina.

Teorema 4.5 (Fórmula de Plücker). *Si $F \in k[x_0, x_1, x_2]$ es un polinomio totalmente irreducible de grado d y $X = \mathcal{V}(f)$, el género de X es $(d-1)(d-2)/2$.*

Demostración. La prueba se basa en construir una familia de divisores de grado arbitrariamente alto y calcular sus espacios de funciones H^0 explícitamente. Así, el resultado puede deducirse del corolario 4.3. La prueba puede encontrarse con detalle en [1].

Hablemos por último un poco de los divisores de clase canónica. Como sabemos, el número $h^0(D)$ solo depende de la clase de equivalencia de D luego cualquier divisor equivalente a uno de clase canónica es otro divisor de clase canónica (Este es el motivo por el que se le dice *clase* canónica). Podemos caracterizar muy fácilmente a esta clase de equivalencia.

Corolario 4.5. Si D es un divisor que verifica que $\deg(D) = 2g - 2$ y $h^0(D) = g$, entonces D es un divisor de clase canónica.

Demostración. Sea K un divisor de clase canónica. Vamos a ver que D es equivalente a K. El teorema de Riemman-Roch aplicado a D nos da:

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

Como $h^0(K - D) = 1$ (ya que $K - D$ es de grado 0), existe un $f \in \mathcal{K}(D)$ con $(f) + K - D \geq 0$. Tomando grados, vemos que $\deg((f) + K - D) = 0$ luego necesariamente $(f) + K - D = O$ y por tanto $D = K + (f)$ por lo que D y K son equivalentes.

Una vez visto cómo funciona el teorema de Riemman-Roch, veamos qué consecuencia arroja sobre los códigos algebraico-geométricos y demos una explicación a porqué a los códigos de Goppa clásicos se les da dicho nombre.

Teorema 4.6 (Dualidad en códigos de Goppa). *Sea $C(D,G)$ un código de Goppa. Si denotamos por $C(D,G)^\perp$ su código dual como en 4.1, entonces:*

$$C(D,G)^\perp = C(D, K+D-G),$$

donde K es un divisor de clase canónica.

Demostración. Recordemos que si $C(D,G)$ es un código algebraico-geométrico, su dimensión viene dada por $k = h^0(G) - h^0(G-D)$ luego el código $C(D,K+D-G)$ tendrá dimensión $k' = h^0(K-(G-D)) - h^0(K-G)$. Por tanto, por el teorema de Riemman-Roch, si sumamos estas dos cantidades obtenemos que:

$$\begin{aligned} k+k' &= h^0(G) - h^0(K-G) - (h^0(G-D) - h^0(K-(G-D))) \\ &= g - 1 - \deg(G-D) - (g-1-\deg(G)) \\ &= \deg(G-D) + \deg(G) = \deg(D) = n \end{aligned}$$

Luego las dimensiones son adecuadas. Por otro lado, si $f \in H^0(G)$ y $g \in H^0(K+D-G)$, su producto $fg \in H^0(K+D)$. Algunos resultados extras y un poco más de trabajo prueba que al sumar sobre todos los puntos de evaluación obtenemos cero probando que el código es el ortogonal. La prueba completa puede verse en [9]. ∎

Ejemplo 4.1 (Códigos de Goppa clásicos). Terminemos la sección viendo los códigos de Goppa clásicos como un códigos algebraico-geométricos utlilizando el teorema anterior. Al igual que dijimos de forma vaga en la sección 3.2, tomaremos Z como el divisor de ceros de una función $g(x) \in \mathbb{F}_{q^m}[x]$ en la curva $X = \mathbb{P}^1$ que será la recta proyectiva. Tomando $Q = (1:0)$, $P_i = (\gamma_i : 1)$ de manera que g no se anula en nigún γ_i y $D = P_0 + \ldots + P_{n-1}$, vamos a ver que el código de Goppa clásico $\Gamma(L,g)$ (donde $L = \{\gamma_0, \ldots, \gamma_{n-1}\}$) es el espacio $C(D, Z-Q)^\perp$ lo que, en virtud del teorema anterior, probará que $\Gamma(L,g)$ es el código algebraico geométrico $C(D, K+D-Z+Q)$.

Para ello, observamos que $h^0(Z-Q) = \deg(Z) - \deg(Q) = \deg(Z) - 1$ ya que la desigualdad de Riemman se da con igualdad por estar en una curva de género cero. Por tanto, un conjunto generador de $H^0(Z-Q)$ serían las funciones de la forma $x_1/(x_0 - \zeta_j)$ donde los ζ_j son los ceros de g. Por ende, una palabra $(c_0, \ldots, c_{n-1})$ está en $\Gamma(L,g)$ si y solo si

$$\sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} \equiv 0 \mod g,$$

lo cual es equivalente a decir que dicho polinomio se anula en todos los ceros de g pero observamos que eso es equivalente a decir que un elemento de $C(D, Z-Q)$ por $(c_0, \dots, c_{n-1})$ sea cero lo cual prueba que $\Gamma(L,g) = C(D, Z-Q)^{\perp}$ y por tanto prueba que $\Gamma(L,g)$ es un código algebraico-geométrico sobre la recta proyectiva con divisor $G = K + D - Z + Q$.

4.4 Descripción de $\mathrm{Gal}(\overline{k}/k)$

Basándonos en la teoría básica de cuerpos finitos, pasamos a describir la estructura del grupo absoluto de Galois sobre uno de estos cuerpos. Para ello, asumiremos todos los resultados de Teoría de Códigos y Criptografía y ACGA.

Recordemos que si $k = \mathbb{F}_{p^r}$ es un cuerpo finito de característica $p > 0$, entonces su clausura algebraica

$$\overline{k} = \bigcup_{s=1}^{\infty} \mathbb{F}_{q^s}$$

es la unión de todos los cuerpos finitos de característica p.

Lema 4.4. Si $q = p^r$ con p un primo, todo subcuerpo de $\mathbb{F}_q$ tiene cardinal p^s con $s|r$. Recíprocamente, si $s|r$, existe un único subcuerpo de $\mathbb{F}_q$ con p^s elementos.

Demostración. Que todo subcuerpo contenido en $\mathbb{F}_{p^r}$ tiene p^s elementos con $s|r$ es evidente ya que $\mathbb{F}_{p^r}$ tendrá estructura de espacio vectorial sobre ese cuerpo.

Recíprocamente, si $s|r$, es fácil comprobar que $(p^s - 1)|(p^r - 1)$ por lo que

$$\left(x^{p^s-1} - 1\right) \mid \left(x^{p^r-1} - 1\right)$$

lo que implica que $\left(x^{p^s} - x\right)|\left(x^{p^r} - x\right)$. Como los polinomios de la forma $x^q - x$ factorizan completamente en $\mathbb{F}_q$, vemos que las raíces de $x^{p^s} - x$ forman un cuerpo de p^s elementos.

Para ver la unicidad, basta usar que todo elemento de $\mathbb{F}_q$ es raíz de $x^q - x$ luego si hubiese dos cuerpos de p^s elementos, todos los elementos de la unión deberían ser raíces de $x^{p^s} - x$ pero este polinomio solo puede tener p^s raíces. ∎

Sea $\mathbb{F}_{q^m}$ el cuerpo finito de q^m elementos. Por el lema anterior, $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$. Sea ahora $\alpha \in \mathbb{F}_{q^m}^*$ y consideremos su polinomio irreducible $f(x)$ sobre $\mathbb{F}_q$. Si $\mathbb{F}_{q^r} = \mathbb{F}_q[\alpha]$ es

el cuerpo más pequeño que contiene a α, entonces f es de grado r y podemos ver $\mathbb{F}_q \subseteq \mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^m}$. Entonces se tiene que:

Lema 4.5. En las condiciones anteriores, las raíces de f son $\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}$ y todas son distintas entre sí. Por tanto, el grupo de Galois de cualquier extensión $\mathbb{F}_q \subseteq \mathbb{F}_{q^r}$ es isomorfo a $\mathbb{Z}/\mathbb{Z}r$.

Demostración. Recordemos que en $\mathbb{F}_q$, $a^q = a \quad \forall a \in \mathbb{F}_q$ y que $(a+b)^p = a^p + b^p$. Por tanto, si $f(x) = a_0 + a_1 x + \ldots + a_{r-1}x^{r-1} + x^r$ con $a_i \in \mathbb{F}_q$, se tiene que

$$f(x^q) = a_0 + \ldots + a_{r-1}x^{q(r-1)} + x^{qr} = (a_0 + \ldots + a_{r-1}x^{r-1} + x^r)^q = f(x)^q$$

luego todos los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}$ son raíces de f. Por otro lado, si existiesen i, j tales que $\alpha^{q^i} = \alpha^{q^j}$, entonces $\alpha^{q^{j-i}} = 1$ lo que nos daría un polinomio de grado menor que r para α lo cual no puede pasar porque f es su polinomio mínimo. ∎

Corolario 4.6. El grupo de Galois de la extensión $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ es cíclico de orden m y está generado por el automorfismo de Frobenius

$$\begin{array}{rccc} \phi : & \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ & x & \mapsto & \phi(x) = x^q \end{array}$$

Proposición 4.2 (Estructura de $\mathrm{Gal}(\overline{k}/k)$). Si $k = \mathbb{F}_q$ es un cuerpo finito, entonces $\mathrm{Gal}(\overline{k}/k)$ es isomorfo al grupo de los enteros profinitos, esto es, el conjunto de sucesiones $\{a_n\}_{n\in\mathbb{N}}$ de manera que $a_n \in \mathbb{Z}/\mathbb{Z}n$ para todo n y si $m|n$, $a_m \equiv a_n \bmod m$ con la operación de sumar componente a componente.

Demostración. Si $\sigma \in \mathrm{Gal}(\overline{k}/k)$, su restricción a cualquier cuerpo $\mathbb{F}_{q^n}$ es alguna potencia del automorfismo de Frobenius ϕ, esto es, $\sigma = \phi^{a_n}$ restringiendo σ a $\mathbb{F}_{q^n}$ para algún $0 \leq a_n < n$. Como $\overline{\mathbb{F}_q}$ es la unión de todas las extensiones de $\mathbb{F}_q$, σ queda unívocamente determinado por estos números a_n. Además, por el lema 4.4, si $m|n$, se tiene que $\mathbb{F}_m \subseteq \mathbb{F}_n$ y por tanto las correspondientes potencias del automorfismo de Frobenius deben coincidir, esto es, $a_m \equiv a_n \bmod m$. Se puede comprobar que la composición de automorfismos se corresponde con la suma componente a componente de estas sucesiones lo que concluye la prueba. ∎

Bibliografía

[1] Lorenzini, Dino: *An invitation to arithmetic geometry*. American Mathematical Society (1996).

[2] MacWilliams, F. J., Sloane, N. J. A., & Goethals, J. M. (1972). *The MacWilliams identities for nonlinear codes*. Bell System Technical Journal, 51(4), 803-819.

[3] Munuera, Carlos; Tena, Juan: *Codificación de la Información*. Universidad de Valladolid (1997).

[4] Peterson, William W.; Weldon, Jr. Edward J.: *Error-correcting codes*. MIT Press (1972).

[5] Singh, Harshdeep: *Code based Cryptography: Classic McEliece*. arXiv preprint arXiv:1907.12754.

[6] Stichtenoth, Henning: *Algebraic function fields and codes*. Springer (2009).

[7] Tsfasman, Michael A.; Vlăduţ, Serge G.; Nogin, Dmitry: *Algebraic Geometric Codes: Basic Notions: Basic Notions*. American Mathematical Society (2007).

[8] Tsfasman, Michael A.; Vlăduţ, Serge G.; Zink, Thomas: *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*. Mathematische Nachrichten **109** (1) 21–28.

[9] Van Lint, Jacobus H.; van der Geer, Gerard: *Introduction to coding theory and algebraic geometry*. Birkhäuser (2012).