UNIVERSIDAD NACIONAL DEL LITORAL
FACULTAD DE INGENIERÍA QUÍMICA

Tesis presentada como parte de los requisitos de la
Universidad Nacional del Litoral
para la obtención del Grado Académico de

Doctor en Matemática

En el campo de: **Teoría de Códigos**

Título de la tesis:

Estudio de códigos algebraico-geométricos cíclicos

Instituciones donde se realizó:
Instituto de Matemática Aplicada del Litoral (CONICET-UNL)
Departamento de Matemática - FIQ (UNL)

Autor:

Gustavo Andrés Cabaña

Director de Tesis: Dr. Ricardo Toledano

Codirector de Tesis: Dr. Ricardo Podestá

Jurado de Tesis

Dr. Cícero Carvalho Dr. Guillermo Matera Dra. Luciane Quoos

Año de presentación: 2022

A Alcides, Coco, Daysi,
Dora, Ernesto y Gordo.

Agradecimientos

Quiero agradecer de corazón a todas las personas e instituciones que hicieron posible, directa e indirectamente, la concreción de esta tesis. Partiendo del Jardín de Infantes número 98 Dr. Esteban Maradona, la Escuela número 316 Guillermo Lehmann y la Escuela Normal número 30 Domingo Sarmiento, por haberme brindado educación pública de calidad, y especialmente a las docentes de matemáticas que tuve, que siempre enseñaron con amor y cariño esos temas que a veces son los menos queridos.

A Almagro, que fue mucho más que un club para mi durante muchos años. Ahí aprendí a jugar al basquet y a nadar, pero también aprendí una gran cantidad de valores positivos que rodean al deporte. Aprendí a tratar con mis compañeros, entrenadores, utileros, dirigentes, y además aprendí que son muchas las piezas que deben funcionar de manera perfecta para que un plan funcione.

A la Universidad Nacional del Litoral, la Facultad de Ciencias Económicas y la Facultad de Ingeniería Química, que fueron fundamentales para mi formación como Licenciado y como docente, y que luego lo siguieron siendo durante los años de este Doctorado. También gracias al CONICET, cuyo aporte económico fue vital para poder destinar mucho tiempo exclusivamente a estudiar.

Gracias al IMAL (Instituto de Matemática Aplicada del Litoral) y al Departamento de Matemáticas de FIQ, por brindarme lugares de trabajo con todas las comodidades necesarias, y por ser fundamentales para la formación matemática en Santa Fe.

Gracias infinitas a Galindez, Lunático Sr. Yamaguchi, Simón Fuga, Bajofondo, Color Humano, Almendra, Pescado Rabioso, Alejandro Sanz, Kevin Johansen, The Nada, Zambayonny, Púrpura, y todas las bandas musicales que me han acompañado y me acompañan día a día. Y hablando de contenido sonoro, gracias a todos los podcasts y a las personas responsables de que existan, como Gerry con Aprender de Grandes, Max con Desde Lejos, Fierita con No Es Nada y todo el equipo de Ciencia del Fin del Mundo.

Gracias a todas las personas que compartieron conmigo su sabiduría matemática desde 2010 en adelante, siendo docentes en los cursos que he ido tomando: Pola, Néstor, Ingrid, Negro, Ivana, Richie, Marta, Fernanda, Rober, Eleonora, Gladis, Rubén, Claudia, Hugo,

Marce, Andre, La Jose, Carlos, Edu, Maikel, Pedro, Marisa, Gabi, Laura, Pío, Estefi, Goro, Marilina, Manu, Conrad y Nora.

Gracias a todas las personas con las cuales compartí equipos docentes y a todas las personas que tomaron algún curso dado por mi, han transformado mi vida de una manera que es difícil dimensionar, y me han permitido (y me siguen permitiendo) ejercer la pasión de la docencia.

Gracias a Clau, que comparte su vida conmigo desde 2009, y ha sido el soporte principal cuando cambié de carrera de CPN a LMA, cuando decidí hacer un doctorado, y cada vez que quería abandonar me daba fuerzas para seguir. Gracias por acompañar mi vida académica y por el proyecto de vida en común más allá de lo laboral.

Gracias a Mami, Papi, Guille, Evi y Belu, por todos los momentos compartidos, los recuerdos de la infancia, el apoyo constante, y soportarme desde que nací (o desde que nacieron, según corresponda).

Gracias a todas las amistades que me dió la matemática, y especialmente a Estefi, Flor, La Jose, Maikel, Mariel y Marilina, que no solamente me han brindado su amistad y cariño, sino que me han ayudado con consejos, correcciones de escritura, charlas de todo tipo y compañía en silencio cuando era necesario. También a Fede, por haberme abierto la puerta de su casa, por todos los momentos compartidos y por ser una persona siempre amable y generosa.

Gracias a María, amiga y firme compañera de batallas matemáticas desde 2012, con quien compartimos muchas charlas, horas de trabajo, congresos, frustraciones y felicidades. Espero que sigamos aprendiendo, pensando, y compartiendo muchos momentos dentro y fuera del trabajo.

Gracias a mis directores Richie y Richar por haberme permitido aprender el oficio de la investigación, acercarme temas que seguramente no hubiera conocido de otra manera y animarme a no darme por vencido en los momentos más complicados. Gracias también a Cícero, Guillermo y Luciane por leer y evaluar este trabajo, y por los comentarios constructivos que me hicieron acerca de la tesis.

Gracias a todas las personas que no he nombrado pero igualmente fueron y son importantes para mi. Si estás leyendo esto, gracias.

Índice general

Resumen

La presente tesis se enmarca dentro de la teoría de códigos, más precisamente estudiamos códigos algebraico-geométricos cíclicos y logramos avances originales significativos para comprender propiedades estructurales de estos códigos, especialmente dentro de los códigos algebraico-geométricos racionales.

Usando como base el lenguaje de cuerpos de funciones desarrollado en el libro *Algebraic Function Fields and Codes*, de Henning Stichtenoth [16], que es bibliografía de referencia en el área (ver también [10,17,19]), iniciamos el estudio de códigos algebraico-geométricos cíclicos y brindamos respuestas a los siguientes problemas:

- Construir códigos algebraico-geométricos cíclicos.
- Clasificar códigos algebraico-geométricos cíclicos racionales, según la equivalencia monomial.

Primero nos centramos en entender la estructura de los códigos algebraico-geométricos cíclicos en el contexto de cuerpos de funciones algebraicas sobre cuerpos finitos, $F/\mathbb{F}_q$, y luego tuvimos la necesidad de encontrar un método para construir tales códigos. En el caso general, pudimos hacerlo mediante el uso del grupo de automorfismos $\mathrm{Aut}_{\mathbb{F}_q}(F)$. Para ello, diseñamos un método, al cual llamamos método sigma, que nos permite construir tales códigos, y desarrollamos ejemplos de aplicación del método. Denominamos como códigos sigma-cíclicos a los códigos obtenidos con el método sigma. Un artículo importante relacionado al análisis de automorfismos de códigos es [14].

Además de considerar dichas construcciones en cuerpos de funciones, desarrollamos resultados y ejemplos de códigos algebraico-geométricos cíclicos construidos en extensio-

nes F'/F de cuerpos de funciones, lo que puede ser de suma importancia al momento de intentar construir sucesiones de códigos cíclicos, como puede verse en [3, 15, 18].

También presentamos otra manera de hallar códigos cíclicos, en este caso racionales, usando polinomios interpoladores de Lagrange, siguiendo el espíritu mostrado en [6]. Esto dió origen a los códigos L-cíclicos y nos condujo a analizar la relación que puede existir entre códigos sigma-cíclicos y códigos L-cíclicos sobre cuerpos de funciones racionales.

Después de dar respuesta al problema de construcción de códigos algebraico-geométricos cíclicos, nos enfocamos en estudiar la equivalencia monomial en el caso de códigos sigma-cíclicos racionales, siguiendo la idea de López y Nart dada en [9].

En su trabajo, López y Nart estudian los denominados códigos de Reed-Solomon Generalizados, o simplemente códigos RSG, y logran realizar una clasificación según clases de equivalencia de tales códigos. Este trabajo nos motivó a intentar realizar tal clasificación considerando la familia de códigos cíclicos. El problema de identificar códigos cíclicos equivalentes fue tratado también en, por ejemplo, los artículos [1, 5], mientras que en [12] se estudia, no la equivalencia, sino la igualdad de códigos en el caso general.

Con respecto al problema de la equivalencia, consideramos códigos sigma-cíclicos racionales $\mathcal{C}_{\mathcal{L}}(D, G)$, con divisores G de un solo punto, es decir, $G = rP$ para un lugar P y un número natural r. Si P es un lugar racional cualquiera, probamos que existe un único código sigma-cíclico, salvo equivalencias, para cada longitud y dimensión fijas. Si P no es racional, en algunos casos pudimos reducir el problema a lo ya demostrado y, en otros, realizamos experimentos computacionales para obtener información al respecto.

Parte de lo desarrollado en esta tesis se encuentra publicado en la revista *Finite Fields and Their Applications* [2].

Introducción

Motivación

Puede decirse que la teoría clásica de códigos comienza en 1948 con el trabajo [13] de Shannon, donde se muestra que a todo canal de comunicación con ruido se le puede asignar un número, llamado capacidad del canal, y que ésta se relaciona con el tipo de herramientas que se pueden usar para evitar transmitir mensajes erróneos. A partir de este trabajo, se comenzaron a desarrollar fundamentos matemáticos que luego serían la base de las implementaciones prácticas que permitieron, efectivamente, colaborar en la detección y corrección de errores en la transmisión de información.

Dentro de los códigos usados en la industria, adquirieron una gran relevancia ciertas clases particulares de códigos cíclicos, como los códigos de Reed-Solomon y los códigos BCH, debido a sus capacidades de corrección y a la sencillez de su implementación.

En 1981, Manin muestra en [11] que existe una función α_q que involucra a los denominados parámetros relativos y que brinda información de suma importancia respecto a los códigos que se obtienen a partir de usar como alfabeto al cuerpo finito con q elementos, $\mathbb{F}_q$. Sin embargo α_q resulta ser una función que no podemos explicitar.

Dentro de la teoría clásica de códigos fue posible obtener ciertas cotas inferiores y superiores para α_q. Pero, sin dudas, la cota más importante proviene del trabajo [18] de Tsfasman, Vlăduţ y Zink, que requiere de la utilización de los denominados códigos algebraico-geométricos, construidos dentro del contexto de cuerpos de funciones o de curvas algebraicas, motivo por el cual los códigos algebraico-geométricos adquieren gran popularidad.

Así, es de gran interés estudiar códigos algebraico-geométricos cíclicos, para combinar todas las bondades de los códigos cíclicos con las de los códigos algebraico-geométricos.

Objeto de estudio, problemas y antecedentes

El objeto de estudio de esta tesis está formado por los códigos algebraico-geométricos cíclicos. Estamos interesados en entender su estructura y en sistematizar formas de identificarlos o construirlos.

La definición clásica de código de bloque sobre un cuerpo finito $\mathbb{F}_q$ indica que un código $\mathcal{C}$ de longitud n es un subespacio vectorial de $\mathbb{F}_q^n$. Decimos que $\mathcal{C}$ es cíclico si es cerrado por permutaciones cíclicas de sus coordenadas, es decir, si $(c_1, c_2, c_3, \ldots, c_n) \in \mathcal{C}$, entonces debe suceder que $(c_2, c_3, \ldots, c_n, c_1) \in \mathcal{C}$.

Dentro de la teoría clásica de códigos, construir códigos cíclicos de longitud n sobre $\mathbb{F}_q$ consiste simplemente en considerar un polinomio mónico g que divida a $x^n - 1$, y usar el ideal $\langle g \rangle$ del anillo $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ para obtener el código cíclico

$$\mathcal{C} = \left\{ (c_0, c_1, c_2, \ldots, c_{n-1}) \ : \ c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \langle g \rangle \right\}.$$

En nuestro caso, usamos la teoría de cuerpos de funciones para construir códigos

$$\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) = \{ (z(P_1), z(P_2), \ldots, z(P_n)) \ : \ z \in \mathcal{L}(G) \},$$

donde D y G son divisores con soportes disjuntos tales que $D = P_1 + P_2 + \cdots + P_n$ está formado por n lugares racionales distintos, y $\mathcal{L}(G)$ es el espacio de Riemann-Roch asociado al divisor G dado por

$$\mathcal{L}(G) = \{ z \in F \ : \ (z) + G \geq 0 \} \cup \{0\}.$$

En este contexto, $\mathcal{C}$ es cíclico si y solo si

$$(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) \in \mathcal{C} \quad \forall \ (u(P_1), \ldots, u(P_n)) \in \mathcal{C}.$$

Luego, $(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) \in \mathcal{C}$ si y solo si existe $v \in \mathcal{L}(G)$ tal que

$$(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) = (v(P_1), v(P_2), \ldots, v(P_{n-1}), v(P_n)).$$

Así, podemos determinar que $\mathcal{C}$ es cíclico si para cada $u \in \mathcal{L}(G)$ hallamos un elemento $v \in \mathcal{L}(G)$, que satisfaga el siguiente sistema:

$$\begin{cases} v(P_1) &= u(P_2), \\ v(P_2) &= u(P_3), \\ &\vdots \\ v(P_{n-1}) &= u(P_n), \\ v(P_n) &= u(P_1). \end{cases} \tag{1}$$

Luego, el problema de construir códigos cíclicos queda reducido a determinar cómo y cuándo podemos encontrar, para cada $u \in \mathcal{L}(G)$, un elemento $v \in \mathcal{L}(G)$ satisfaciendo (1).

Respecto a este problema, una manera de resolverlo consiste en trabajar con el grupo de automorfismos $\mathrm{Aut}_{\mathbb{F}_q}(F)$, como lo haremos a lo largo de casi todo el Capítulo 3 (Secciones 3.1 a 3.4). Otra manera, pero que solo será aplicable al caso de cuerpos de funciones racionales, consiste en utilizar polinomios interpoladores de Lagrange (Sección 3.5).

Una vez resuelto el problema de construir códigos algebraico-geométricos cíclicos, nos interesa determinar cuántos códigos no equivalentes podemos obtener, para lo cual, en esta tesis, consideramos la equivalencia monomial. Este problema es de suma importancia por estar relacionado con el problema de determinar si la familia de códigos cíclicos es asintóticamente buena, lo que aún se encuentra sin respuesta.

Relacionado a este problema de códigos equivalentes pudimos dar respuestas, a lo largo del Capítulo 4, en el contexto de códigos racionales, y con divisores G de un solo punto, es decir, cuyo soporte tiene un solo lugar. En este caso, usamos fuertemente propiedades de los cuerpos de funciones racionales y también que el grupo $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ es isomorfo a $\mathrm{PGL}_2(\mathbb{F}_q)$.

Resumiendo, los dos grandes problemas a los que nos enfrentamos en esta tesis son:

- Construir códigos algebraico-geométricos cíclicos.
- Clasificar códigos algebraico-geométricos cíclicos racionales, según la equivalencia monomial.

Con respecto al problema de construir códigos cíclicos en nuestro contexto de cuerpos de funciones, no hay trabajos previos directamente relacionados. Los trabajos más cercanos

son [15], donde se estudian códigos transitivos y autoduales, y [3], donde se estudian códigos transitivos por bloques.

Lo mismo sucede con el problema de clasificar códigos según clases de equivalencias, pero vale la pena destacar algunos artículos relacionados, donde diferentes autores trabajan con el enfoque clásico de códigos.

En [1] se analiza la equivalencia de códigos cíclicos en base a los polinomios generadores y usando isometrías. También se relacionan códigos cíclicos de longitud n con códigos cíclicos de longitud nm, con un mismo generador g, ya que si g divide a $x^n - 1$, también divide a $x^{nm} - 1$. Además, se tratan los llamados códigos constacíclicos, que surgen de considerar divisores g de $x^n - a$ para $a \in \mathbb{F}_q$ no nulo.

En [5] se estudió la equivalencia de códigos cíclicos de longitudes p^r, donde p es un número primo y r es un número natural. En este caso el enfoque es desde la teoría de grupos, mediante el uso de p-subgrupos de Sylow de los grupos de automorfismos asociados a los códigos que se quieren comparar.

En [9] López y Nart no se enfocan en códigos cíclicos sino que trabajan con códigos racionales en general, considerando solamente divisores $G = rP_\infty$. Deducen que la cantidad de códigos no equivalentes de longitud n se relaciona con el conteo de órbitas de longitud n, y realizan un trabajo combinatorio para obtener los resultados buscados.

En general, ni los trabajos antes mencionados, ni otros trabajos del área, utilizan nuestro enfoque de cuerpos de funciones y nuestra construcción de códigos sigma-cíclicos al momento de intentar determinar equivalencia de códigos cíclicos.

Organización del texto

La tesis se separa en dos partes. Por un lado, encontraremos los **Preliminares** y, por otro, lo que corresponde al **Trabajo original**. En Preliminares brindaremos las bases necesarias de cuerpos de funciones (Capítulo 1) y de códigos algebraico-geométricos (Capítulo 2), mientras que en la segunda parte desarrollaremos el trabajo original que sustenta esta tesis, estudiando por un lado códigos algebraico-geométricos cíclicos en general (Capítulo 3), y códigos algebraico-geométricos cíclicos racionales en particular (Capítulo 4). Para tener en claro la notación y el lenguaje que usaremos en esta tesis,

recomendamos leer la Parte I: Preliminares, aún si la persona que lee está familiarizada con el tema, para poder tener una lectura lo más fluida posible de la Parte II: Trabajo original.

En el Capítulo 1 agruparemos las definiciones y resultados fundamentales para trabajar con cuerpos de funciones algebraicas. Particularmente, en la Sección 1.2 presentaremos los cuerpos de funciones racionales que serán de suma importancia a lo largo de todo el Capítulo 4. También definiremos los divisores de un cuerpo de funciones que se necesitan, por ejemplo, para definir los espacios de Riemann-Roch, y enunciaremos el Teorema de Riemann-Roch y varias consecuencias importantes del mismo.

En el Capítulo 2 describiremos brevemente las definiciones básicas de la teoría clásica de códigos, para después adentrarnos en los códigos algebraico-geométricos en general, pero también en los códigos algebraico-geométricos racionales en particular.

En el Capítulo 3 realizamos un análisis pormenorizado de los códigos algebraico-geométricos cíclicos que pueden construirse mediante automorfimos, a los cuales denominamos códigos sigma-cíclicos, y desarrollamos el método sigma que nos permite construir tales códigos. En relación a esta construcción, el Lema 3.1.5 sustenta al método sigma. Luego presentamos varios ejemplos de códigos sigma-cíclicos, tanto sobre cuerpos de funciones racionales como no racionales. Seguidamente, exponemos relaciones entre códigos sigma-cíclicos y extensiones cíclicas de cuerpos en la Sección 3.4. Los resultados más importantes de esta sección son la Proposición 3.4.1, el Corolario 3.4.4, y el Teorema 3.4.6. Finalizamos el capítulo con una construcción alternativa, que nos permite incluso pensar la ciclicidad en códigos más generales que los códigos algebraico-geométricos.

En la Sección 3.1 analizamos las propiedades estructurales de los códigos AG cíclicos y mostramos cómo podemos construirlos mediante el uso de automorfismos de $\mathrm{Aut}_{\mathbb{F}_q}(F)$, dando lugar a los denominados códigos sigma-cíclicos, basados en los Lemas 3.1.3 y 3.1.5. Esto da lugar a la Sección 3.2, donde esquematizamos el método sigma, que usaremos sistemáticamente para construir códigos sigma-cíclicos.

En la Sección 3.3 brindamos una serie de ejemplos, algunos con un enfoque general como en el Lema 3.3.1, y otros más específicos, donde construimos códigos usando raíces

de la unidad (Ejemplo 3.3.2), o polinomios de Artin-Schreier (Ejemplo 3.3.3), o un cuerpo de funciones hermitiano (Ejemplo 3.3.4).

En la Sección 3.4 procedemos a estudiar y aplicar nuestro método al caso de extensiones de cuerpos de funciones, y vemos que los códigos cíclicos están fuertemente ligados con extensiones de Galois cíclicas, como puede apreciarse en la Proposición 3.4.1 y en el Teorema 3.4.6. Además, presentamos ejemplos sobre extensiones de Kummer (Ejemplo 3.4.2) y extensiones de Artin-Schreier (Ejemplo 3.4.3).

En la Sección 3.5 dejamos por un momento de lado los automorfismos, y presentamos una construcción alternativa en el caso de cuerpos de funciones racionales, que nos permite en ciertas ocasiones determinar ciclicidad, dando lugar a los llamados códigos L-cíclicos. Mostramos condiciones para que un código sea sigma-cíclico y L-cíclico, pero también vemos que un código puede ser L-cíclico sin que haya automorfismo alguno involucrado.

En el Capítulo 4 nos enfocamos en el problema principal de esta tesis, que es el de clasificar según clases de equivalencia a los códigos sigma-cíclicos racionales, construidos a partir de cuerpos de funciones, y determinar, cuando sea posible, cuántos códigos no equivalentes existen. Nos motiva a estudiar este problema el trabajo [9], en el cual se realiza un análisis relacionado a la cantidad de órbitas que existen de una longitud dada, considerando la acción del grupo $\mathrm{PGL}_2(\mathbb{F}_q)$ sobre el conjunto $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$. Sin embargo, no todos los códigos que se consideran en [9] son cíclicos. Así, al concentrarnos en esta tesis en códigos cíclicos, logramos probar resultados que no son posibles en el caso general.

En la Sección 4.1 analizamos códigos construidos a partir de automorfismos, no solamente describiendo tales códigos sino también dando formas explícitas para construirlos. Usando que $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ es isomorfo a $\mathrm{PGL}_2(\mathbb{F}_q)$ y considerando la acción de $\mathrm{PGL}_2(\mathbb{F}_q)$ sobre $\mathbb{P}^1(\mathbb{F}_q)$, probamos que las órbitas generadas por esta acción nos permiten construir códigos cíclicos. También caracterizamos los automorfismos que fijan el lugar en el infinito, que resulta ser fundamental para las siguientes secciones.

En la Sección 4.2 brindamos una clasificación de los códigos abordados en la sección anterior, en cuanto a equivalencia de códigos, y demostramos que, salvo equivalencias, existe un único código sigma-cíclico, fijadas la longitud y la dimensión. Más precisamente,

estudiamos códigos de la forma $\mathcal{C}_{\mathcal{L}}(D, G)$ con $G = rP_\beta$, para algún $\beta \in \mathbb{P}^1(\mathbb{F}_q)$. En primer lugar, probamos algunos resultados técnicos junto con las Proposiciones 4.2.2 y 4.2.6, que nos permitieron reducir el problema a considerar $\beta = \infty$, ya que cualquier código de la forma $\mathcal{C}_{\mathcal{L}}(D, rP_\beta)$ con $\beta \neq \infty$, puede escribirse como $\mathcal{C}_{\mathcal{L}}(D', rP_\infty)$, eligiendo D' adecuadamente.

Como caracterizamos las matrices de $\mathrm{PGL}_2(\mathbb{F}_q)$ que fijan a P_∞, podemos usar esas matrices para determinar las longitudes posibles de los códigos. Así, fijada la longitud, solo resta comparar los posibles códigos que pueden construirse. En algunos casos encontramos que, fijadas la longitud y la dimensión, todos los códigos son iguales, y en otros casos encontramos que todos son equivalentes. Este desarrollo se plasma en el Teorema 4.2.12, que es consecuencia de las Proposiciones 4.2.3, 4.2.6 y 4.2.11.

Finalmente, en la Sección 4.3 estudiamos el caso de códigos sigma-cíclicos construidos con divisores G que no sean racionales. En algunos casos, podemos reducir el problema a lo expuesto en las secciones anteriores, pero hay situaciones que no pueden contemplarse en el análisis previo. Así, desarrollamos ejemplos computacionales para dar alguna respuesta parcial acerca de las alternativas que quedan fuera de nuestro desarrollo teórico.

Como hacemos notar al comienzo de dicha sección, si trabajamos con algún automorfismo que fija algún lugar racional, digamos P_β, entonces para cualquier lugar Q no racional que también quede fijo tenemos que los divisores Q y $(\deg Q)P$ son equivalentes, y los códigos asociados también lo son. Así, solamente nos queda por analizar qué sucede si el automorfismo usado para construir códigos mueve todos los lugares racionales.

Si A es la matriz asociada a un automorfismo que no fija lugares racionales, entonces $|A|$ divide a $q+1$. Si resulta que $|A| = q+1$, mostramos en la Proposición 4.3.3 que todos los códigos de longitud $q+1$, fijada la dimensión, son equivalentes. Llegados a esta situación, resta analizar el caso en que $|A|$ es un divisor propio de $q+1$. En este caso, solamente podemos probar qué sucede en el caso particular de la Proposición 4.3.4, donde vemos que $\mathcal{C}_{\mathcal{L}}(D, G_1) \sim \mathcal{C}_{\mathcal{L}}(D, G_2)$, pero no podemos cambiar arbitrariamente D por D' como sucedía en la sección anterior. Para comprender mejor esto, procedimos a realizar ejemplos computacionales, y encontramos casos donde existen dos códigos sigma-cíclicos no equivalentes.

Parte I

Preliminares

Capítulo 1

Cuerpos de funciones algebraicas

En este capítulo introduciremos las definiciones básicas y los resultados de la teoría de cuerpos de funciones algebraicas. Salvo que se indique lo contrario, las definiciones y los resultados (con sus demostraciones) pueden encontrarse en [16].

A lo largo de este capítulo K será un cuerpo arbitrario.

1.1. Lugares

Definición 1.1.1. Un cuerpo de funciones algebraicas F/K de una variable sobre K es una extensión de cuerpos $F \supset K$ tal que F es una extensión algebraica finita de $K(x)$ para algún elemento $x \in F$ trascendente sobre K.

$$\begin{array}{c} F \\ | \quad < \infty \\ K(x) \\ | \\ K \end{array}$$

Nos referimos a F/K simplemente como cuerpo de funciones.

Como es usual, supondremos que K es el cuerpo total de constantes de F, es decir, que

$$K = \{z \in F \ : \ z \text{ es algebraico sobre } K\}.$$

Observación 1.1.2. Los elementos de F que son trascendentes sobre K pueden caracterizarse así: $z \in F$ es trascendente sobre K si y solo si $F/K(z)$ es una extensión de cuerpos finita, o de grado finito.

Ejemplo 1.1.3. El ejemplo más simple de cuerpos de funciones algebraicas es el cuerpo de funciones racionales $F = K(x)$ para algún elemento x trascendente sobre K. Cada elemento $0 \neq z \in K(x)$ tiene una única representación de la forma

$$z = a \prod_{i=1}^{s} p_i(x)^{n_i}, \tag{1.1}$$

con $0 \neq a \in K$, $p_i \in K[x]$ mónico irreducible para todo i, $p_i \neq p_j$ si $i \neq j$, y $n_i \in \mathbb{Z}$ para todo i. $\Diamond$

Un cuerpo de funciones F/K puede representarse como una extensión de cuerpos algebraica simple de un cuerpo de funciones racionales $K(x)$, es decir, $F = K(x, y)$ donde $\varphi(y) = 0$ para algún polinomio irreducible $\varphi(T) \in K(x)[T]$. Si F/K es un cuerpo de funciones que no es racional no es claro que todo elemento $0 \neq z \in F$ admita una descomposición análoga a (1.1).

A continuación presentamos objetos claves en el contexto de cuerpos de funciones, los anillos de valuación, que se asocian con los conceptos de lugar y valuación discreta.

Definición 1.1.4. Un anillo de valuación de un cuerpo de funciones F/K es un anillo $\mathcal{O} \subset F$ que satisface:

1. $K \subsetneq \mathcal{O} \subsetneq F$.

2. Para todo $z \in F$ resulta que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

La definición anterior está motivada por el caso de un cuerpo de funciones racionales $K(x)$. Dado $p(x) \in K(x)$ un polinomio mónico irreducible, consideramos el conjunto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in K(x),\ p(x) \nmid g(x) \right\}.$$

Es sencillo ver que $\mathcal{O}_{p(x)}$ es un anillo de valuación de $K(x)/K$.

Notar que si $q(x) \in K(x)$ es mónico irreducible distinto de $p(x)$, entonces $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Proposición 1.1.5. *Sea $\mathcal{O}$ un anillo de valuación de F/K. Entonces:*

1. *$\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal $P = \mathcal{O} \backslash \mathcal{O}^*$, donde $\mathcal{O}^*$ es el grupo de unidades de $\mathcal{O}$.*

2. *Sea* $0 \neq z \in F$. *Entonces* $z \in P$ *si y solo si* $z^{-1} \notin \mathcal{O}$.

3. *El cuerpo de constantes* K *satisface que* $K \subset \mathcal{O}$ *y* $K \cap P = \{0\}$.

La importancia de los anillos de valuación se aprecia en el siguiente teorema.

Teorema 1.1.6. *Sean* $\mathcal{O}$ *un anillo de valuación de un cuerpo de funciones* F/K *y* $P \subset \mathcal{O}$ *su único ideal maximal. Entonces:*

1. P *es un ideal principal.*

2. *Si* $P = t\mathcal{O}$ *y* $0 \neq z \in F$, *entonces* z *tiene una única representación de la forma* $z = t^n u$ *para algún* $n \in \mathbb{Z}$ *y algún* $u \in \mathcal{O}^*$.

Definición 1.1.7. Un lugar P del cuerpo de funciones F/K es el ideal maximal de algún anillo de valuación $\mathcal{O}$ de F/K. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ se denomina elemento primo o parámetro local para P. Denotaremos con $\mathbb{P}(F)$ al conjunto de todos los lugares de F/K.

Observación 1.1.8. Si $\mathcal{O}$ es un anillo de valuación de F/K con ideal maximal P, entonces es usual escribir $\mathcal{O}_P$ en lugar de solamente $\mathcal{O}$ pues este anillo está unívocamente determinado por P. En efecto,

$$\mathcal{O}_P = \{z \in F \ : \ z^{-1} \notin P\}.$$

Otra descripción del concepto de lugar puede darse en términos de una valuación discreta.

Definición 1.1.9. Una valuación discreta (o simplemente una valuación) de F/K es una función $\nu : F \to \mathbb{Z} \cup \{\infty\}$ que satisface lo siguiente:

1. $\nu(z) = \infty \Leftrightarrow z = 0$.

2. $\nu(z_1 z_2) = \nu(z_1) + \nu(z_2)$ para todos $z_1, z_2 \in F$.

3. $\nu(z_1 + z_2) \geq \min\{\nu(z_1), \nu(z_2)\}$ para todos $z_1, z_2 \in F$.

4. Existe $u \in F$ tal que $\nu(u) = 1$.

5. $\nu(a) = 0$ para todo $a \in K^*$.

En este contexto, el símbolo ∞ hace referencia a un elemento que no está en $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ y $\infty > m$ para cualesquiera números enteros n y m. Además, de las propiedades 2 y 4 se obtiene que ν es sobreyectiva. Por último, cabe mencionar que la propiedad 3 se denomina desigualdad triangular.

Observación 1.1.10. Sean ν una valuación discreta de F/K y $0 < c < 1$ un número real fijo. Entonces podemos definir $|\cdot|_\nu : F \to \mathbb{R}$ como

$$|z|_\nu = \begin{cases} c^{\nu(z)}, & z \neq 0, \\ 0, & z = 0. \end{cases}$$

Así, $|\cdot|_\nu$ es un valor absoluto donde la desigualdad triangular es consecuencia de la propiedad 3 de la valuación ν.

Lema 1.1.11. *Si ν es una valuación de F/K y $z_1, z_2 \in F$ satisfacen que $\nu(z_1) \neq \nu(z_2)$, entonces $\nu(z_1 + z_2) = \min\{\nu(z_1), \nu(z_2)\}$.*

Definición 1.1.12. A cada lugar $P \in \mathbb{P}(F)$ se le asocia una función $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$ inducida por el Teorema 1.1.6 de la siguiente manera: si $z \neq 0$ y $z = t^n u$, donde t es un elemento primo para P y $u \in \mathcal{O}_P^*$, entonces $\nu_P(z) = n$ y $\nu_P(0) = \infty$.

Teorema 1.1.13. *Sea F/K un cuerpo de funciones.*

1. *Para todo lugar P la función ν_P es una valuación discreta. Más aún:*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \ : \ \nu_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{z \in F \ : \ \nu_P(z) = 0\}, \\ P &= \{z \in F \ : \ \nu_P(z) > 0\}. \end{aligned}$$

2. *Un elemento $t \in F$ es primo para P si y solo si $\nu_P(t) = 1$.*

3. *Si ν es una valuación de F y $P = \{z \in F \ : \ \nu(z) > 0\}$, entonces P es un lugar de F.*

Definición 1.1.14. Dado P un lugar de un cuerpo de funciones F/K, se define el cuerpo de clases residuales de P como el cociente $F_P = \mathcal{O}_P/P$. Para cada $z \in F$ se denota a

la clase de z módulo P mediante $z(P)$, teniendo en cuenta que si $z \notin \mathcal{O}_P$ se considera que $z(P) = \infty$.

Puede verse que K es un subcuerpo de F_P, por lo que se define el grado de P mediante $\deg P = [F_P : K]$. Si $\deg P = 1$ decimos que P es un lugar racional.

Proposición 1.1.15. *Si P es un lugar de F/K y $0 \neq x \in P$, entonces*

$$\deg P \leq [F : K(x)] < \infty.$$

Observación 1.1.16. Si K es algebraicamente cerrado, todos los lugares son racionales, pues para un lugar P tenemos que $[F_P : K] < \infty$, y por lo tanto F_P/K es algebraica. Pero entonces $F_P = K$. En este caso podemos ver a cada elemento $z \in F$ como una función $z : \mathbb{P}(F) \to K \cup \{\infty\}$ tal que $P \mapsto z(P)$.

Esta es la razón por la cual F/K se denomina cuerpo de funciones y, como los elementos de K resultan ser funciones constantes, K se denomina cuerpo de constantes de F.

Definición 1.1.17. Sean $z \in F$ y $P \in \mathbb{P}(F)$. Decimos que P es un cero de z si $\nu_P(z) > 0$, y que es un cero de orden $m > 0$ si $\nu_P(z) = m$. Decimos que P es un polo de z si $\nu_P(z) < 0$, y que es un polo de orden $m > 0$ si $\nu_P(z) = -m$.

Observación 1.1.18. Todo $z \in F$ no constante posee al menos un cero y al menos un polo.

1.2. Cuerpos de funciones racionales

Consideremos ahora el caso del cuerpo de funciones racionales $F = K(x)$, donde x es trascendente sobre K.

Cada polinomio mónico irreducible $p(x) \in K[x]$ determina un anillo de valuaciones con su correspondiente lugar, de la siguiente manera:

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\}, \tag{1.2}$$

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in K[x],\ p(x) | f(x),\ p(x) \nmid g(x) \right\}, \tag{1.3}$$

donde $p(x)|f(x)$ significa que $p(x)$ divide a $f(x)$, mientras que $p(x) \nmid g(x)$ indica que $p(x)$ no divide a $g(x)$.

En el caso particular de polinomios lineales de la forma $p(x) = x - \alpha$ es usual escribir, simplemente, P_α en lugar de $P_{x-\alpha}$.

Además de los lugares y anillos de valuaciones asociados a los polinomios mónicos irreducibles, el cuerpo de funciones racionales presenta un lugar y un anillo de valuaciones especiales dados por:

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in K[x], \ \deg f \leq \deg g \right\}, \tag{1.4}$$

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in K[x], \ \deg f < \deg g \right\}. \tag{1.5}$$

El lugar P_∞ se denomina lugar en el infinito de F.

Observemos que las notaciones dependen de la elección del elemento generador x. Por ejemplo, $K(x) = K(x^{-1})$ y el lugar en el infinito con respecto a x^{-1} es el lugar P_0 con respecto a x.

En el siguiente resultado se enuncian propiedades muy importantes de los cuerpos de funciones racionales.

Proposición 1.2.1. *Sea $F = K(x)$ el cuerpo de funciones racionales sobre K.*

1. *Sea $P = P_{p(x)}$ un lugar de F definido por (1.3), donde $p(x) \in K[x]$ es irreducible y mónico. Entonces $p(x)$ es un elemento primo para P, el cuerpo de clases residuales $F_P = K(x)_P$ es isomorfo a $K[x]/\langle p(x) \rangle$, y $\deg P = \deg p(x)$.*

2. *Si $p(x) = x - \alpha$ para algún $\alpha \in K$, entonces $\deg P = 1$ y la función de clases residuales está dada por $z(P) = z(\alpha)$ para $z \in F$, donde $z(\alpha)$ se define a partir de cualquier representación irreducible de $z = f(x)/g(x)$, $f(x), g(x) \in K[x]$, de la siguiente manera:*

$$z(\alpha) = \begin{cases} f(\alpha)/g(\alpha), & g(\alpha) \neq 0, \\ \infty, & g(\alpha) = 0. \end{cases}$$

3. *Sea $P = P_\infty$ el lugar en el infinito de F definido por (1.5). Entonces $\deg P = 1$, un elemento primo para P es x^{-1}, y $\nu_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x)$, para polinomios $f(x), g(x) \in K[x]$.*

Teorema 1.2.2. *No existen otros lugares en $K(x)/K$ diferentes de los lugares $P_{p(x)}$ y P_∞ definidos por (1.3) y (1.5).*

Corolario 1.2.3. *Los lugares racionales de $K(x)/K$ están en correspondencia biunívoca con $K \cup \{\infty\}$.*

1.3. Independencia de valuaciones

El resultado principal de esta sección es el Teorema de Aproximación Débil, o Teorema de Independencia, cuya esencia es la siguiente: si $\nu_1, \ldots, \nu_n$ son diferentes valuaciones discretas de F/K y $z \in F$ es un elemento del cual conocemos las valuaciones $\nu_1(z), \ldots, \nu_{n-1}(z)$, entonces no podemos concluir información alguna acerca de $\nu_n(z)$. El Teorema de Aproximación Débil dice lo siguiente:

Teorema 1.3.1. *Consideremos F/K un cuerpo de funciones, $P_1, \ldots, P_n$ lugares distintos de F, $x_1, \ldots, x_n \in F$, y $r_1, \ldots, r_n \in \mathbb{Z}$, entonces existe $x \in F$ tal que $\nu_{P_i}(x - x_i) = r_i$ para $i = 1, \ldots, n$.*

El teorema anterior, además de la importancia propia, tiene consecuencias fundamentales para esta teoría.

Corolario 1.3.2. *Todo cuerpo de funciones tiene infinitos lugares.*

Proposición 1.3.3. *Consideremos un cuerpo de funciones F/K, $P_1, \ldots, P_r \in \mathbb{P}(F)$, y $x \in F$ tal que $\nu_{P_i}(x) > 0$ (P_i es un cero de x) para todo $i = 1, \ldots, r$, entonces*

$$\sum_{i=1}^{r} \nu_{P_i}(x) \deg P_i \leq [F : K(x)].$$

Corolario 1.3.4. *En un cuerpo de funciones F/K sucede que todo elemento no nulo $x \in F$ tiene una cantidad finita de ceros y polos.*

1.4. Divisores

Definición 1.4.1. El grupo de divisores de un cuerpo de funciones F/K se define como el grupo abeliano libre (denotado aditivamente) generado por los lugares de F/K. Este

grupo se simboliza como $\mathrm{Div}(F)$ y sus elementos se llaman divisores de F/K. Un divisor es una suma formal como:

$$D = \sum_{P \in \mathbb{P}(F)} n_P P, \quad n_P \in \mathbb{Z},$$

donde $n_P = 0$ salvo quizás para una cantidad finita de lugares P. El soporte de D se define como $\mathrm{sop}(D) = \{P \in \mathbb{P}(F) \ : \ n_P \neq 0\}$. Un divisor de la forma $D = P$ para algún lugar P se denomina divisor primo. Notemos que la suma de dos divisores se realiza de la siguiente manera:

$$D + D' = \sum_{P \in \mathbb{P}(F)} n_P P + \sum_{P \in \mathbb{P}(F)} n'_P P = \sum_{P \in \mathbb{P}(F)} (n_P + n'_P) P.$$

El elemento neutro del grupo es:

$$0 = \sum_{P \in \mathbb{P}(F)} 0P.$$

Para cada lugar P, definimos $\nu_P(D) = n_P$, por lo que podemos escribir

$$\mathrm{sop}(D) = \{P \in \mathbb{P}(F) \ : \ \nu_P(D) \neq 0\}$$

y

$$D = \sum_{P \in \mathbb{P}(F)} \nu_P(D) P.$$

Además, tenemos un orden parcial dado por:

$$D_1 \leq D_2 \Leftrightarrow \nu_P(D_1) \leq \nu_P(D_2) \ \forall \ P \in \mathbb{P}(F).$$

Si $D_1 \leq D_2$ y $D_1 \neq D_2$, escribimos $D_1 < D_2$. Análogamente podemos escribir $D_1 \geq D_2$ y $D_1 > D_2$. En particular, decimos que D es positivo o efectivo si $D \geq 0$. Definimos el grado de un divisor como:

$$\deg D = \sum_{P \in \mathbb{P}(F)} \nu_P(D) \deg P.$$

Definición 1.4.2. Sean $0 \neq z \in F$, $Z \subset \mathbb{P}(F)$ el conjunto de ceros de z, y $N \subset \mathbb{P}(F)$ el conjunto de polos de z. Se definen los siguientes divisores asociados a z:

$$(z)_0 = \sum_{P \in Z} \nu_P(z) P, \text{ divisor de ceros de } z,$$

$$(z)_\infty = \sum_{P \in N} (-\nu_P(z)) P, \text{ divisor de polos de } z,$$

$$(z) = (z)_0 - (z)_\infty, \text{ divisor principal de } z.$$

Notemos que $(z)_0$ y $(z)_\infty$ son divisores efectivos. Los elementos $0 \neq z \in F$ que son constantes se caracterizan mediante

$$z \in K^* \Leftrightarrow (z) = 0.$$

Definición 1.4.3. El grupo de divisores principales de F/K es un subgrupo de $\mathrm{Div}(F)$ que se denota por $\mathrm{Prin}(F)$. El grupo cociente $\mathrm{Cl}(F) = \mathrm{Div}(F)/\mathrm{Prin}(F)$ se denomina grupo de clases de divisores de F/K. Si $D \in \mathrm{Div}(F)$, denotamos su clase por $[D]$. Dos divisores D y D' son equivalentes si $[D] = [D']$, y si esto sucede escribimos $D \sim D'$. Es decir, $D \sim D'$ si y solo si $D - D' = (z)$ para algún $z \in F$.

A continuación, se definen los espacios de Riemann-Roch, que son fundamentales en la teoría de códigos algebraico-geométricos sobre la cual trabajamos.

Definición 1.4.4. Sea A un divisor de un cuerpo de funciones F/K. Definimos el espacio de Riemann-Roch asociado a A como:

$$\mathcal{L}(A) = \{z \in F \ : \ (z) + A \geq 0\} \cup \{0\}.$$

Observación 1.4.5. Si $A \in \mathrm{Div}(F)$, entonces:

1. $z \in \mathcal{L}(A)$ si y solo si $\nu_P(z) \geq -\nu_P(A)$ para todo $P \in \mathbb{P}(F)$.
2. $\mathcal{L}(A) \neq \{0\}$ si y solo si existe $A' \sim A$ tal que $A' \geq 0$.

Lema 1.4.6. *Sean $A, B \in \mathrm{Div}(F)$.*

1. *$\mathcal{L}(A)$ es un espacio vectorial sobre K.*
2. *Si $A' \sim A$, entonces $\mathcal{L}(A')$ y $\mathcal{L}(A)$ son espacios vectoriales isomorfos.*
3. *$\mathcal{L}(0) = K$ y $\mathcal{L}(A) = \{0\}$ si $A < 0$.*
4. *Si $A \leq B$, entonces $\mathcal{L}(A) \subset \mathcal{L}(B)$ y*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A,$$

donde $\mathcal{L}(B)/\mathcal{L}(A)$ es el espacio cociente de $\mathcal{L}(B)$ por $\mathcal{L}(A)$.

Notemos que todo divisor A puede escribirse como $A = A_+ - A_-$ con $A_+, A_- \geq 0$.

Proposición 1.4.7. *Si $A \in \mathrm{Div}(F)$, entonces $\mathcal{L}(A)$ es un espacio vectorial de dimensión finita sobre K. Mas aún,* $\dim \mathcal{L}(A) \leq \deg A_+ + 1$.

Definición 1.4.8. Si A es un divisor de F/K, definimos la dimensión de A como la dimensión del espacio de Riemann-Roch asociado a A, y la denotamos por $\ell(A)$. Es decir,

$$\ell(A) = \dim \mathcal{L}(A).$$

Teorema 1.4.9. *Todo divisor principal es de grado cero. Más precisamente, si $z \in F - K$,*

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

Corolario 1.4.10. *Sea F/K un cuerpo de funciones.*

1. *Si $A, A' \in \mathrm{Div}(F)$ tales que $A \sim A'$, entonces $\ell(A) = \ell(A')$ y $\deg A = \deg A'$.*
2. *Si $\deg A \geq 0$, entonces $\ell(A) \leq 1 + \deg A$.*
3. *Si $\deg A < 0$, $\ell(A) = 0$.*
4. *Si $A \in \mathrm{Div}(F)$ y $\deg A = 0$, entonces:*

$$A \text{ es principal } \Leftrightarrow \ell(A) \geq 1 \Leftrightarrow \ell(A) = 1.$$

Ejemplo 1.4.11. Consideremos el cuerpo de funciones racionales $F = K(x)$ y un elemento $0 \neq z \in F$. Entonces existen $0 \neq a \in K$ y $f(x), g(x) \in K[x]$ polinomios mónicos y coprimos tales que $z = af(x)/g(x)$. Ahora bien, $f(x)$ y $g(x)$ pueden escribirse como productos de polinomios según sus divisores irreducibles de la siguiente manera:

$$f(x) = \prod_{i=1}^{r} f_i(x)^{n_i}, \qquad g(x) = \prod_{j=1}^{s} g_j(x)^{m_j},$$

donde los polinomios $f_i(x)$, para $i = 1, \ldots, r$, y $g_j(x)$, para $j = 1, \ldots, s$, son mónicos e irreducibles, y son coprimos entre ellos. Por lo tanto cada uno de ellos tiene asociado un lugar del cuerpo de funciones . Si $P_i = P_{f_i(x)}$ para cada i, y $Q_j = Q_{g_j(x)}$ para cada j, tenemos que

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\deg g(x) - \deg f(x)) P_\infty.$$

Así, el divisor principal de z tiene como soporte a los lugares asociados a los polinomios mónicos irreducibles que forman parte de la escritura de z. $\Diamond$

Los siguientes resultados nos conducirán a la definición de género de un cuerpo de funciones, otra de las nociones fundamentales de esta teoría.

Proposición 1.4.12. *Dado un cuerpo de funciones F/K, existe $\gamma \in \mathbb{Z}$ (que solamente depende de F) tal que para todo $A \in \mathrm{Div}(F)$ se satisface*

$$\deg A - \ell(A) \leq \gamma.$$

Definición 1.4.13. El género $g = g(F)$ de un cuerpo de funciones F/K está definido como:

$$g = \max_{A \in \mathrm{Div}(F)} (\deg A - \ell(A) + 1).$$

Corolario 1.4.14. *$g(F) \geq 0$ para cualquier cuerpo de funciones F/K .*

El siguiente teorema se conoce como Teorema de Riemann, y nos proporciona información sobre las dimensiones $\ell(A)$ de espacios de Riemann-Roch.

Teorema 1.4.15. *Sea F/K un cuerpo de funciones de género g.*

1. *$\ell(A) \geq \deg A + 1 - g$ para todo $A \in \mathrm{Div}(F)$.*

2. *Existe una constante c que solo depende de F tal que $\ell(A) = \deg A + 1 - g$ para todo divisor A tal que $\deg A \geq c$.*

Ejemplo 1.4.16. Veamos que el género de $F = K(x)$ es $g = 0$. Sea P_∞ el divisor de polos de x y consideremos para $r \geq 0$ el espacio $\mathcal{L}(rP_\infty)$. Como $\{1, x, x^2, \ldots, x^r\} \subset \mathcal{L}(rP_\infty)$, si tomamos r suficientemente grande, tenemos que:

$$r + 1 \leq \ell(rP_\infty) = \deg rP_\infty + 1 - g = r + 1 - g.$$

Así, $g \leq 0$ y, por el Corolario 1.4.14, obtenemos que $g = 0$. $\Diamond$

1.5. Teorema de Riemann-Roch

En esta sección F/K será un cuerpo de funciones de género g.

Definición 1.5.1. Para cada $A \in \mathrm{Div}(F)$ se define su índice de especialidad como:

$$i(A) = \ell(A) - \deg A - 1 + g.$$

El Teorema de Riemann (1.4.15) implica que $i(A) \geq 0$ y además $i(A) = 0$ si $\deg A$ es suficientemente grande.

Vamos a interpretar $i(A)$ como la dimensión de ciertos espacios vectoriales, para lo cual introduciremos la noción de adel.

Definición 1.5.2. Un adel de F/K es una función

$$\begin{array}{rccc} \alpha\colon & \mathbb{P}(F) & \to & F, \\ & P & \mapsto & \alpha_P, \end{array}$$

tal que $\alpha_P \in \mathcal{O}_P$ para casi todo $P \in \mathbb{P}(F)$. Podemos considerar a un adel como un elemento del producto directo $\prod_{P\in\mathbb{P}(F)} F$ y usar la notación $\alpha = (\alpha_P)_{P\in\mathbb{P}(F)}$ o directamente $\alpha = (\alpha_P)$.

El conjunto $\mathcal{A}_F$ de todos los adeles de F se denomina espacio de adeles de F/K y lo consideraremos como un espacio vectorial sobre K, aunque en realidad posee una estructura de anillo.

El adel principal de un elemento $z \in F$ es el adel $\alpha = (z)$, es decir, $\alpha_P = z$ para todo $P \in \mathbb{P}(F)$. Obtenemos así una inmersión de F en $\mathcal{A}_F$.

Las valuaciones de F se extienden naturalmente a $\mathcal{A}_F$ considerando que si $\alpha = (\alpha_P)$, entonces $\nu_P(\alpha) = \nu_P(\alpha_P)$. Como $\alpha_P \in \mathcal{O}_P$, obtenemos que $\nu_P(\alpha) \geq 0$ para casi todo $P \in \mathbb{P}(F)$.

Definición 1.5.3. Para $A \in \mathrm{Div}(F)$ definimos un K-subespacio vectorial de $\mathcal{A}_F$ dado por:

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F \ :\ \nu_P(\alpha) + \nu_P(A) \geq 0,\ \forall\ P \in \mathbb{P}_F\}.$$

Teorema 1.5.4. *Para todo A divisor de F se satisface que:*

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

Notemos que $\mathcal{A}_F$, $\mathcal{A}_F(A)$ y F son K-espacios vectoriales de dimensión infinita, pero el teorema establece que el cociente $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$ es de dimensión finita.

El teorema anterior también puede formularse de la siguiente manera: para todo divisor A de F se satisface:

$$\ell(A) = \deg A + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)).$$

Así, obtenemos una versión preliminar del Teorema de Riemann-Roch.

Además, tomando el divisor nulo $A = 0$ se obtiene el siguiente corolario que brinda otra descripción del género.

Corolario 1.5.5. $g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F))$.

Definición 1.5.6. Un diferencial de Weil de F/K es una función K-lineal $w : \mathcal{A}_F \to K$ que se anula en $\mathcal{A}_F(A)+F$ para algún divisor A de F. Llamamos módulo de diferenciales de Weil al conjunto Ω_F de todos los diferenciales de Weil, y denotamos $\Omega_F(A)$, para un divisor A, al conjunto de los diferenciales de Weil que se anulan en $\mathcal{A}_F(A)+F$.

Podemos considerar a Ω_F como un K-espacio vectorial: sean $w_1, w_2 \in \Omega_F$ tales que w_i se anula en $\mathcal{A}_F(A_i)+F$ para $i = 1, 2$. Entonces w_1+w_2 se anula en $\mathcal{A}_F(A_3)+F$, donde A_3 cumple que $A_3 \leq A_1$ y $A_3 \leq A_2$. Además, si $a \in K$, aw_1 se anula en $\mathcal{A}_F(A_1)+F$. Así, se tiene que $\Omega_F(A)$ es un K-subespacio vectorial de Ω_F.

Lema 1.5.7. $\dim \Omega_F(A) = i(A)$ *para todo* $A \in \mathrm{Div}(F)$.

Una consecuencia del lema anterior es que $\Omega_F \neq \{0\}$, pues tomando $\deg A \leq -2$ obtenemos que $\dim \Omega_F(A) \geq 1$.

Definición 1.5.8. Si $z \in F$ y $w \in \Omega_F$, se define $zw : \mathcal{A}_F \to K$ como $zw(\alpha) = w(z\alpha)$. De esta manera dotamos a Ω_F de una estructura de F-espacio vectorial.

Proposición 1.5.9. $\dim_F \Omega_F = 1$.

Se quiere poder asociar un divisor en particular a cada diferencial de Weil $w \neq 0$. Para ello consideramos el siguiente conjunto de divisores:

$$M(w) = \{A \in \mathrm{Div}(F) \ : \ w|_{\mathcal{A}_F(A)+F} = 0\}.$$

Lema 1.5.10. *Sea $0 \neq w \in \Omega_F$. Entonces existe un único divisor $W \in M(w)$ tal que $A \leq W$ para todo $A \in M(w)$.*

Definición 1.5.11. En este contexto tenemos las siguientes definiciones:

1. El divisor (w) de un diferencial de Weil $w \neq 0$ es el divisor de F/K determinado por el lema anterior.

2. Para $0 \neq w \in \Omega_F$ y $P \in \mathbb{P}(F)$ se define $\nu_P(w) = \nu_P((w))$.

3. Para $0 \neq w \in \Omega_F$ y $P \in \mathbb{P}(F)$, decimos que P es un cero de w si $\nu_P(w) > 0$ y que es un polo de w si $\nu_P(w) < 0$. Decimos que w es regular en P si $\nu_P(w) \geq 0$ y que w es regular u holomorfo si es regular en todos los lugares P.

4. Un divisor W se dice canónico si $W = (w)$ para algún diferencial de Weil w.

Observación 1.5.12. Con las definiciones anteriores, obtenemos una nueva descripción de los siguientes espacios:

$$\Omega_F(A) = \{w \in \Omega_F \ : \ (w) \geq A\} \cup \{0\},$$
$$\Omega_F(0) = \{w \in \Omega_F \ : \ w \text{ es regular}\}.$$

Proposición 1.5.13.

1. Si $0 \neq z \in F$ y $0 \neq w \in \Omega_F$, entonces $(zw) = (z) + (w)$.

2. Todos los divisores canónicos de F son equivalentes entre sí.

Teorema 1.5.14. *Si $A \in \mathrm{Div}(F)$ y $W = (w)$ es un divisor canónico no nulo, entonces $\mathcal{L}(W - A)$ y $\Omega_F(A)$ son espacios vectoriales isomorfos. En particular, se tiene que $i(A) = \ell(W - A)$.*

Estamos en condiciones de enunciar el Teorema de Riemann-Roch, que es el resultado más importante de la teoría de cuerpos de funciones.

Teorema 1.5.15. *Sean $A, W \in \mathrm{Div}(F)$, con W un divisor canónico de F/K. Entonces*
$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

Corolario 1.5.16. *Si W es un divisor canónico, entonces*
$$\deg W = 2g - 2, \quad \ell(W) = g.$$

Teorema 1.5.17. *Sea $A \in \mathrm{Div}(F)$ con $\deg A > 2g - 2$. Entonces*
$$\ell(A) = \deg A + 1 - g.$$

1.6. Extensiones de cuerpos de funciones

Comenzamos esta sección con algunas definiciones básicas.

Definición 1.6.1.

1. Un cuerpo de funciones algebraicas F'/K' es una extensión algebraica de F/K si $F' \supset F$ es una extensión algebraica de cuerpos y si $K' \supset K$.

2. La extensión algebraica F'/K' de F/K es una extensión por cuerpo de constantes si $F' = K'F$, el cuerpo composición de K' y F.

3. La extensión algebraica F'/K' de F/K es una extensión finita si $[F' : F] < \infty$.

Lema 1.6.2. *Sea F'/K' una extensión algebraica de F/K. Entonces:*

1. *K'/K es algebraica y $K = F \cap K'$.*

2. *F'/K' es una extensión finita de F/K si y solo si $[K' : K] < \infty$.*

3. *Sea $F_1 = FK'$. Entonces F_1/K' es una extensión por cuerpo de constantes de F/K y F'/K' es una extensión finita de F_1/K'.*

Analizamos ahora la relación entre los lugares de F' y los de F.

Definición 1.6.3. Consideremos una extensión algebraica F'/K' de F/K, un lugar P' de F' y un lugar P de F. Decimos que P' está arriba de P, y escribimos $P'|P$, si sucede que $P' \supset P$. También podemos decir que P está abajo de P'.

Proposición 1.6.4. *Sean F'/K' una extensión algebraica de F/K, P' y P lugares de F' y F respectivamente, $\mathcal{O}_{P'} \subset F'$ y $\mathcal{O}_P \subset F$ los anillos de valuaciones correspondientes, y sean $\nu_{P'}$ y ν_P las valuaciones asociadas. Entonces equivalen:*

1. *$P'|P$.*

2. *$\mathcal{O}_{P'} \supset \mathcal{O}_P$.*

3. *Existe $e \in \mathbb{N}$ tal que $\nu_{P'}(z) = e\nu_P(z)$ para todo $z \in F$.*

Más aún, si $P'|P$, entonces $P = P' \cap F$ y $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Por esta razón, también suele decirse que P es la restricción de P' en F.

Definición 1.6.5. Sean F'/K' una extensión algebraica de F/K, $P' \in \mathbb{P}(F')$ y $P \in \mathbb{P}(F)$ tales que $P'|P$.

1. El índice de ramificación $e(P'|P)$ de P' sobre P es el entero positivo e que satisface $\nu_{P'}(z) = e\nu_P(z)$ para todo $z \in F$. Decimos que $P'|P$ es ramificado si $e(P'|P) > 1$ y que no es ramificado si $e(P'|P) = 1$.

2. El grado de inercia o grado relativo $f(P'|P)$ de P' sobre P es $f(P'|P) = [F'_{P'} : F_P]$. Este valor puede ser finito o no.

Proposición 1.6.6. *Sean F'/K' una extensión algebraica de F/K, $P' \in \mathbb{P}(F')$ y $P \in \mathbb{P}(F)$ tales que $P'|P$. Entonces:*

1. *$f(P'|P) < \infty$ si y solo si $[F' : F] < \infty$.*

2. *Si F''/K'' es una extensión algebraica de F'/K' y $P'' \in \mathbb{P}(F'')$ está arriba de P', entonces*

$$\begin{aligned} e(P''|P) &= e(P''|P')e(P'|P), \\ f(P''|P) &= f(P''|P')f(P'|P). \end{aligned}$$

Proposición 1.6.7. *Sea F'/K' una extensión algebraica de F/K. Entonces:*

1. *Para cada lugar P' de F' hay exactamente un lugar P de F tal que $P'|P$.*

2. *Para cada lugar P de F hay al menos un lugar P' de F' tal que $P'|P$.*

El siguiente resultado se conoce como igualdad fundamental, y será relevante al momento de relacionar códigos cíclicos con extensiones cíclicas.

Teorema 1.6.8. *Sean F'/K' una extensión fiinita de F/K, $P \in \mathbb{P}(F)$ un lugar de F y $P_1, \ldots, P_m \in \mathbb{P}(F')$ todos los lugares de F' que están arriba de P. Entonces:*

$$\sum_{i=1}^{m} e(P_i|P)f(P_i|P) = [F' : F].$$

Como consecuencias directas de la igualdad fundamental obtenemos:

Corolario 1.6.9. *Sean F'/K' una extensión finita de F/K y P un lugar de F. Entonces:*

1. $|\{P' \in \mathbb{P}(F') \ : \ P'|P\}| \leq [F' : F]$.

2. *Si $P' \in \mathbb{P}(F')$ está arriba de P, entonces $e(P'|P) < [F' : F]$ y $f(P'|P) < [F' : F]$.*

Definición 1.6.10. Sean F'/K' una extensión algebraica finita de F/K, donde se satisface que $[F' : F] = n$, y P un lugar de F.

1. Decimos que P se descompone completamente en F'/F si existen exactamente n lugares de F' arriba de P.

2. Decimos que P es totalmente ramificado en F'/F si existe un lugar P' de F' arriba de P tal que $e(P'|P) = n$.

Observación 1.6.11. Por la igualdad fundamental, P se descompone completamente si y solo si $e(P'|P) = f(P'|P) = 1$ para todo $P'|P$ y P es totalmente ramificado si existe un único lugar $P'|P$ y, además, $e(P'|P) = n$ y $f(P'|P) = 1$.

Capítulo 2

Códigos algebraico-geométricos

En este capítulo describimos la construcción dada por Goppa de códigos correctores de errores usando cuerpos de funciones algebraicas. Comenzamos con algunos conceptos básicos de la teoría de códigos, luego definimos los códigos algebraico-geométricos (códigos AG) y presentamos sus principales propiedades. Los códigos construidos en base a cuerpos de funciones racionales (fundamentales en el desarrollo de esta tesis) se estudian con detalle en la Sección 2.3.

2.1. Códigos

Si $\mathbb{F}_q$ es el cuerpo finito con q elementos, consideramos el espacio vectorial de dimensión n sobre $\mathbb{F}_q$ denotado por $\mathbb{F}_q^n$, cuyos elementos son de la forma $(a_1, \ldots, a_n)$, con $a_1, \ldots, a_n \in \mathbb{F}_q$.

Definición 2.1.1. Sean $a = (a_1, \ldots, a_n),\ b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ y $0 \in \mathbb{F}_q^n$ el vector nulo. Se definen la distancia de Hamming $d(a, b)$ y el peso de Hamming $w(a)$ como:

$$\begin{aligned} d(a,b) &= |\{i \ : \ a_i \neq b_i,\ 1 \leq i \leq n\}|, \\ w(a) &= d(a,0). \end{aligned}$$

Observación 2.1.2. La distancia de Hamming es efectivamente una distancia o métrica en $\mathbb{F}_q^n$.

Definición 2.1.3. Un código lineal de bloque $\mathcal{C}$ sobre el alfabeto $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$. Los elementos de $\mathcal{C}$ se denominan palabras código, o simplemente palabras. Llamamos a n la longitud de $\mathcal{C}$ y a $k = \dim_{\mathbb{F}_q} \mathcal{C}$ la dimensión de $\mathcal{C}$. Así, un $[n, k]$-código sobre $\mathbb{F}_q$ es un código de longitud n y dimensión k. La distancia mínima $d = d(\mathcal{C})$ es:

$$d(\mathcal{C}) = \text{mín}\{d(c_1, c_2) \ : \ c_1, c_2 \in \mathcal{C}, \ c_1 \neq c_2\},$$

pero también puede calcularse mediante el peso mínimo $w(\mathcal{C})$:

$$d(\mathcal{C}) = w(\mathcal{C}) = \min_{0 \neq c \in \mathcal{C}} w(c).$$

Un $[n, k, d]$-código es un $[n, k]$-código con distancia mínima d.

Observación 2.1.4. En esta tesis solamente trabajaremos con códigos lineales de bloque, por lo que hablaremos simplemente de códigos para referirnos a ellos.

Observación 2.1.5. Sean $\mathcal{C}$ un código con distancia mínima d y $t = \lfloor (d-1)/2 \rfloor$. Decimos que $\mathcal{C}$ es t-corrector, o que corrige t errores, pues si $u \in \mathbb{F}_q^n$ y $c \in \mathcal{C}$ son tales que $d(u, c) \leq t$, entonces c es la única palabra código tal que $d(u, c) \leq t$.

Una manera simple de describir un código $\mathcal{C}$ explícitamente es mediante una base de $\mathcal{C}$ como espacio vectorial sobre $\mathbb{F}_q$.

Definición 2.1.6. Sea $\mathcal{C}$ un $[n, k]$-código sobre $\mathbb{F}_q$. Una matriz generadora de $\mathcal{C}$ es una matriz de tamaño $k \times n$ cuyas filas forman una base de $\mathcal{C}$.

Definición 2.1.7. El producto interno canónico en $\mathbb{F}_q^n$ está dado por

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. Ésta es una forma bilineal simétrica no degenerada en $\mathbb{F}_q^n$.

Definición 2.1.8. Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código, definimos el código dual de $\mathcal{C}$ como:

$$\mathcal{C}^{\perp} = \{u \in \mathbb{F}_q^n \ : \ \langle u, c \rangle = 0, \ \forall \ c \in \mathcal{C}\}.$$

Decimos que $\mathcal{C}$ es auto-dual si $\mathcal{C} = \mathcal{C}^{\perp}$ y que es auto-ortogonal si $\mathcal{C} \subset \mathcal{C}^{\perp}$. Es bien sabido, por álgebra lineal, que si $\mathcal{C}$ es un $[n, k]$-código, entonces $\mathcal{C}^{\perp}$ es un $[n, n-k]$-código, y que $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. En particular, la dimensión de un código auto-dual de longitud n es $n/2$.

Definición 2.1.9. Si H es una matriz generadora de $\mathcal{C}^{\perp}$, decimos que H es una matriz de paridad de $\mathcal{C}$.

Observación 2.1.10. Una matriz de paridad H de un $[n,k]$-código $\mathcal{C}$ es una matriz de tamaño $(n-k)\times n$, con rango $n-k$, y se tiene que

$$\mathcal{C} = \{c \in \mathbb{F}_q^n \ : \ Hc^t = 0\},$$

donde c^t es el vector columna que se obtiene de transponer c. Así, la matriz de paridad chequea cuándo un vector de $\mathbb{F}_q^n$ es una palabra código y cuándo no.

Uno de los problemas básicos en teoría de códigos algebraicos es construir, sobre un alfabeto fijo $\mathbb{F}_q$, códigos cuyas dimensión y distancia mínima sean comparables, de alguna manera adecuada, con su longitud. Sin embargo, hay algunas restricciones. La siguiente se conoce como la cota de Singleton:

Proposición 2.1.11 (Cota de Singleton)**.** *Si $\mathcal{C}$ es un $[n,k,d]$-código, entonces:*

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

Definición 2.1.12. Si $\mathcal{C}$ es un $[n,k,d]$-código tal que $k+d = n+1$, decimos que $\mathcal{C}$ es un código MDS (Máxima Distancia de Separación).

Observación 2.1.13. Si $n \leq q+1$, existen códigos MDS sobre $\mathbb{F}_q$ de longitud n, para cualquier dimensión $k \leq n$.

Uno de los aportes más importantes de esta tesis consiste en clasificar ciertos códigos según clases de equivalencia. Lo haremos considerando lo siguiente:

Definición 2.1.14. Dos códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ sobre $\mathbb{F}_q$ son llamados equivalentes, y escribimos $\mathcal{C}_1 \sim \mathcal{C}_2$, si existe una matriz monomial M tal que $\mathcal{C}_2 = \mathcal{C}_1 M$ (una matriz monomial es un producto de una matriz diagonal por un matriz de permutaciones). En otras palabras, $\mathcal{C}_1 \sim \mathcal{C}_2$ si cada palabra código de $\mathcal{C}_2$ puede obtenerse a partir de una palabra código de $\mathcal{C}_1$ mediante una combinación de las siguientes operaciones:

1. Permutación de los dígitos de una palabra código.

2. Multiplicación de cada dígito de una palabra código por algún escalar no nulo (no necesariamente el mismo escalar para cada dígito).

2.2. Códigos algebraico-geométricos

Los códigos algebraico-geométricos, en adelante códigos AG, fueron introducidos por Goppa, por lo que también se denominan códigos de Goppa geométricos. Como una motivación para la construcción de los códigos AG, consideraremos primero los llamados códigos de Reed-Solomon sobre $\mathbb{F}_q$.

Los códigos de Reed-Solomon son muy conocidos en teoría de códigos, y en esta tesis mostraremos algunas características de ellos que no estaban desarrolladas.

Sean $n = q - 1$ y $\beta \in \mathbb{F}_q$ un elemento primitivo del grupo multiplicativo $\mathbb{F}_q^*$, es decir:

$$\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^{n-1}, \beta^n = 1\}.$$

Para $0 \leq r \leq n-1$ consideramos el espacio vectorial de dimensión $k = r + 1$ dado por:

$$L_r = \{f \in \mathbb{F}_q[x] \ : \ \deg f \leq r\},$$

y la función de evaluación dada por:

$$\begin{aligned} ev: \ L_r &\to \mathbb{F}_q^n, \\ f &\mapsto (f(\beta), f(\beta^2), \ldots, f(\beta^n)). \end{aligned}$$

La función ev es $\mathbb{F}_q$-lineal y es inyectiva. Así, podemos obtener un $[n, k]$-código dado por:

$$\mathcal{C} = \mathrm{Im}(ev) = ev(L_r) = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) \ : \ f \in L_r\}.$$

Estos códigos son llamados códigos de Reed-Solomon, y resultan ser códigos MDS sobre $\mathbb{F}_q$.

Vamos a introducir la noción de códigos AG fijando la siguiente notación para el resto de la sección:

- $F/\mathbb{F}_q$ es un cuerpo de funciones algebraicas de género g.
- $P_1, \ldots, P_n$ son n lugares racionales distintos de F.
- $D = P_1 + \cdots + P_n$ es un divisor de F.
- G es un divisor de F tal que $\mathrm{sop}(G) \cap \mathrm{sop}(D) = \emptyset$.

Definición 2.2.1. El código AG asociado a los divisores D y G, $\mathcal{C}_{\mathcal{L}}(D,G)$, se define como

$$\mathcal{C}_{\mathcal{L}}(D,G) = \{(z(P_1),\ldots,z(P_n)) \in \mathbb{F}_q^n \ : \ z \in \mathcal{L}(G)\}.$$

Notar que esta definición tiene sentido pues, si $z \in \mathcal{L}(G)$, como $\mathrm{sop}(D) \cap \mathrm{sop}(G) = \emptyset$, entonces $\nu_{P_i}(z) \geq 0$ para $i = 1,\ldots,n$. Además, la clase residual $z(P_i)$ es un elemento de F_{P_i}. Pero como P_i es un lugar racional, podemos considerar que $F_{P_i} = \mathbb{F}_q$, y luego tenemos que $z(P_i) \in \mathbb{F}_q$ para todo i.

Si consideramos la función de evaluación dada por:

$$\begin{aligned} ev_D : \ \mathcal{L}(G) &\to \mathbb{F}_q^n, \\ z &\mapsto (z(P_1), z(P_2), \ldots, z(P_n)), \end{aligned}$$

vemos que $\mathcal{C}_{\mathcal{L}}(D,G) = \mathrm{Im}(ev_D)$, y como ev_D es una aplicación $\mathbb{F}_q$-lineal, $C_L(D,G)$ es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$.

El siguiente teorema nos presenta los parámetros de $\mathcal{C}_{\mathcal{L}}(D,G)$. En particular, a través de la teoría de códigos AG pueden obtenerse cotas no triviales para la distancia mínima en un contexto muy general.

Teorema 2.2.2. *$\mathcal{C}_{\mathcal{L}}(D,G)$ es un $[n,k,d]$-código tal que*

$$d \geq n - \deg G \quad \text{y} \quad k = \ell(G) - \ell(G-D).$$

Si disponemos de más información de G, podemos obtener lo siguiente:

Corolario 2.2.3. *Si $\deg G < n$, entonces ev_D es inyectiva y tenemos que:*

1. *$k = \ell(G) \geq \deg G + 1 - g$ y $k + d \geq n + 1 - g$.*
2. *Si $2g - 2 < \deg G < n$, entonces $k = \deg G + 1 - g$.*
3. *Si $\{z_1,\ldots,z_k\}$ es una base de $\mathcal{L}(G)$, una matriz generadora para $\mathcal{C}_{\mathcal{L}}(D,G)$ es:*

$$M = \begin{pmatrix} z_1(P_1) & z_1(P_2) & \cdots & z_1(P_n) \\ z_2(P_1) & z_2(P_2) & \cdots & z_2(P_n) \\ \vdots & & & \vdots \\ z_k(P_1) & z_k(P_2) & \cdots & z_k(P_n) \end{pmatrix}.$$

Observación 2.2.4. Notemos que la cota inferior obtenida para $k + d$ es similar a la cota de Singleton, que es una cota superior. Así, si $\deg G < n$ y combinamos ambas cotas obtenemos que:

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

Si $g(F) = 0$ obtenemos que $k + d = n + 1$, es decir, que los códigos AG sobre cuerpos de funciones racionales $\mathbb{F}_q(x)$ son códigos MDS.

Definición 2.2.5. El entero $d^* = n - \deg G$ se denomina distancia designada de $\mathcal{C}_{\mathcal{L}}(D, G)$.

Notar que $d \geq d^*$. Nos interesa saber si podemos distinguir si $d = d^*$ o $d > d^*$.

Proposición 2.2.6. *Sean $\ell(G) > 0$ y $d^* > 0$. Entonces $d = d^*$ si y solo si existe un divisor $D' \in \mathrm{Div}(F)$ tal que $0 \leq D' \leq D$, $\deg D' = \deg G$ y $\ell(G - D') > 0$.*

Otro código, también llamado código AG, puede asociarse a los divisores D y G usando componentes locales de diferenciales de Weil. Si $A \in \mathrm{Div}(F)$, $\Omega_F(A)$ es el espacio de los diferenciales de Weil w tales que $(w) \geq A$. Además, $\Omega_F(A)$ es un espacio vectorial de dimensión finita $i(A)$ sobre $\mathbb{F}_q$. Para un diferencial de Weil w y un lugar P, la función $w_P : F \to \mathbb{F}_q$ denota a la componente local de w en P.

Definición 2.2.7. Dados D y G como antes, definimos el código $\mathcal{C}_\Omega(D, G) \subset \mathbb{F}_q^n$ como:

$$\mathcal{C}_\Omega(D, G) = \left\{ (w_{P_1}(1), \ldots, w_{P_n}(1)) \in \mathbb{F}_q^n \ : \ w \in \Omega_F(G - D) \right\}.$$

2.3. Códigos AG racionales

Estudiaremos los códigos AG asociados a divisores de un cuerpo de funciones racionales. Describiremos estos códigos explícitamente, mediante matrices generadoras y de paridad. En teoría de códigos, esta clase de códigos se conoce como códigos de Reed-Solomon Generalizados, o simplemente códigos RSG, y son unos de los objetos principales en el desarrollo de esta tesis.

Definición 2.3.1. Un código AG racional es un código $\mathcal{C}_{\mathcal{L}}(D, G)$ definido sobre un cuerpo de funciones racionales $F = \mathbb{F}_q(x)$.

Notemos que la longitud de un código AG racional es a lo sumo $q+1$ pues $\mathbb{F}_q(x)$ tiene exactamente $q+1$ lugares racionales, que son los lugares $P_a = P_{x-a}$ para cada $a \in \mathbb{F}_q$ y el lugar P_∞, el polo de x.

Proposición 2.3.2. *Si $\mathcal{C} = \mathcal{C}_\mathcal{L}(D,G)$ es un $[n,k,d]$-código racional sobre $\mathbb{F}_q$, entonces:*

1. $n \leq q+1$.
2. $k = 0$ *si y solo si* $\deg G < 0$, *y* $k = n$ *si y solo si* $\deg G > n-2$.
3. *Si* $0 \leq \deg G \leq n-2$, *entonces* $k = 1 + \deg G$ *y* $d = n - \deg G$. *En particular,* $\mathcal{C}$ *es un código MDS.*
4. $\mathcal{C}^\perp$ *es también un código AG racional.*

Proposición 2.3.3. *Sea $\mathcal{C} = \mathcal{C}_\mathcal{L}(D,G)$ un $[n,k,d]$-código AG racional sobre $\mathbb{F}_q$.*

1. *Si $n \leq q$, existen n elementos distintos $a_1, \ldots, a_n \in \mathbb{F}_q$ y n elementos (no necesariamente distintos) $v_1, \ldots, v_n \in \mathbb{F}_q^*$ tales que*

$$\mathcal{C} = \{(v_1 f(a_1), \ldots, v_n f(a_n)) \ : \ f \in \mathbb{F}_q[x],\ \deg f \leq k-1\}.$$

Una matriz generadora para $\mathcal{C}$ es

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ a_1 v_1 & a_2 v_2 & \cdots & a_n v_n \\ a_1^2 v_1 & a_2^2 v_2 & \cdots & a_n^2 v_n \\ \vdots & & & \vdots \\ a_1^{k-1} v_1 & a_2^{k-1} v_2 & \cdots & a_n^{k-1} v_n \end{pmatrix}.$$

2. *Si $n = q+1$, escribimos $\mathbb{F}_q = \{a_1, a_2, \ldots, a_{n-1}\}$ y existen $n-1$ elementos (no necesariamente distintos) $v_1, \ldots, v_{n-1} \in \mathbb{F}_q^*$ tales que una matriz generadora para $\mathcal{C}$ es*

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ a_1 v_1 & a_2 v_2 & \cdots & a_{n-1} v_{n-1} & 0 \\ a_1^2 v_1 & a_2^2 v_2 & \cdots & a_{n-1}^2 v_{n-1} & 0 \\ \vdots & & & & \vdots \\ a_1^{k-1} v_1 & a_2^{k-1} v_2 & \cdots & a_{n-1}^{k-1} v_{n-1} & 1 \end{pmatrix}.$$

Definición 2.3.4. Sean $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, $v = (v_1, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, con $a_i \neq a_j$ para todo $i \neq j$. El código RSG de dimensión k es

$$RSG_k(a, v) = \{(v_1 f(a_1), \ldots, v_n f(a_n)) \ : \ f \in \mathbb{F}_q[x], \ \deg f \leq k-1\}.$$

Si β es un elemento generador del grupo multiplicativo $\mathbb{F}_q^*$ y $n = q - 1$, podemos considerar $a = (\beta, \beta^2, \ldots, \beta^n)$ y $v = (1, 1, \ldots, 1)$, de donde se obtiene que $RSG_k(a, v)$ es un código de Reed-Solomon.

La Proposición 2.3.3 establece que todos los códigos AG racionales sobre $\mathbb{F}_q$, cuya longitud n satisface que $n \leq q$, son códigos RSG. El recíproco también es cierto:

Proposición 2.3.5. *Todo código RSG puede representarse como un código AG racional.*

Parte II

Trabajo original

Capítulo 3

Códigos AG sigma-cíclicos

3.1. Definiciones y propiedades

En esta sección vamos a interpretar la condición de ciclicidad de un código AG sobre un cuerpo de funciones F, y analizar cómo cumplir esa condición a través del uso de automorfismos de F.

Recordemos que un código lineal es cíclico si es cerrado por permutaciones cíclicas de sus coordenadas; que estamos considerando cuerpos de funciones $F/\mathbb{F}_q$ en los cuales $\mathbb{F}_q$ es el cuerpo total de constantes; y que denotamos con $\mathbb{P}(F)$ al conjunto de lugares de F.

Sean $F/\mathbb{F}_q$ un cuerpo de funciones, $D = P_1 + \cdots + P_n \in \mathrm{Div}(F)$ un divisor formado por lugares P_i racionales y distintos, y $G \in \mathrm{Div}(F)$ un divisor tal que $\nu_{P_i}(G) = 0$ para todo $i = 1, \ldots, n$. Además, consideramos el espacio de Riemann-Roch asociado a G, que está dado por:

$$\mathcal{L}(G) = \{z \in F \ : \ (z) + G \geq 0\} \cup \{0\},$$

y un código AG asociado a los divisores D y G es:

$$\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) = \{(z(P_1), z(P_2), \ldots, z(P_n)) \ : \ z \in \mathcal{L}(G)\}.$$

En el caso de estos códigos AG, tendremos que $\mathcal{C}$ es cíclico si y solo si

$$(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) \in \mathcal{C} \quad \forall\, (u(P_1), \ldots, u(P_n)) \in \mathcal{C}.$$

Luego, $(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) \in \mathcal{C}$ si y solo si existe $v \in \mathcal{L}(G)$ tal que

$$(u(P_2), u(P_3), \ldots, u(P_n), u(P_1)) = (v(P_1), v(P_2), \ldots, v(P_{n-1}), v(P_n)).$$

Así, podemos determinar que $\mathcal{C}$ es cíclico si hallamos un elemento $v \in \mathcal{L}(G)$, para cada $u \in \mathcal{L}(G)$, que satisfaga el siguiente sistema:

$$\begin{cases} v(P_1) & = & u(P_2), \\ v(P_2) & = & u(P_3), \\ & \vdots & \\ v(P_{n-1}) & = & u(P_n), \\ v(P_n) & = & u(P_1). \end{cases} \tag{3.1}$$

Recíprocamente, si $\mathcal{C}$ es cíclico y $u \in \mathcal{L}(G)$, podemos estudiar si existe alguna regla general para hallar $v \in \mathcal{L}(G)$ que satisfaga (3.1).

Como un primer acercamiento a entender los códigos AG cíclicos, vamos a presentar ciertas condiciones relacionadas con un automorfismo que nos garantizan ciclicidad.

En primer lugar, recordando la Definición 1.6.3 que indica que si F'/F es una extensión de cuerpos de funciones, P' es un lugar de F' y P es un lugar de F, entonces denotamos por $P'|P$ al hecho de que $P = P' \cap F$. Tenemos algunos resultados básicos acerca de extensiones de cuerpos e isomorfismos, que pueden encontrarse en el Lema 3.5.2 y el Teorema 3.7.1 de [16].

Lema 3.1.1. *Sean F/K un cuerpo de funciones, H, H' extensiones de F, $\sigma : H \to H'$ un K-isomorfismo y $F' = \sigma(F)$. Tenemos que:*

1. *Si Q es un lugar de H, entonces $\sigma(Q) = \{\sigma(x) \ : \ x \in Q\}$ es un lugar de H' y se tiene que $\sigma(\mathcal{O}_Q) = \mathcal{O}_{\sigma(Q)}$. Además,* $\deg \sigma(Q) = \deg Q$.

2. *Si $0 \neq z \in H'$, entonces $\nu_{\sigma(Q)}(z) = \nu_Q\left(\sigma^{-1}(z)\right)$.*

3. *Si Q es un lugar de H y P es un lugar de F tales que $Q|P$, entonces $\sigma(Q)|\sigma(P)$ y además $e(\sigma(Q)|\sigma(P)) = e(Q|P)$ y $f(\sigma(Q)|\sigma(P)) = f(Q|P)$.*

4. *La acción de σ sobre $\mathbb{P}(H)$ se extiende naturalmente a una acción sobre* $\mathrm{Div}(H)$ *por linealidad.*

5. *Si H/F es una extensión de Galois, entonces* $\mathrm{Gal}(H/F)$ *actúa transitivamente en el conjunto $\mathbb{P}(H)$. Es decir, para cada par de lugares $P, Q \in \mathbb{P}(H)$ que satisfacen $P \cap F = Q \cap F$, existe $\tau \in \mathrm{Gal}(H/F)$ tal que $\tau(P) = Q$.*

Observación 3.1.2. Es sabido que $\mathrm{Aut}_{\mathbb{F}_q}(F)$ es un grupo finito. Además, la acción sobre el grupo de divisores puede escribirse como

$$\sigma\left(\sum_P a_P P\right) = \sum_P a_P \sigma(P).$$

Así, para cualquier código AG definido sobre F, $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$, con $D = P_1 + \cdots + P_n$, donde cada P_i es un lugar racional de F, y para cualquier $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ tenemos un código AG dado por $\mathcal{C}^\sigma = \mathcal{C}_{\mathcal{L}}(\sigma(D), \sigma(G))$. Notar que $\mathcal{C}^\sigma$ está bien definido pues $\nu_{P_i}(G) = 0$ para todo $i = 1, \ldots, n$ y, por el lema anterior, cada lugar $\sigma(P_i)$ es racional, de donde obtenemos que

$$\nu_{\sigma(P_i)}(\sigma(G)) = \nu_{P_i}(\sigma^{-1}(\sigma(G))) = \nu_{P_i}(G) = 0 \quad \forall\, i = 1, \ldots, n.$$

Notemos que si $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ satisface que $\sigma(D) = D$ y $\sigma(G) = G$, entonces $\mathcal{C}^\sigma = \mathcal{C}$.

Lema 3.1.3. *Si $G \in \mathrm{Div}(F)$ y $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ satisfacen $\sigma(G) = G$, entonces:*

$$z \in \mathcal{L}(G) \quad \Leftrightarrow \quad \sigma^{-1}(z) \in \mathcal{L}(G). \tag{3.2}$$

Demostración. Si Q es un lugar cualquiera y $P = \sigma(Q)$, entonces tenemos que

$$\nu_Q(\sigma^{-1}(z)) + \nu_Q(G) = \nu_{\sigma(Q)}(z) + \nu_{\sigma(Q)}(\sigma(G)) = \nu_{\sigma(Q)}(z) + \nu_{\sigma(Q)}(G) = \nu_P(z) + \nu_P(G).$$

Es decir que $\nu_Q(\sigma^{-1}(z)) + \nu_Q(G) = \nu_P(z) + \nu_P(G)$. Luego, es inmediata la aserción planteada. □

Observación 3.1.4. Del lema anterior, se obtiene que si $\sigma(G) = G$, entonces

$$\mathcal{L}(G) = \sigma(\mathcal{L}(G)) = \sigma^{-1}(\mathcal{L}(G)).$$

De (3.2), tenemos que si $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ satisface $\sigma(D) = D$ y $\sigma(G) = G$, a partir de una palabra código $(z(P_1), \ldots, z(P_n)) \in \mathcal{C}_{\mathcal{L}}(D, G)$, tenemos otra palabra código, dada por

$$\sigma \cdot (z(P_1), \ldots, z(P_n)) = ((\sigma^{-1}(z))(P_1), \ldots, (\sigma^{-1}(z))(P_n)).$$

El mapeo $z(\sigma(P)) \mapsto (\sigma^{-1}(z))(P)$ define un isomorfismo entre los cuerpos de clases residuales $F_{\sigma(P)} = \mathcal{O}_{\sigma(P)}/\sigma(P)$ y $F_P = \mathcal{O}_P/P$, para cualquier lugar P y cualquier $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$, usando la Proposición 8.2.3 de [16]. Podemos considerar entonces

$$z(\sigma(P)) = (\sigma^{-1}(z))(P). \tag{3.3}$$

La condición $\sigma(D) = D$ implica que $\sigma \cdot (z(P_1), \ldots, z(P_n))$ es una permutación de la palabra $(z(P_1), \ldots, z(P_n))$.

Dicho todo esto, es natural considerar el siguiente grupo, fijados los divisores D y G:

$$\mathrm{Aut}_{D,G}(F) = \{\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F) \,:\, \sigma(D) = D \ \text{ y } \ \sigma(G) = G\}. \tag{3.4}$$

A continuación, vamos a presentar una manera de construir códigos AG cíclicos, que luego denominaremos método sigma, y será fundamental a lo largo de esta tesis.

Lema 3.1.5. *Sean $P_1, \ldots, P_n$ lugares racionales diferentes de un cuerpo de funciones F sobre $\mathbb{F}_q$, y G un divisor tal que $\nu_{P_i}(G) = 0$ para todo $i = 1, \ldots, n$. Consideremos el divisor $D = P_1 + \cdots + P_n$ y supongamos que existe $\sigma \in \mathrm{Aut}_{D,G}(F)$ tal que*

$$\sigma(P_1) = P_2, \ \ldots, \ \sigma(P_{n-1}) = P_n, \ \sigma(P_n) = P_1. \tag{3.5}$$

Entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código AG cíclico, el orden de σ como elemento de $\mathrm{Aut}_{\mathbb{F}_q}(F)$ es divisible por n y, además, n es el menor entero positivo tal que $\sigma^n(P_1) = P_1$.

Demostración. Recordemos de (3.1) que $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ es cíclico si y solo si para cada $u \in \mathcal{L}(G)$ existe $v \in \mathcal{L}(G)$ tal que

$$v(P_i) = u(P_{i+1 \mod n}), \qquad 1 \leq i \leq n.$$

Supongamos ahora que $\sigma \in \mathrm{Aut}_{D,G}(F)$ satisface (3.5). Para cada $u \in \mathcal{L}(G)$ podemos considerar el elemento $v = \sigma^{-1}(u)$, que pertenece a $\mathcal{L}(G)$ por (3.2) y satisface (3.1). Además, por (3.3),

$$v(P_i) = \big(\sigma^{-1}(u)\big)(P_i) = u(\sigma(P_i)) = u(P_{i+1 \mod n}),$$

para cada $1 \leq i \leq n$, y entonces $\mathcal{C}$ es un código AG cíclico.

Sea m el orden de σ en el grupo $\mathrm{Aut}_{\mathbb{F}_q}(F)$. Luego, $\sigma^m = id$ y tenemos que $\sigma^m(P) = P$ para cualquier lugar P de F. Por otro lado, notemos que

$$\begin{aligned} P_2 &= \sigma(P_1), \\ P_3 &= \sigma^2(P_1), \\ &\vdots \\ P_n &= \sigma^{n-1}(P_1), \\ P_1 &= \sigma^n(P_1). \end{aligned}$$

En particular, $\sigma^{nk}(P_1) = P_1$ para cualquier $k \in \mathbb{N}$. Si $m < n$, entonces resulta que $P_1 = \sigma^m(P_1) = P_{m+1}$, por lo que $P_1 \in \{P_2, \ldots, P_n\}$, lo cual contradice la hipótesis de que los lugares $P_1, \ldots, P_n$ son n lugares distintos. Así $m \geq n$ y deben existir únicos enteros $k \geq 1$ y $r \geq 0$ tales que $m = kn + r$, con $0 \leq r \leq n-1$. Si suponemos que $r \neq 0$, entonces $1 \leq r \leq n-1$ y

$$P_1 = \sigma^m(P_1) = \sigma^{r+kn}(P_1) = \sigma^r(\sigma^{nk}(P_1)) = \sigma^r(P_1) = P_{r+1},$$

de donde obtenemos que $P_1 \in \{P_2, \ldots, P_n\}$, pero esto no es posible. Por lo tanto $r = 0$ y $m = kn$. Finalmente, de la misma manera, obtenemos que no es posible que $\sigma^j(P_1) = P_1$ para ningún número entero positivo $j < n$. □

Observación 3.1.6. Lo que nos dice el Lema 3.1.5 es que si un elemento σ de $\mathrm{Aut}_{D,G}(F)$ permuta cíclicamente los lugares del divisor D, entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código cíclico.

Así, podemos dar la siguiente definición:

Definición 3.1.7. Sea $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ un código AG definido sobre un cuerpo de funciones F sobre $\mathbb{F}_q$, con $D = P_1 + \cdots + P_n$. Decimos que $\mathcal{C}$ es sigma-cíclico si es un código cíclico y además existe $\sigma \in \mathrm{Aut}_{D,G}(F)$ que satisface (3.5).

Vamos a utilizar las condiciones (3.5) descriptas en el Lema 3.1.5 para enunciar un método, que llamaremos método sigma, mediante el cual vamos a construir códigos AG cíclicos. Consideremos un cuerpo de funciones F sobre $\mathbb{F}_q$ y un automorfismo $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ de orden m. Para un lugar P de F vamos a denotar con $[P]_\sigma$ a la órbita definida por la acción del subgrupo cíclico $\langle\sigma\rangle$ of $\mathrm{Aut}_{\mathbb{F}_q}(F)$ generado por σ sobre el conjunto de lugares de F, es decir

$$[P]_\sigma = \left\{\sigma(P), \sigma^2(P), \ldots, \sigma^m(P) = P\right\}.$$

Si consideramos los n lugares racionales $P_1, \ldots, P_n$ del Lema 3.1.5, tenemos la órbita $[P_1]_\sigma = \{P_1, \ldots, P_n\}$, con $\sigma \in \mathrm{Aut}_{D,G}(F)$ que satisface (3.5). Luego, se cumple que $m = nk$ donde k es el orden del llamado grupo de isotropía

$$\langle\sigma\rangle_{P_1} = \left\{\sigma^i \ : \ \sigma^i(P_1) = P_1\right\}.$$

Viendo la prueba del Lema 3.1.5, se obtiene que este grupo puede ser descripto explícitamente como $\langle\sigma\rangle_{P_1} = \{\sigma^{ik}\}_{i=1}^{n}$.

3.2. El método sigma

Vamos a describir los pasos a realizar para construir códigos sigma-cíclicos, dando lugar a lo que denominamos como método sigma:

1. Elegir $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ de orden $m \geq 2$ y un divisor G tal que $\sigma(G) = G$.

2. Hallar un lugar racional P de F tal que $P \notin \mathrm{sop}(G)$ y $\sigma(P) \neq P$ (si $\sigma(P) = P$, la órbita $[P]_\sigma$ es trivial, es decir, $[P]_\sigma = \{P\}$).

3. Calcular el orden k del grupo de isotropía $\langle\sigma\rangle_P$.

4. Si $n = m/k$, tenemos que n es el divisor de m más pequeño tal que $\sigma^n(P) = P$. Así, los lugares $P, \sigma(P), \sigma^2(P), \ldots, \sigma^{n-1}(P)$ son n lugares racionales distintos de F y

$$[P]_\sigma = \left\{P, \sigma(P), \sigma^2(P), \ldots, \sigma^{n-1}(P)\right\}. \tag{3.6}$$

5. Consideramos el divisor $D = P + \sigma(P) + \cdots + \sigma^{n-1}(P)$, que tiene soporte disjunto con el soporte de G.

6. $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código AG sigma-cíclico sobre $\mathbb{F}_q$, ya que escribiendo $P_1 = P$ y $P_{i+1} = \sigma^i(P)$ para $i = 1, \ldots, n-1$, se satisfacen las condiciones del Lema 3.1.5.

Observación 3.2.1. La longitud de un código sigma-cíclico construido con el método sigma depende del tamaño de la órbita (3.6), pero determinar tal tamaño equivale a encontrar el orden del grupo de isotropía $\langle\sigma\rangle_P$ o probar que n es el menor entero divisor de m tal que $\sigma^n(P) = P$. Estos cálculos representan la mayor dificultad del método.

Uno de los contextos más favorables para aplicar el método es el cuerpo de funciones racionales $F = \mathbb{F}_q(x)$, no solamente por conocer el grupo de automorfismos $\mathrm{Aut}_{\mathbb{F}_q}(F)$, sino también por lo sencillo de describir sus lugares racionales. Además, gracias al trabajo de López y Nart [9], conocemos el tamaño de las órbitas en cuestión. Usaremos todas estas ventajas en las secciones 4.1 y 4.2.

3.3. Ejemplos

Para comenzar a trabajar en el caso del cuerpo de funciones racionales, presentamos una versión más explícita del Lema 3.1.5, que nos permitirá dar algunos ejemplos simples de códigos AG sigma-cíclicos.

Recordemos que si $F = \mathbb{F}_q(x)$, es usual denotar con P_α al lugar de F que es el único cero de $x-\alpha$, para cada $\alpha \in \mathbb{F}_q$, y con P_∞ al único polo de x. También sabemos que éstos son los únicos lugares racionales de F. En este contexto, tenemos el siguiente resultado:

Lema 3.3.1. *Sean $\alpha_1, \ldots, \alpha_n, \beta \in \mathbb{F}_q$ diferentes entre sí. Supongamos que existe un automorfismo $\sigma \in \mathrm{Aut}(\mathbb{F}_q(x))$ tal que*

$$\sigma(x-\alpha_i) \in P_{\alpha_{i+1}} \mod n, \qquad \sigma(x-\beta) \in P_\beta, \qquad y \qquad \sigma(x^{-1}) \in P_\infty. \tag{3.7}$$

Entonces el código $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$ con

$$D = P_{\alpha_1} + \cdots + P_{\alpha_n} \qquad y \qquad G = rP_\beta + sP_\infty, \quad r,s \in \mathbb{Z},$$

es un código AG sigma-cíclico de longitud n sobre $\mathbb{F}_q$. Además, si $0 < r+s < n$, tenemos que $\mathcal{C}$ es un código MDS no trivial con $k = r+s+1$ y $d = n-(r+s)$.

Demostración. Es claro que D y G son divisores disjuntos, y además (3.7) implica que

$$\sigma(P_{\alpha_i}) = P_{\alpha_{i+1}} (1 \le i \le n-1), \quad \sigma(P_{\alpha_n}) = P_{\alpha_1}, \quad \sigma(P_\beta) = P_\beta, \quad \text{y} \quad \sigma(P_\infty) = P_\infty.$$

Luego, $\sigma(D) = D$ y $\sigma(G) = G$. Así, por el Lema 3.1.5, $\mathcal{C}$ es cíclico. Por último, usando la Proposición 2.3.2, obtenemos que el código es MDS, con $k = r+s+1$ y $d = n-(r+s)$. □

Veamos algunos ejemplos de códigos sigma-cíclicos racionales.

Ejemplo 3.3.2 (Raíces de la unidad). Sean q una potencia de un número primo, y $n \ge 2$ un divisor de $q-1$. Luego, $\mathbb{F}_q$ contiene una raíz n-ésima primitiva de la unidad ω y x^n-1 se factoriza en n factores lineales

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1})$$

en $\mathbb{F}_q[x]$. Esta factorización nos induce n lugares racionales $P_1, P_\omega, \ldots, P_{\omega^{n-1}}$ de $\mathbb{F}_q(x)$. Sea $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ dado por

$$\sigma(x) = \omega^{-1}x \qquad \text{y} \qquad \sigma(a) = a, \quad a \in \mathbb{F}_q. \tag{3.8}$$

Notemos que $\sigma(x) \in P_0$ y además

$$\sigma(x-\omega^i) = \sigma(x) - \sigma(\omega^i) = \omega^{-1}x - \omega^i = \omega^{-1}(x-\omega^{i+1}).$$

Así, $\sigma(x-\omega^i) \in P_{\omega^{i+1}}$ para todo $1 \leq i \leq n$. Tomando $\alpha_i = \omega^{i-1}$ para $i = 1, \ldots, n$, obtenemos que $\sigma(P_{\alpha_i}) = P_{\alpha_{i+1}}$ para $i = 1, \ldots, n$, $\sigma(P_0) = P_0$ y $\sigma(P_\infty) = P_\infty$. Por lo tanto, $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ con $D = P_{\alpha_1} + \cdots + P_{\alpha_n}$, $G = rP_0 + sP_\infty$ y $r, s \in \mathbb{Z}$, es un código AG sigma-cíclico sobre $\mathbb{F}_q$ de longitud n, usando el Lema 3.3.1. ◊

Ejemplo 3.3.3 (Polinomio de Artin-Schreier). Consideremos el polinomio $f(x) = x^p - x - a$ en $\mathbb{F}_q[x]$, donde $p = \mathrm{Char}(\mathbb{F}_q)$. Sea $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_p$ y tomemos $a = \alpha^p - \alpha$ (notemos que $a \neq 0$). Luego, α es una raíz de $x^p - x - a$. Además, $\alpha + 1$ también es raíz de f, pues

$$f(\alpha+1) = (\alpha+1)^p - \alpha - 1 - a = \alpha^p + 1 - \alpha - 1 - a = 0.$$

Así, podemos obtener que

$$x^p - x - a = (x-\alpha)(x-(\alpha+1)) \cdots (x-(\alpha+p-1)).$$

Consideremos el automorfismo dado por

$$\sigma(x) = x - 1.$$

Denotando $\alpha_i = \alpha + i - 1$ para $i = 1, \ldots, p$, tenemos que $\sigma(P_{\alpha_i}) = P_{\alpha_{i+1}}$ para $i = 1, \ldots, p$ y $\sigma(P_\infty) = P_\infty$. Si consideramos $D = P_{\alpha_1} + \cdots + P_{\alpha_p}$ y $G = sP_\infty$ con $s \in \mathbb{N}$, por el Lema 3.1.5, el código $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ es un código sigma-cíclico de longitud prima p. ◊

Veamos ahora un ejemplo sobre un cuerpo de funciones no racional. Usaremos el cuerpo de funciones hermitiano $H = \mathbb{F}_{q^2}(x, y)$ descripto en la Sección 8.3 de [16].

Ejemplo 3.3.4 (Cuerpo de funciones hermitiano). Sea $H = \mathbb{F}_{q^2}(x, y)$ el cuerpo de funciones hermitiano, visto como una extensión abeliana de grado q de $\mathbb{F}_{q^2}(x)$, definida por la ecuación

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

De la Sección 8.3 de [16] sabemos que, para cada $\alpha \in \mathbb{F}_{q^2}$ y cada $\beta \in \mathbb{F}_{q^2}$ que satisface la igualdad $\beta^q + \beta = \alpha^{q+1}$, existe un lugar racional $P_{\alpha,\beta}$ de H arriba del lugar racional P_α de $\mathbb{F}_{q^2}(x)$ y, además, los lugares $P_{\alpha,\beta}$ son todos los lugares de H que están arriba de P_α.

Más aún, $x-\alpha, y-\beta \in P_{\alpha,\beta}$, existe un único lugar Q_∞ de H que es polo de x y de y en H, y para cualquier elemento no nulo $a \in \mathbb{F}_{q^2}$, existe un automorfismo $\sigma_a \in \mathrm{Aut}_{\mathbb{F}_{q^2}}(H)$ tal que $\sigma_a(Q_\infty) = Q_\infty$ y

$$\sigma_a(x) = ax \quad \text{y} \quad \sigma_a(y) = a^{q+1}y.$$

Notemos que

$$\sigma_a^n(x) = a^n x \quad \text{y} \quad \sigma_a^n(y) = a^{nq+n}y,$$

para cualquier $n \in \mathbb{N}$. Así, el orden de σ_a, como elemento del grupo $\mathrm{Aut}_{\mathbb{F}_{q^2}}(H)$, es el mismo que el orden de a como elemento del grupo multiplicativo $\mathbb{F}_{q^2}^*$. Si $a \in \mathbb{F}_{q^2}\backslash\{0,1\}$, tenemos que σ_a es un $\mathbb{F}_{q^2}$-automorfismo de H de orden $m \geq 2$.

Por otro lado, el polinomio $T^q + T - 1$ se descompone en factores lineales en $\mathbb{F}_{q^2}[T]$, entonces, para cada $\beta \in \mathbb{F}_{q^2}$ tal que $\beta^q + \beta = 1$, el lugar $P_{1,\beta}$ es un lugar racional de H que está arriba del lugar P_1 de $\mathbb{F}_{q^2}(x)$. Supongamos que $a \in \mathbb{F}_{q^2} - \{0,1\}$ satisface $\sigma_a(P_{1,\beta}) = P_{1,\beta}$, para algún $\beta \in \mathbb{F}_{q^2}$ tal que $\beta^q + \beta = 1$, entonces $x-1, ax-1 \in P_{1,\beta}$ y esto implica que $(a-1)x \in P_{1,\beta}$. Como $a-1 \neq 0$, obtenemos que $P_{1,\beta}$ está arriba de P_0, contradiciendo el hecho de que $P_{1,\beta}$ está arriba de P_1. Luego, tenemos que $\sigma(P_{1,\beta}) \neq P_{1,\beta}$ para todo $\beta \in \mathbb{F}_{q^2}$ que satisfaga $\beta^q + \beta = 1$, y para todo $a \in \mathbb{F}_{q^2}\backslash\{0,1\}$.

Ahora, podemos aplicar el método sigma para obtener códigos sigma-cíclicos con el automorfismo σ_a de H, cuyo orden es $m \geq 2$, asociado a algún elemento $a \in \mathbb{F}_{q^2}\backslash\{0,1\}$, y considerando los divisores $G = rQ_\infty$ y $D = P + \sigma_a(P) + \cdots + \sigma_a^{n-1}(P)$, donde n es el menor entero que divide a m y satisface $\sigma_a^n(P) = P$, tomando $P = P_{1,\beta}$ para algún $\beta \in \mathbb{F}_{q^2}$ con $\beta^q + \beta = 1$.

Veamos que, en este caso, $n = m$. En efecto, sea n el menor divisor de m que verifica $\sigma_a^n(P_{1,\beta}) = P_{1,\beta}$. Entonces $x-1, a^n x - 1 \in P_{1,\beta}$ y esto implica que $(a^n-1)x \in P_{1,\beta}$. La única posibilidad es que $a^n - 1 = 0$ (de otro modo, el lugar $P_{1,\beta}$ estaría arriba de P_0, lo cual no es posible) y entonces $n = m$. Por lo tanto, hemos construido un código AG sigma-cíclico con respecto al automorfismo σ_a, de longitud m, donde m es el orden de a como elemento del grupo multiplicativo $\mathbb{F}_{q^2}^*$. En particular, si a es un generador de $\mathbb{F}_{q^2}^*$, obtenemos un código AG sigma-cíclico de longitud $q^2 - 1$. $\Diamond$

3.4. Extensiones cíclicas

Hasta ahora, hemos presentado ejemplos de códigos sigma-cíclicos construidos en cuerpos de funciones. En lo que sigue vamos a considerar extensiones de cuerpos de funciones, en particular, extensiones cíclicas F'/F de cuerpos de funciones sobre $\mathbb{F}_q$ y el subgrupo $\mathrm{Gal}(F'/F)$ de $\mathrm{Aut}_{\mathbb{F}_q}(F')$. Primeramente, veamos un resultado acerca de cómo construir códigos sigma-cíclicos a partir de extensiones cíclicas.

Proposición 3.4.1. *Sean F'/F una extensión cíclica de grado m de cuerpos de funciones sobre $\mathbb{F}_q$. Sea P un lugar de F y sean $P_1, \ldots, P_n$ todos los lugares de F' que están arriba de P. Entonces n divide a m y para cualquier generador σ de $\mathrm{Gal}(F'/F)$ tenemos que la órbita de P_1 es*

$$[P_1]_\sigma = \{P_1, \ldots, P_n\}.$$

Más aún, sea $Q \neq P$ un lugar de F y sea $G = Q_1 + \cdots + Q_k$ un divisor de F' formado por todos los lugares de F' que están arriba de Q. Entonces $\sigma(G) = G$ y $\mathrm{sop}(G) \cap \mathrm{sop}(D) = \emptyset$, donde $D = P_1 + \cdots + P_n$. En particular, si algún P_i es racional, entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código sigma-cíclico.

Demostración. Supongamos que F'/F es una extensión cíclica de grado m y sea σ un generador del grupo de Galois $\mathcal{G} = \mathrm{Gal}(F'/F)$. Primero, notemos que $n \mid m$, pues $nef = m$, donde $e = e(P_i \,|\, P)$ y $f = f(P_i \,|\, P)$ son el índice de ramificación y el grado de inercia, respectivamente, para $i = 1, \ldots, n$, debido a que la extensión es de Galois.

Veamos ahora que la órbita $[P_1]_\sigma$ consiste de los lugares $P_1, \ldots, P_n$. Consideremos el grupo de descomposición

$$D(P_1 \,|\, P) = \{\sigma \in \mathcal{G} : \sigma(P_1) = P_1\}$$

de P_1 sobre P. Si $\sigma^i(P_1) = \sigma^j(P_1)$ para algunos valores $1 \leq i < j \leq n$, entonces tenemos que $\sigma^k \in D(P_1 \,|\, P)$, para $k = j - i > 0$. Como $D(P_1 \,|\, P)$ es un grupo de orden ef, tenemos que $\sigma^{kef} = id$, el elemento identidad de $\mathrm{Gal}(F'/F)$. Pero $k < n$, por lo que $kef < nef = m$, contradiciendo que m es el orden de σ. Por lo tanto, el conjunto $\{\sigma^i(P_1)\}_{i=1}^n$ consiste de n lugares diferentes de F' que están arriba de P, es decir que

$$\{\sigma(P_1), \sigma^2(P_1), \ldots, \sigma^n(P_1)\} = \{P_1, P_2, \ldots, P_n\}.$$

Esto significa que $\sigma^j(P_1) = P_1$ para algún $1 \leq j \leq n$. Pero por el argumento anterior, no es posible que $1 \leq j \leq n-1$, y entonces $\sigma^n(P_1) = P_1$.

Por otro lado, tenemos que $\sigma(G) = G$ y además $\mathrm{sop}(G) \cap \mathrm{sop}(D) = \emptyset$, por la elección de los divisores D y G, y si algún P_i es racional, entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código AG sigma-cíclico. Esto se debe a que, al ser una extensión de Galois, si algún P_i es racional, entonces todos lo son. □

En el siguiente ejemplo, y también más adelante, se hace mención a un resultado muy importante llamado Teorema de Kummer, cuyo enunciado requiere una serie de definiciones que no están directamente relacionadas con lo presentado en esta tesis. Puede leerse en el Teorema 3.3.7 de [16], de donde también se destaca el Corolario 3.3.8, asociado al Teorema de Kummer.

Ejemplo 3.4.2 (Códigos sigma-cíclicos sobre una extensión de Kummer). Consideremos el cuerpo de funciones racionales $F = \mathbb{F}_q(x)$ y una extensión de Kummer $F' = F(y)$ dada por

$$y^n = (x - \alpha)(x - \alpha^{-1}),$$

donde $n \mid q-1$, $\alpha \in \mathbb{F}_q^*$ y $\alpha \neq \alpha^{-1}$. Por la Proposición 6.3.1 en [16] sabemos que F'/F es una extensión cíclica de grado n y que $\mathbb{F}_q$ es el cuerpo total de constantes de F'. Además, los lugares P_α y $P_{\alpha^{-1}}$, ceros de $x - \alpha$ y $x - \alpha^{-1}$ en F respectivamente, son totalmente ramificados en F'/F.

Por otro lado, podemos ver que P_0, el cero de x en F, se descompone completamente en F'. Sea

$$\varphi(T) = T^n - (x - \alpha)(x - \alpha^{-1}) \in \mathbb{F}_q(x)[T]$$

y sea $\bar{\varphi}(T)$ su reducción módulo P_0. Como $x(P_0) = 0$ y $n \mid q-1$, tenemos que

$$\bar{\varphi}(T) = T^n - 1 = \prod_{i=1}^{n} (T - a_i) \in \mathbb{F}_q[T]\,.$$

Luego, por el Teorema de Kummer, P_0 se descompone completamente en F'.

Consideremos ahora el divisor $D = P_1 + \cdots + P_n$, donde $P_1, \ldots, P_n$ son todos los lugares de F' arriba de P_0, y el divisor $G = rQ_\alpha$, donde r es un entero positivo y Q_α es el único lugar de F' arriba de P_α. Por la Proposición 3.4.1 tenemos que $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ es sigma-cíclico.

Más aún, podemos presentar cotas para los parámetros $[n, k, d]$ de $\mathcal{C}$. Se sabe que el género g de F' es $g = \lfloor \frac{n-1}{2} \rfloor$. Si tomamos $0 < r < n$, d y k satisfacen lo siguiente:

$$d \geq n - r \qquad \text{y} \qquad k \geq r + 1 - \lfloor \tfrac{n-1}{2} \rfloor,$$

según el Corolario 2.2.3. ◊

Ejemplo 3.4.3 (Códigos sigma-cíclicos sobre una extensión de Artin-Schreier). Sea p un número primo impar. Consideremos la extensión de Artin-Schreier $F'/\mathbb{F}_p(x)$, donde la extensión $F' = \mathbb{F}_p(x, y)$ está generada por la ecuación

$$y^p - y = x^2.$$

De la Proposición 3.7.8 de [14] tenemos que F' es una extensión cíclica de $F = \mathbb{F}_p(x)$ de grado p, el lugar P_∞, el polo de x en F, es totalmente ramificado en F', y cualquier otro lugar de $\mathbb{F}_p(x)$ es no ramificado en F'. Usando que

$$T^p - T = T^p - T - x \mod P_0$$

obtenemos, por el Teorema de Kummer, que P_0 se descompone completamente en F' en p lugares racionales $P_1, \ldots, P_p$.

Si consideramos los divisores $D = P_1 + \cdots + P_p$ y $G = rQ$, donde Q es el único lugar de F' arriba de P_∞, y $1 \leq r \leq p - 1$, entonces por la Proposición 3.4.1 $\mathcal{C}_\mathcal{L}(D, G)$ es sigma-cíclico. Usando que el género de F' es $g = \frac{1}{2}(p - 1)$, del Corolario 2.2.3 tenemos que

$$d \geq p - r \qquad \text{y} \qquad k \geq r + 1 - \tfrac{p-1}{2}.$$

Notemos que r deberá cumplir $\frac{1}{2}(p - 3) \leq r \leq p - 1$ para tener dimensión positiva. ◊

Como consecuencia del Lema 3.1.5 y la Proposición 3.4.1, tenemos el siguiente resultado:

Corolario 3.4.4. *Sea F'/F una extensión de Galois de grado n de cuerpos de funciones sobre $\mathbb{F}_q$. Sean $P_1, \ldots, P_n$ diferentes lugares racionales de F'. Supongamos que (3.5) se cumple con los lugares $P_1, \ldots, P_n$ para algún $\sigma \in \mathrm{Gal}(F'/F)$. Entonces la extensión F'/F es cíclica, σ genera a $\mathrm{Gal}(F'/F)$, y existe un lugar $P \in \mathbb{P}(F)$ que se descompone en F'*

en los lugares $P_1, \ldots, P_n$*. Recíprocamente, si* F'/F *es cíclica y algún lugar* $P \in \mathbb{P}(F)$ *se descompone en* F' *en los lugares* $P_1, \ldots, P_n$*, entonces* (3.5) *se cumple para esos lugares y cualquier generador* σ *de* $\mathrm{Gal}(F'/F)$*.*

Demostración. Sea $\sigma \in \mathrm{Gal}(F'/F)$ tal que (3.5) se satisface para los n lugares $P_1, \ldots, P_n$. Por el Lema 3.1.5, tenemos que n divide al orden de σ. Como $\mathrm{Gal}(F'/F)$ es un grupo de orden n, tenemos que σ genera a $\mathrm{Gal}(F'/F)$ y entonces F'/F es una extensión cíclica. Si P es un lugar de F que está abajo de P_1, como σ restringido a F es el automorfismo identidad, todo lugar en la órbita $[P_1]_\sigma$ está arriba de P. Pero, por hipótesis, $[P_1]_\sigma = \{P_1, \ldots, P_n\}$, por lo que todo lugar P_i está arriba de P, para $i = 1, \ldots, n$, y esto significa que P se descompone completamente en F'.

La implicación recíproca es consecuencia directa de la Proposición 3.4.1. □

Tanto en los ejemplos como en los resultados anteriores de esta sección estamos considerando extensiones de Galois y automorfismos del grupo de Galois asociado. Nos proponemos ahora considerar automorfismos del grupo $\mathrm{Aut}_{\mathbb{F}_q}(F)$, para analizar qué podemos decir al respecto sobre F y algunas subextenciones asociadas a F.

Proposición 3.4.5. *Sean* F *un cuerpo de funciones sobre* $\mathbb{F}_q$ *y* $P_1, \ldots, P_n$ *lugares diferentes de* F*. Supongamos que existe un automorfismo* $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ *de orden* m *que satisface* (3.5)*. Entonces* n *divide a* m *y existen un subcuerpo* E *de* F *y un lugar* P *de* E *tales que* F/E *es una extensión cíclica de grado* m *y* P *se descompone en* F *en los lugares* $P_1, \ldots, P_n$*, cumpliendo que*

$$e(P_i|P)f(P_i|P) = \frac{m}{n} \quad \text{para } i = 1, \ldots, n. \tag{3.9}$$

Demostración. Consideremos el subgrupo $G = \langle\sigma\rangle$ generado por σ de $\mathrm{Aut}_{\mathbb{F}_q}(F)$ y el cuerpo fijo por el grupo G, $E = F^G$. Por el Teorema 11.36 de [7], tenemos que F/E es una extensión cíclica de grado m con grupo de Galois $\mathrm{Gal}(F/E) = \langle\sigma\rangle = G$.

Además, $P = P_1 \cap E$ es un lugar de E, y por (3.5) obtenemos que $P = P - i \cap E$ para cualquier $i = 1, \ldots, n$. Ahora bien, como G actúa transitivamente en los lugares de F que están arriba de P, tenemos que $P_1, \ldots, P_n$ son todos los lugares de F arriba de P, y no hay otros.

Finalmente, por la igualdad fundamental (Teorema 1.6.8):

$$m = [F : E] = \sum_{i=1}^{n} e(P_i|P) f(P_i|P) = nef,$$

donde $e = e(P_i|P)$ y $f = f(P_i|P)$ son constantes por ser F/E una extensión de Galois. De aquí se deduce (3.9). □

Notemos que en la proposición previa no necesariamente se cumple que $\mathbb{F}_q(x)$ sea un subcuerpo de E. A continuación, veremos que, bajo ciertas hipótesis, podemos construir un cuerpo E de tal manera que $\mathbb{F}_q(x) \subset E \subsetneq F$, F/E sea cíclica y existan lugares $Q_1, \ldots, Q_d$ que se descompongan completamente en F en los lugares $P_1, \ldots, P_n$.

Teorema 3.4.6. *Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ que contiene al cuerpo de funciones racionales $\mathbb{F}_q(x)$. Sean $P_1, \ldots, P_n$ diferentes lugares de F. Sea $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ un automorfismo de orden m que satisface (3.5). Entonces:*

1. *n divide a m.*

2. *Existen un divisor k de n, un entero positivo d que divide tanto a m/k como a n y un cuerpo de funciones E sobre $\mathbb{F}_q$ tales que $\mathbb{F}_q(x) \subset E \subset F$ y F/E es cíclica. Además, existen lugares $Q_1, \ldots, Q_d$ de E que se descomponen completamente en F en los lugares $P_1, \ldots, P_n$.*

3. *Sean $y \in F$ tal que $F = \mathbb{F}_q(x, y)$ y $G = \langle \sigma \rangle$ el subgrupo generado por σ de $\mathrm{Aut}_{\mathbb{F}_q}(F)$. Si sucede que $\alpha x + y \notin F^G$ para todo $\alpha \in \mathbb{F}_q$, entonces la extensión cíclica F/E obtenida en el inciso anterior cumple que $E \subsetneq F$.*

Demostración. En la Figura 3.1 pueden verse los objetos involucrados en el teorema. Sea G el subgrupo cíclico de $\mathrm{Aut}_{\mathbb{F}_q}(F)$ generado por σ y sea $E' = F^G$, el cuerpo fijo de F por G. Por la Proposición 3.4.5 tenemos que el primer inciso es cierto, y también que F/E' es una extensión cíclica de grado m con grupo de Galois G. Más aún, si $P' = P_1 \cap E'$, entonces sucede que $P_1, \ldots, P_n$ son todos los lugares de F que están arriba de P' y además $e(P_i \,|\, P') f(P_i \,|\, P') = \frac{m}{n}$ para $i = 1, \ldots, n$.

Consideremos ahora la composición de cuerpos $E = E'\mathbb{F}_q(x)$. Como $E' \subset E \subset F$ y F/E' es una extensión cíclica con grupo de Galois G, tenemos que F/E también es una

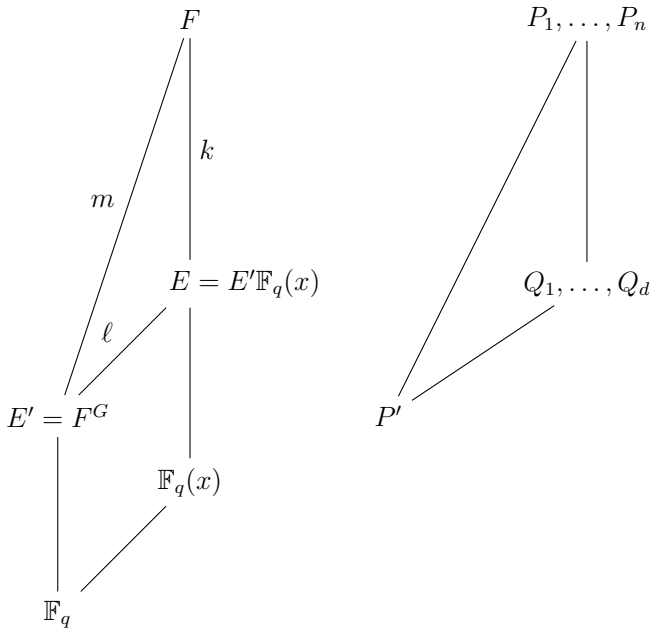

Figura 3.1: Diagrama de objetos del Teorema 3.4.6.

extensión cíclica con grupo de Galois T generado por $\tau = \sigma^\ell$ para algún divisor ℓ de m. Esto implica que $[F : E] = k$ donde $k\ell = m$.

Sean $Q_1, \ldots, Q_d$ todos los lugares de E que están abajo de los lugares $P_1, \ldots, P_n$. Como la órbita $[P_1]_\sigma$ es el conjunto $\{P_1, \ldots, P_n\}$ y F/E es una extención cíclica cuyo grupo de Galois está generado por $\tau = \sigma^\ell$, el conjunto de lugares de F que están arriba de cada Q_i es un subconjunto de $\{P_1, \ldots, P_n\}$ determinado por la órbita $[P_{j_i}]_\tau$, donde P_{j_i} está arriba de Q_i para algún $1 \leq j_i \leq n$. Notemos que k es la longitud de la órbita $[P_{j_i}]_\tau$, pues de otro modo $\sigma^s(P_{j_i}) = P_{j_i}$ para algún entero positivo $s < n$, contradiciendo que la longitud de $[P_1]_\sigma$ es n. Luego, tenemos que cada Q_i se descompone completamente en F y entonces $dk = n$. Resta probar que d es también un divisor de m/k. Ahora bien, como $Q_1, \ldots, Q_d$ son todos los lugares de E arriba de P', y como la extensión E/E' es cíclica de grado $\ell = m/k$, por la Proposición 3.4.1 deducimos que d divide a m/k.

Finalmente, veamos el inciso 3. Por el inciso 2 tenemos que $E' = F^G$ es una subextensión finita de F. Esto implica que existen elementos trascendentes $x_1, \ldots, x_r \in E'$ sobre $\mathbb{F}_q$ tales que $E' = \mathbb{F}_q(x_1, \ldots, x_r)$. Luego, podemos escribir

$$E = \mathbb{F}_q(x, x_1, \ldots, x_r).$$

Supongamos que $y \in E'$. Entonces $y = \alpha x + \sum_{i=1}^{r} \alpha_i x_i$ donde $\alpha, \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q$, y obtenemos que

$$y - \alpha x = \sum_{i=1}^{r} \alpha_i x_i \in E' = F^G,$$

contradiciendo la hipótesis. Por lo tanto $y \in F \backslash E'$ y esto implica que $E \subsetneq F$. □

Ejemplo 3.4.7 (Cuerpo de funciones hermitiano). Sea H el cuerpo de funciones hermitiano sobre $\mathbb{F}_{q^2}$ como en el Ejemplo 3.3.4, es decir $H = \mathbb{F}_{q^2}(x, y)$ donde $y^q + y = x^{q+1}$. Consideramos el automorfismo σ_a dado por $\sigma_a(x) = ax$ y $\sigma_a(y) = a^{q+1}y$, con $a \in \mathbb{F}_{q^2} \backslash \{0, 1\}$. Sean $G = \langle \sigma_a \rangle$ el grupo cíclico generado por σ_a y m el orden de a en el grupo multiplicativo $\mathbb{F}_{q^2}^*$.

Si $\alpha x + y \in H^G$ para algún $\alpha \in \mathbb{F}_{q^2}$, entonces para todo $i = 0, 1, \ldots, m-1$ tenemos que $\sigma_a^i(\alpha x + y) = \alpha x + y$. Luego:

$$\alpha a^i x + a^{iq+i} y = \alpha x + y,$$

de donde obtenemos que $\alpha\left(a^i - 1\right) x + \left(a^{iq+i} - 1\right) y = 0$. Ahora bien, como $a^i - 1 \neq 0$ y $a^{iq+i} - 1 \neq 0$, para todo $i = 1, \ldots, m-1$, sucede que

$$y = \begin{cases} 0 & \text{si } \alpha = 0 \\ \frac{\alpha\left(a^i - 1\right)}{1 - a^{iq+i}} x & \text{si } \alpha \neq 0 \end{cases},$$

pero esto significa que y es un elemento de $\mathbb{F}_{q^2}(x)$, lo cual es un absurdo.

Por lo tanto, $\alpha x + y \notin H^G$ para todo $\alpha \in \mathbb{F}_{q^2}$. ◊

Observación 3.4.8. Bajo las condiciones del Teorema 3.4.6, si $\sigma(x) = x$ y los lugares $P_1, \ldots, P_n$ son todos racionales, entonces podemos dar una descripción mucho más precisa. Por un lado, existen un cuerpo de funciones E sobre $\mathbb{F}_q$ y un lugar racional P' de E tales que $\mathbb{F}_q(x) \subset E \subset F$, F/E es cíclica de grado m y el lugar P' se descompone completamente en F en $P_1, \ldots, P_n$. Por otra parte, si $P'' = P' \cap \mathbb{F}_q(x)$, entonces P'' es racional y está totalmente ramificado en P'. Todo esto sucede debido a que, con la notación del teorema, $x \in E' = F^G$, de modo que $E = E'\mathbb{F}_q(x) = E'$.

3.5. Códigos L-cíclicos racionales

Consideremos el cuerpo de funciones racionales $F = \mathbb{F}_q(x)$ sobre el cuerpo finito $\mathbb{F}_q$, y un código $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ con divisores D y G adecuados, queremos estudiar el sistema (3.1) en este caso particular.

Sabemos, por la Proposición 1.2.1, que los lugares racionales de F son los ceros de los polinomios lineales $x - a$, para cada $a \in \mathbb{F}_q$, denotados por P_a, y el polo de x, denotado por P_∞. Consideremos un divisor $D = P_1 + \cdots + P_n$, donde $P_1, \ldots, P_n$ son n lugares racionales distintos y $P_i = P_{a_i}$ para algun $a_i \in \mathbb{F}_q$, y $G = rP_\infty$ para algún entero $r > 0$. En este caso es sabido que las funciones de clases residuales para lugares racionales corresponden a evaluar, es decir, $z(P_i) = z(a_i)$, por lo que el código AG asociado a los divisores D y G es

$$\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) = \{(u(a_1), \ldots, u(a_n)) \ : \ u \in \mathcal{L}(G)\}.$$

En este caso, $\mathcal{C}$ es cíclico si y solo si para cada $u \in \mathcal{L}(G)$ existe $v \in \mathcal{L}(G)$ tal que

$$\begin{cases} v(a_1) & = & u(a_2) \\ v(a_2) & = & u(a_3) \\ & \vdots & \\ v(a_{n-1}) & = & u(a_n) \\ v(a_n) & = & u(a_1) \end{cases} \tag{3.10}$$

Queremos determinar si v puede hallarse a partir de u, y bajo qué condiciones podemos asegurar que $\mathcal{C}$ es cíclico, más allá de los códigos sigma-cíclicos que ya hemos estudiado.

Notemos que el espacio de Riemann-Roch $\mathcal{L}(G)$ coincide con los polinomios de grado a lo sumo r, pues ningún polinomio mónico irreducible puede dividir a elementos de $\mathcal{L}(G)$ y $\nu_{P_\infty}(f/g) = \deg g - \deg f$; en efecto:

$$\begin{aligned} \mathcal{L}(G) &= \{z \in F \ : \ (z) + G \geq 0\} \cup \{0\} \\ &= \{z \in F \ : \ (z) + rP_\infty \geq 0\} \cup \{0\} \\ &= \{z \in F \ : \ \nu_P(z) \geq 0 \ \forall P \neq P_\infty, \ \nu_{P_\infty}(z) \geq -r\} \cup \{0\} \\ &= \{z \in F \ : \ z = f(x) \in \mathbb{F}_q[x], \ \deg f \leq r\} \cup \{0\}. \end{aligned}$$

Consideremos el polinomio interpolador de Lagrange $L(x) \in \mathbb{F}_q[x]$ tal que $L(a_i) = a_{i+1}$ para $1 \leq i \leq n$, es decir

$$L(x) = \sum_{k=1}^{n} a_{k+1} \prod_{j \neq k} \frac{x - a_j}{a_k - a_j}.$$

Notemos que si $v(x) = u(L(x))$ para $u \in \mathcal{L}(G)$, entonces $v \in F$, $\deg v = \deg u \deg L$ y $v(a_i) = u(a_{i-1})$ satisfaciendo (3.10). Pero necesitamos que v sea un elemento de $\mathcal{L}(G)$. Ahora bien, como v es un polinomio, tenemos que

$$v \in \mathcal{L}(G) \quad \Leftrightarrow \quad \deg v \leq r \quad \Leftrightarrow \quad \deg u \deg L \leq r \quad \Leftrightarrow \quad \deg u \leq \frac{r}{\deg L}.$$

Considerando que $L(x)$ no depende de u, podemos encontrar un elemento $v \in \mathcal{L}(G)$ en función de $u \in \mathcal{L}(G)$ tal que u, v satisfagan (3.10) siempre que $\deg u \leq \frac{r}{\deg L}$. En particular, si $\deg L = 1$, $u(L(x)) \in \mathcal{L}(G)$ para todo $u \in \mathcal{L}(G)$.

Escribiremos u_L en lugar de v si queremos resaltar que v se obtuvo mediante esta técnica, es decir, $u_L = u \circ L$ para algún $u \in \mathcal{L}(G)$.

Sea $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) \subset \mathbb{F}_q^n$ un código racional, con $D = P_1 + \cdots + P_n$, $G = rP_\infty$ y $r < n$, hemos demostrado entonces lo siguiente:

Teorema 3.5.1. *Si $u \in \mathcal{L}(G)$ y $\deg u \leq \frac{r}{\deg L}$, existe $u_L \in \mathcal{L}(G)$ que satisface (3.10).*

Ejemplo 3.5.2. Consideremos el cuerpo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, con $\alpha^2 + \alpha + 1 = 0$ y los divisores $D = P_0 + P_1 + P_\alpha + P_{\alpha+1}$, $G = 2P_\infty$.

En este caso $a_1 = 0, a_2 = 1, a_3 = \alpha, a_4 = \alpha + 1$ y el polinomio $L(x)$ es $L(x) = \alpha^2 x^2 + 1$, es decir que $\deg L = 2$. Por otro lado,

$$\mathcal{L}(G) = \{f(x) \in \mathbb{F}_4[x] \ : \ \deg f \leq 2\}.$$

Así, si $u \in \mathbb{F}_4[x]$ es un polinomio con $\deg u \leq 1$, entonces $v(x) = u(L(x)) \in \mathcal{L}(G)$. Por ejemplo, si $u(x) = x + \alpha \in \mathcal{L}(G)$, entonces $v(x) = \alpha^2(x^2 + 1) \in \mathcal{L}(G)$. ◊

Corolario 3.5.3. *Si $\deg L = 1$, para cada $u \in \mathcal{L}(G)$ existe $u_L \in \mathcal{L}(G)$ que satisface (3.10). En consecuencia, $\mathcal{C}$ es cíclico.*

Definición 3.5.4. Decimos que un código AG racional $\mathcal{C}_{\mathcal{L}}(D, G)$, con $D = P_1 + \cdots + P_n$, donde cada P_i es de la forma P_{x-a_i}, y $G = rP_\infty$, es L-cíclico si el polinomio de Lagrange permite, para cada $u \in \mathcal{L}(G)$, hallar $u_L \in \mathcal{L}(G)$ satisfaciendo (3.10).

Ejemplo 3.5.5. Consideremos el cuerpo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, con $\alpha^2 + \alpha + 1 = 0$ y los divisores $D = P_0 + P_1 + P_\alpha$, $G = P_\infty$.

En este caso tenemos $a_1 = 0, a_2 = 1, a_3 = \alpha$, y el polinomio $L(x)$ es $L(x) = \alpha^2 x + 1$, es decir que $\deg L = 1$. Por lo tanto, $C_{\mathcal{L}}(D, G)$ es cíclico. ◊

Notemos que tanto $u_\sigma = \sigma^{-1}(u)$ como $u_L = u \circ L$ satisfacen, junto a u, (3.10). Veamos ahora cómo se relacionan u_σ y u_L:

Proposición 3.5.6. *Sea $\sigma \in \mathrm{Aut}(F)$ tal que $\sigma(P_i) = P_{i-1 \pmod n}$ y $\sigma(G) = G$. Si $u \in \mathcal{L}(G)$ y $\deg u_L < n$, entonces $u_\sigma = u_L$, donde $u_\sigma = \sigma^{-1}(u)$.*

Demostración. Sabemos que u_σ y u_L son polinomios, con $\deg u_\sigma \leq r < n$ y $\deg u_L < n$, y $u_\sigma \in \mathcal{L}(G)$. Además ambos satisfacen (3.10), por lo que $u_\sigma(a_i) = u_L(a_i)$ para $i = 1, \ldots, n$. Luego, $u_\sigma - u_L$ es un polinomio de grado menor a n con al menos n raíces. Así, $u_\sigma - u_L = 0$ y por lo tanto $u_\sigma = u_L$. □

Observación 3.5.7. Notemos que la condición $\deg u_L < n$ equivale a $\deg u \leq n/\deg L$. Como $r < n$, la hipótesis es más débil que en el Teorema 3.5.1, pero se requiere la existencia del automorfismo que permuta ciclícamente los lugares.

Ejemplo 3.5.8. Consideremos $\sigma \in \mathrm{Aut}(F)$ dado por $\sigma(x) = \alpha(x+1)$, asociado a la matriz

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

cuya inversa es

$$A^{-1} = \begin{pmatrix} 1 & \alpha \\ 0 & \alpha \end{pmatrix}.$$

Así, $[0]_A = \{0, 1, \alpha\}$ y $\sigma(P_\infty) = P_\infty$. Por lo tanto el código L-cíclico estudiado en el Ejemplo 3.5.5 es también sigma-cíclico. ◊

Ejemplo 3.5.9. En este ejemplo vamos a analizar un caso de un código cíclico que no es sigma-cíclico, y en principio tampoco es L-cíclico, pero utilizando las propiedades del cuerpo finito veremos que resulta ser un caso especial de código L-cíclico.

Vamos a retomar el Ejemplo 3.5.2, donde consideramos el cuerpo $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, con $\alpha^2 + \alpha + 1 = 0$ y los divisores $D = P_0 + P_1 + P_\alpha + P_{\alpha+1}$, $G = 2P_\infty$.

En primer lugar, notemos que $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ no puede ser un código sigma-cíclico, pues al tomar $G = 2P_\infty$, el código debe ser construido con una matriz de la forma

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

y la longitud del código será $|a|$, el orden de a en el grupo multiplicativo $\mathbb{F}_4^*$. Pero la longitud de $\mathcal{C}$ es 4, y ningún elemento de $\mathbb{F}_4^*$ posee orden 4. Así, $\mathcal{C}$ no es sigma-cíclico.

En segundo lugar, si calculamos el polinomio de Lagrange correspondiente a $\mathcal{C}$, obtenemos $L(x) = \alpha^2 x^2 + 1$, con $\deg L = 2$, por lo que no podemos aplicar el Corolario 3.5.3.

Sin embargo, como estos códigos racionales se forman evaluando polinomios, podemos hacer uso de la aritmética de $\mathbb{F}_4$ para hallar una función polinomial apropiada, y de allí obtener el polinomio necesario en $\mathcal{L}(G)$. Para todo $\beta \in \mathbb{F}_4$ se cumple que $\beta^4 = \beta$. Si tomamos $u(x) = ax^2 + bx + c \in \mathcal{L}(G)$, entonces:

$$\begin{aligned} u_L(x) &= u(L(x)) \\ &= u(\alpha^2 x^2 + 1) \\ &= a(\alpha^2 x^2 + 1)^2 + b(\alpha^2 x^2 + 1) + c \\ &= a\alpha^4 x^4 + a + b\alpha^2 x^2 + b + c \\ &= a\alpha x^4 + b\alpha^2 x^2 + a + b + c. \end{aligned}$$

En principio, u_L es un polinomio de grado 4, pero como nos interesa la función polinomial, podemos considerar que $a\alpha x^4 + b\alpha^2 x^2 + a + b + c = a\alpha x + b\alpha^2 x^2 + a + b + c$, como funciones sobre $\mathbb{F}_4$. y utilizar entonces el polinomio $a\alpha x + b\alpha^2 x^2 + a + b + c$ que sí es un elemento de $\mathcal{L}(G)$.

Así, para todo $u(x) = ax^2 + bx + c \in \mathcal{L}(G)$ existe $v(x) = b\alpha^2 x^2 + a\alpha x + a + b + c \in \mathcal{L}(G)$ satisfaciendo (3.10) y por lo tanto el código es cíclico. ◊

Analicemos ahora un poco más en detalle lo que sucede en el ejemplo anterior. Recordemos que estamos trabajando con $F = \mathbb{F}_q(x)$, $G = rP_\infty$ y

$$\mathcal{L}(G) = \{z \in \mathbb{F}_q[x] \ : \ \deg z \leq r\} \cup \{0\}.$$

Notemos que el operador $\cdot_L : \mathcal{L}(G) \to \mathbb{F}_q[x]$, considerando a $\mathcal{L}(G), \mathbb{F}_q[x]$ como espacios funcionales, dado por $u_L = u \circ L$, es $\mathbb{F}_q$-lineal:

$$\begin{aligned}(\alpha u + v)_L(x) &= (\alpha u + v)(L(x)) \\ &= (\alpha u)(L(x)) + v(L(x)) \\ &= \alpha u(L(x)) + v(L(x)) \\ &= \alpha u_L(x) + v_L(x).\end{aligned}$$

Si denotamos con $L(G) = \mathrm{Im}(\cdot_L)$ a la imagen de $\cdot_L$ (con posibles reducciones usando que $\beta^q = \beta$), tenemos el siguiente resultado:

Proposición 3.5.10. *Dado un código AG racional $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$, con $G = rP_\infty$, si sucede que $L(G) \subset \mathcal{L}(G)$, entonces $\mathcal{C}$ es L-cíclico.*

Capítulo 4

Códigos AG sigma-cíclicos racionales

En este capítulo desarrollaremos diferentes técnicas para construir y/o identificar códigos AG racionales cíclicos. Comenzaremos aplicando el método sigma en el cuerpo de funciones racionales, para luego realizar una clasificación según clases de equivalencia, logrando obtener resultados muy interesantes. Además, vamos a presentar otra manera de identificar códigos cíclicos, usando polinomios interpoladores de Lagrange. Presentaremos tales códigos bajo el nombre de códigos L-cíclicos, y realizaremos una comparación con códigos sigma-cíclicos.

4.1. Definiciones y propiedades

En esta sección nos enfocaremos en comprender los códigos sigma-cíclicos racionales, para lo cual usamos que $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ es isomorfo a $\mathrm{PGL}_2(\mathbb{F}_q)$, mediante la siguiente relación: si $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$, entonces existe una matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$$

tal que

$$\sigma(x) = \frac{ax+b}{cx+d}.$$

Una herramienta fundamental en nuestro estudio será la acción del grupo $\mathrm{PGL}_2(\mathbb{F}_q)$ sobre el conjunto $\mathbb{F}_q \cup \{\infty\}$, la cual está dada por:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha = \begin{cases} \frac{a\alpha+b}{c\alpha+d}, & c\alpha + d \neq 0 \\ \infty, & c\alpha + d = 0 \end{cases}$$

si $\alpha \in \mathbb{F}_q$, y

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c}, & c \neq 0 \\ \infty, & c = 0 \end{cases}.$$

Además, será de gran utilidad el uso de matrices inversas: si $A \in \mathrm{PGL}_2(\mathbb{F}_q)$, podemos considerar la siguiente representación para A^{-1}:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \quad A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Definición 4.1.1. Si $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ es una matriz de orden n y $\alpha \in \mathbb{F}_q \cup \{\infty\}$ de manera que $A\alpha \neq \alpha$ (es decir que α no es un punto fijo de A), entonces denotaremos con $[\alpha]_A$ a la órbita de α bajo la acción de A^{-1}, es decir $[\alpha]_A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, donde

$$\alpha_1 = \alpha, \quad \alpha_{i+1} = A^{-1}\alpha_i, \quad 1 \leq i \leq n-1.$$

Observación 4.1.2. Por el Lema 2.3 de [8] sabemos que $[\alpha]_A$ consiste de n elementos diferentes de $\mathbb{F}_q \cup \{\infty\}$.

Comenzamos con la constucción de códigos sigma-cíclicos racionales de la siguiente manera:

Proposición 4.1.3. *Consideremos* $[\alpha]_A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, *donde* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_q)$, *y* $\alpha = \alpha_1$ *no queda fijo por* A, $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ *asociado a* A *y los lugares* $P_i = P_{x-\alpha_i}$ *si* $\alpha_i \in \mathbb{F}_q$ *o* $P_i = P_\infty$ *si* $\alpha_i = \infty$. *Entonces* $\sigma(P_i) = P_{i+1 \mod n}$ *para* $1 \leq i \leq n$.

Demostración. En primer lugar, notemos que $P_i \neq P_j$ si $i \neq j$ pues todos los elementos de la órbita de α son distintos. Ahora bien, si $\alpha_i \in \mathbb{F}_q$, entonces

$$\sigma(x - \alpha_i) = \sigma(x) - \sigma(\alpha_i) = \frac{ax+b}{cx+d} - \alpha_i = \frac{(a - c\alpha_i)x - (d\alpha_i - b)}{cx+d}.$$

Si $a \neq c\alpha_i$ tenemos que $A^{-1} \cdot \alpha_i = \alpha_{i+1} \in \mathbb{F}_q$ y además

$$\sigma(x - \alpha_i) = (a - c\alpha_i) \frac{x - A^{-1} \cdot \alpha_i}{cx + d} = \frac{a - c\alpha_i}{cx + d} (x - \alpha_{i+1}).$$

Así, $\sigma(x - \alpha_i) \in P_{i+1}$, es decir que $\sigma(P_i) = P_{i+1}$.

Por otro lado, si $a = c\alpha_i$, sucede que $\alpha_{i+1} = A^{-1} \cdot \alpha_i = \infty$ y $c \neq 0$, ya que si $c = 0$ también $a = 0$ y eso no puede ser posible pues $A \in \mathrm{PGL}_2(\mathbb{F}_q)$. En este caso obtenemos que

$$\sigma(x - \alpha_i) = -\frac{d\alpha_i - b}{cx + d} \in P_\infty.$$

Entonces $\sigma(x - \alpha_i) \in P_{i+1}$ con $P_{i+1} = P_\infty$ y $\sigma(P_i) = P_{i+1}$.

En cambio, si $\alpha_i = \infty$ entonces $P_i = P_\infty$ y $c \neq 0$ ya que si $c = 0$ tenemos que $\alpha_{i+1} = \alpha_i$, lo cual no es posible. Además:

$$\sigma(x^{-1}) = \frac{cx + d}{ax + b} = c \frac{x + dc^{-1}}{ax + b} = c \frac{x - A^{-1} \cdot \infty}{ax + b} = c \frac{x - \alpha_{i+1}}{ax + b}$$

por lo que $\sigma(x^{-1}) \in P_{i+1}$ y $\sigma(P_i) = P_{i+1}$.

Finalmente, $A^{-1}\alpha_n = A^{-n}\alpha_1 = \alpha_1$ y considerando los casos anteriores para $i = n$ se tiene que $\sigma(P_n) = P_1$. □

Bajo las condiciones de la proposición anterior, si $D = P_1 + P_2 + \cdots + P_n$, entonces $\sigma(D) = D$ y podemos obtener códigos sigma-cíclicos racionales $\mathcal{C}_{\mathcal{L}}(D, G)$, eligiendo adecuandamente divisores G invariantes por σ.

Otro resultado importante en nuestro análisis es el siguiente:

Proposición 4.1.4. *Sean* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_q)$ *y* σ *el automorfismo asociado, entonces sucede que* $c = 0$ *si y solamente si* $\sigma(P_\infty) = P_\infty$.

Demostración. Si $c = 0$, $\sigma(P_\infty) = P_\infty$ pues

$$\sigma\left(x^{-1}\right) = \frac{d}{ax + b} \in P_\infty.$$

Recíprocamente, si $\sigma(P_\infty) = P_\infty$, usando que $x^{-1} \in P_\infty$ obtenemos

$$\sigma\left(x^{-1}\right) = \frac{cx + d}{ax + b} \in P_\infty,$$

lo cual solamente es posible si $c = 0$. □

Ejemplo 4.1.5. Sea $F = \mathbb{F}_4(x)$ generado por β tal que $\beta^2 + \beta + 1 = 0$. Consideremos la matriz $A = \left(\begin{smallmatrix} 1 & 1 \\ \beta & 0 \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_4)$. El automorfismo asociado a A es

$$\sigma(x) = \frac{x+1}{\beta x}.$$

Además, A tiene orden 5 en $\mathrm{PGL}_2(\mathbb{F}_4)$ y su inversa es $A^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right)$. Si $\alpha = \alpha_1 = 1$, entonces:

$$\begin{aligned}
\alpha_2 = &\quad \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right) 1 &&= \frac{1}{\beta+1} = \beta \\
\alpha_3 = &\quad \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right) \beta &&= \frac{1}{\beta^2+1} = \beta^2 \\
\alpha_4 = &\quad \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right) \beta^2 &&= \frac{1}{\beta^3+1} = \infty \\
\alpha_5 = &\quad \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right) \infty &&= \frac{0}{\beta} = 0 \\
\alpha_1 = &\quad \left(\begin{smallmatrix} 0 & 1 \\ \beta & 1 \end{smallmatrix}\right) 0 &&= \frac{1}{0+1} = 1.
\end{aligned}$$

Así, $[1]_A = \{1, \beta, \beta^2, \infty, 0\}$ y obtenemos los lugares

$$P_1 = P_{x-1}, \quad P_2 = P_{x-\beta}, \quad P_3 = P_{x-\beta^2}, \quad P_4 = P_\infty, \quad \text{y} \quad P_5 = P_x.$$

Por la Proposición 4.1.3 tenemos que $\sigma(P_i) = P_{i+1}$ para $i = 1, \ldots, 4$ y $\sigma(P_5) = P_1$.

Si $D = P_1 + P_2 + P_3 + P_4 + P_5$, entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ será un código AG cíclico si G es disjunto a D, es decir que G debe consistir de lugares no racionales de $\mathbb{F}_4(x)$, y debe ser invariante por σ. Podemos considerar el lugar Q de grado 2 definido por el polinomio mónico irreducible $x^2 + \beta^2 x + \beta^2$, es decir $Q = P_{x^2+\beta^2 x+\beta^2}$. Notemos que

$$\begin{aligned}
\sigma(x^2 + \beta^2 x + \beta^2) &= \sigma(x)^2 + \beta^2\sigma(x) + \beta^2 \\
&= \left(\frac{x+1}{\beta x}\right)^2 + \beta^2\left(\frac{x+1}{\beta x}\right) + \beta^2 \\
&= \frac{x^2+1}{\beta^2 x^2} + \beta^2\left(\frac{x+1}{\beta x}\right) + \beta^2 \\
&= \frac{x^2+1}{\beta^2 x^2} + \beta^2\left(\frac{x+1}{\beta x}\right)\frac{\beta x}{\beta x} + \beta^2\frac{\beta^2 x^2}{\beta^2 x^2} \\
&= \frac{x^2+1+x^2+x+\beta x^2}{\beta^2 x^2} \\
&= \frac{\beta x^2 + x + 1}{\beta^2 x^2}
\end{aligned}$$

$$\begin{aligned} &= \frac{\beta x^2 + \beta^3 x + \beta^3}{\beta^2 x^2} \\ &= \frac{\beta}{\beta^2 x^2}\left(x^2 + \beta^2 x + \beta^2\right) \\ &= \frac{\beta^2}{x^2}\left(x^2 + \beta^2 x + \beta^2\right) \end{aligned}$$

Entonces:

$$\sigma\left(x^2 + \beta^2 x + \beta^2\right) = \frac{\beta^2}{x^2}\left(x^2 + \beta^2 x + \beta^2\right) \in Q,$$

por lo que $\sigma(Q) = Q$ y podemos elegir $G = rQ$ para algún entero $0 \leq r \leq 3$.

Así, hemos construido un código sigma-cíclico racional sobre $\mathbb{F}_4$, de longitud 5, usando todos los lugares racionales de $\mathbb{F}_4(x)$. ◊

A continuación presentamos códigos AG sigma-cíclicos racionales sobre $\mathbb{F}_q$ cuya longitud es $q-1$, construidos explícitamente, usando la órbita de 1 para el divisor D, y el polo de x, P_∞, para el divisor G.

Ejemplo 4.1.6. Para todo q potencia de un número primo existen códigos AG sigma-cíclicos racionales $\mathcal{C}_\mathcal{L}(D, G)$ sobre $\mathbb{F}_q$, de longitud $q-1$, con $G = rP_\infty$ para algún $r \in \mathbb{N}$.

Sea a un generador del grupo multiplicativo $\mathbb{F}_q^*$ y $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_q)$ cuya inversa es $A^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Veremos en el Lema 4.2.8 que $|A| = |a|$ y en este caso por ser a un generador de $\mathbb{F}_q^*$ tenemos que $|a| = q-1$

Consideremos $\alpha = 1$, entonces $A^{-1}\alpha = A^{-1}1 = a \neq 1$, pues si $a = 1$, a no puede generar $\mathbb{F}_q^*$. Así, $A^{-1}1 \neq 1$ y tenemos que $[1]_A$ posee $q-1$ elementos distintos. Más aún,

$$[1]_A = \{1, a, a^2, \ldots, a^{q-2}\} = \mathbb{F}_q^*.$$

Sean $n = q-1$, $P_i = P_{x-a^{i-1}}$ para cada $1 \leq i \leq n$ y σ el automorfismo asociado a A. Por la Proposición 4.1.3 sabemos que $\sigma(P_i) = P_{i+1 \text{ mód } n}$ y por la Proposición 4.1.4 tenemos que $\sigma(P_\infty) = P_\infty$, motivos por los cuales podemos considerar los divisores $D = P_1 + P_2 + \cdots + P_n$ y $G = rP_\infty$ para obtener códigos AG sigma-cíclicos racionales $\mathcal{C}_\mathcal{L}(D, G)$, para cada $0 \leq r \leq n-2$. ◊

En las próximas secciones nos vamos a enfocar en clasificar códigos sigma-cíclicos racionales según su clase de equivalencia, con el objetivo de demostrar la escasez de tal clase de códigos. Trabajamos con la denominada equivalencia monomial, que indica lo siguiente:

Definición 4.1.7. Dos códigos $\mathcal{C}_1, \mathcal{C}_2$ sobre $\mathbb{F}_q$ son llamados equivalentes, y escribimos $\mathcal{C}_1 \sim \mathcal{C}_2$, si existe una matriz monomial M tal que $\mathcal{C}_2 = \mathcal{C}_1 M$ (una matriz monomial es una matriz obtenida al multiplicar una matriz diagonal por una matriz de permutación). En otras palabras, $\mathcal{C}_1 \sim \mathcal{C}_2$ si cada palabra código de $\mathcal{C}_2$ puede obtenerse a partir de palabras código de $\mathcal{C}_1$ y una combinación de las siguientes operaciones:

1. Permutación de las coordenadas de una palabra código.

2. Multiplicación de cada coordenada de una palabra código por un elemento no nulo de $\mathbb{F}_q$ (no necesariamente el mismo elemento no nulo en cada coordenada).

La definición anterior se usa para códigos de cualquier tipo construidos a partir de cualquier cuerpo de funciones, pero nosotros aquí nos centraremos en los códigos sigma-cíclicos racionales, es decir con $F = \mathbb{F}_q(x)$, como lo venimos haciendo en este capítulo.

Observación 4.1.8. Si solamente se cumple la condición 1, diremos que los códigos son equivalentes por permutaciones y escribiremos $\mathcal{C}_1 \sim_P \mathcal{C}_2$. Si solamente se cumple la condición 2, tenemos la noción de equivalencia considerada en [16], y escribiremos $\mathcal{C}_1 \sim_S \mathcal{C}_2$. Cada una de las anteriores es más restrictiva que la equivalencia monomial. Por lo tanto en determinadas ocasiones probaremos que $\mathcal{C}_1 \sim_P \mathcal{C}_2$ o $\mathcal{C}_1 \sim_S \mathcal{C}_2$, para deducir que los códigos son equivalentes en el sentido monomial: $\mathcal{C}_1 \sim \mathcal{C}_2$.

Además, vale la pena considerar lo siguiente:

Observación 4.1.9. Sabemos por [16, Proposición 2.2.14] que si dos divisores G_1 y G_2 de un cuerpo de funciones F sobre $\mathbb{F}_q$ son equivalentes (es decir que existe un divisor principal (z) de F tal que $G_2 = G_1 + (z)$), entonces $\mathcal{C}_{\mathcal{L}}(D, G_1) \sim_S \mathcal{C}_{\mathcal{L}}(D, G_2)$ siempre que se cumpla que $\operatorname{sop} G_i \cap \operatorname{sop} D = \emptyset$ para $i = 1, 2$. Esto fue usado en [9] para clasificar códigos AG sobre $\mathbb{F}_q$.

Corolario 4.1.10. *Sean* $D, G_1, G_2 \in \operatorname{Div}(F)$ *tales que* $\operatorname{sop} G_i \cap \operatorname{sop} D = \emptyset$ *para* $i = 1, 2$ *y* $G_1 \sim G_2$. *Entonces* $\mathcal{C}_{\mathcal{L}}(D, G_1) \sim \mathcal{C}_{\mathcal{L}}(D, G_2)$.

Demostración. Es consecuencia directa de las dos observaciones anteriores. □

A continuación, nos concentraremos, en primer lugar, en clasificar códigos $\mathcal{C}_{\mathcal{L}}(D, G)$ con $G = rP_\beta$, para luego abordar el caso $G \neq rP_\beta$. Cabe mencionar que en el primer caso

daremos una clasificación completa y veremos que, fijadas la longitud y la dimensión, tendremos un único código AG sigma-cíclico, racional, salvo equivalencias. En el otro relacionaremos a códigos donde $G \neq rP_\beta$ con códigos en los que $G = rP_\beta$ y mostraremos ejemplos computacionales que sugieren la existencia de una cantidad escasa de códigos.

4.2. Equivalencia monomial en el caso $G = rP_\beta$

En esta sección queremos clasificar códigos AG sigma-cíclicos racionales $\mathcal{C}_\mathcal{L}(D, G)$ con $G = rP_\beta$, es decir que G es un divisor de un solo punto, construido a partir de un lugar racional P_β. Para tal fin, será de suma utilidad distinguir tres casos para $\beta \in \mathbb{P}^1(\mathbb{F}_q)$: $\beta = 0$, $\beta \in \mathbb{F}_q^*$ y $\beta = \infty$. Un primer resultado en la dirección deseada requiere considerar $0 \neq \beta \in \mathbb{F}_q$ y $\tau_\beta \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ asociado a la matriz

$$\begin{pmatrix} 1 & \beta \\ 1 & 0 \end{pmatrix},$$

es decir, $\tau_\beta(x) = x + \beta$.

Proposición 4.2.1. *Sea $0 \neq \beta \in \mathbb{F}_q$ y sean P_β y P_0 los lugares asociados a $x - \beta$ y x respectivamente de $\mathbb{F}_q(x)$. Entonces*

$$\tau_\beta(\mathcal{L}(rP_\beta)) = \mathcal{L}(rP_0),$$

para cualquier entero $r \geq 1$.

Demostración. En primer lugar, notemos que $\tau_\beta(P_\beta) = P_0$, pues

$$\tau_\beta(x - \beta) = \tau_\beta(x) - \beta = x + \beta - \beta = x.$$

Recordemos que para un lugar P de $\mathbb{F}_q(x)$ el espacio de Riemann-Roch asociado a P es

$$\mathcal{L}(rP) = \{z \in \mathbb{F}_q(x) : (z) + rP \geq 0\} \cup \{0\}.$$

Veamos ahora que $\tau_\beta(\mathcal{L}(rP_\beta)) \subset \mathcal{L}(rP_0)$. Si $z \in \mathcal{L}(rP_\beta)$, entonces

$$(z) = (z)_0 - (z)_\infty = \sum n_P P - sP_\beta,$$

donde $r \geq s \geq 1$. Tenemos que

$$\nu_{P_0}(\tau_\beta(z)) = \nu_{\tau_\beta^{-1}(P_0)}(z) = \nu_{P_\beta}(z) = -s,$$

y si $\nu_Q(\tau_\beta(z)) < 0$, $Q = P_0$ pues

$$0 > \nu_Q(\tau_\beta(z)) = \nu_{\tau_\beta^{-1}(Q)}(z),$$

por lo que $\tau_\beta^{-1}(Q) = P_\beta$. Luego $(\tau_\beta(z))_\infty = -sP_0$ con $r \geq s$ y obtenemos que

$$\tau_\beta(z) \in \mathcal{L}(rP_0).$$

Recíprocamente, veamos que $\mathcal{L}(rP_0) \subset \tau_\beta(\mathcal{L}(rP_\beta))$. Si $y \in \mathcal{L}(rP_0)$, entonces

$$(y) = (y)_0 - (y)_\infty = \sum n_P P - sP_0,$$

con $r \geq s \geq 1$. En este caso,

$$\nu_{P_\beta}(\tau_\beta^{-1}(y)) = \nu_{\tau_\beta(P_\beta)}(y) = \nu_{P_0}(y) = -s,$$

y si $\nu_Q(\tau_\beta^{-1}(y)) < 0$, $Q = P_\beta$ pues

$$0 > \nu_Q(\tau_\beta^{-1}(y)) = \nu_{\tau_\beta(Q)}(y).$$

Así, $\tau_\beta(Q) = P_0$ y $(\tau_\beta^{-1}(y))_\infty = -sP_\beta$ con $r \geq s$, lo que implica que

$$\tau_\beta^{-1}(y) = z \in \mathcal{L}(rP_\beta).$$

Hemos probado, entonces, que $\tau_\beta(\mathcal{L}(rP_\beta)) = \mathcal{L}(rP_0)$. □

A partir de la proposición anterior, obtenemos un resultado fundamental para nuestro objetivo de clasificar los códigos sigma-cíclicos racionales:

Proposición 4.2.2. *Sean $P_1, \ldots, P_n$ lugares racionales distintos de $\mathbb{F}_q(x)$ y $0 \neq \beta \in \mathbb{F}_q$ tal que $P_i \neq P_{x-\beta}$ para $1 \leq i \leq n$, entonces*

$$\mathcal{C}_\mathcal{L}(D, rP_\beta) = \mathcal{C}_\mathcal{L}(\tau_\beta(D), rP_0),$$

donde $D = P_1 + \cdots + P_n$ y $\tau_\beta(D) = \tau_\beta(P_1) + \cdots + \tau_\beta(P_n)$.

Demostración. Por la Proposición 4.2.1 tenemos que cada elemento $y \in \mathcal{L}(rP_0)$ es de la forma $\tau_\beta(z)$ para algún $z \in \mathcal{L}(rP_\beta)$. Luego $\mathcal{C}_\mathcal{L}(\tau_\beta(D), rP_0) \subset \mathcal{C}_\mathcal{L}(D, rP_\beta)$ pues

$$\begin{aligned}(y(\tau_\beta(P_1)), \ldots, y(\tau_\beta(P_n))) &= (\tau_\beta(z)(\tau_\beta(P_1)), \ldots, \tau_\beta(z)(\tau_\beta(P_n))) \\ &= (z(\tau_\beta^{-1}(\tau_\beta(P_1))), \ldots, z(\tau_\beta^{-1}(\tau_\beta(P_n))) \\ &= (z(P_1), \ldots, z(P_n)).\end{aligned}$$

Recíprocamente, por la Proposición 4.2.1 cada elemento $z \in \mathcal{L}(rP_\beta)$ es de la forma $\tau_\beta^{-1}(y)$ para algún $y \in \mathcal{L}(rP_0)$. Así, $\mathcal{C}_\mathcal{L}(D, rP_\beta) \subset \mathcal{C}_\mathcal{L}(\tau_\beta(D), rP_0)$ pues

$$\begin{aligned}(z(P_1), \ldots, z(P_n)) &= (\tau_\beta^{-1}(y)(P_1), \ldots, \tau_\beta^{-1}(y)(P_n)) \\ &= (y(\tau_\beta(P_1)), \ldots, y(\tau_\beta(P_n))),\end{aligned}$$

y por lo tanto los códigos indicados son iguales. □

Observación 4.2.3. Si el código AG $\mathcal{C}_\mathcal{L}(D, rP_\beta)$ de la Proposición 4.2.2 es sigma-cíclico, es decir que $\sigma(P_i) = P_{i+1 \mod n}$ para $1 \leq i \leq n$ para algún $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$, entonces es fácil ver que $\mathcal{C}_\mathcal{L}(\tau_\beta(D), rP_0)$ también es sigma-cíclico con respecto al $\mathbb{F}_q$-automorfismo $\tau_\beta \sigma \tau_\beta^{-1}$.

Los códigos AG sigma-cíclicos que queremos clasificar son aquellos cuyo divisor G es de un solo lugar racional, es decir que tenemos los siguientes tipos de códigos:

(i) $\mathcal{C}_\mathcal{L}(D, rP_\beta)$ con $0 \neq \beta \in \mathbb{F}_q$,

(ii) $\mathcal{C}_\mathcal{L}(D, rP_0)$ y

(iii) $\mathcal{C}_\mathcal{L}(D, rP_\infty)$.

A partir de la Proposición 4.2.2 y la Observación 4.2.3 podemos ver que el problema de clasificar los códigos AG sigma-cíclicos racionales con divisores G compuestos por un lugar racional según sus clases de equivalencia se reduce a considerar los casos (ii) y (iii).

Sea $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ una matriz de orden n y sean $\alpha, \beta \in \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ tales que $A^{-1} \cdot \alpha \neq \alpha$ y $A^{-1} \cdot \beta = \beta$. Sea $1 \leq r \leq n-2$ un número entero y consideremos la órbita de α bajo la acción de A^{-1}

$$[\alpha]_A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, \tag{4.1}$$

donde $\alpha_1 = \alpha$ y $\alpha_{i+1} = A^{-1} \cdot \alpha_i$ para $1 \leq i \leq n-1$. Por la Proposición 4.1.3, a partir de la órbita $[\alpha]_A$ obtenemos los n lugares racionales distintos $P_{\alpha_1}, \ldots, P_{\alpha_n}$ de $\mathbb{F}_q(x)$. Con estos lugares y con el lugar racional P_β de $\mathbb{F}_q(x)$ construimos los divisores

$$D = P_{\alpha_1} + \cdots + P_{\alpha_n} \quad \text{y} \quad G = rP_\beta,$$

cuyos soportes son disjuntos. Así, si consideramos el $\mathbb{F}_q$-automorfismo σ de $\mathbb{F}_q(x)$ asociado a la matriz A, obtenemos el código sigma-cíclico racional $\mathcal{C}_\mathcal{L}(D, G)$.

Para estudiar el problema de equivalencia de códigos sigma-cíclicos racionales, es conveniente denotar estos códigos mediante

$$\mathcal{C}(A, \alpha, \beta, r),$$

para enfatizar su dependencia de A, α, β y r.

Comenzamos estudiando el caso (ii). Los $\mathbb{F}_q$-automorfismos de $\mathbb{F}_q(x)$ que fijan el lugar P_0 están representados por matrices de $\mathrm{PGL}_2(\mathbb{F}_q)$ que fijan el punto $0 \in \mathbb{P}^1(\mathbb{F}_q)$. En tal dirección, tenemos lo siguiente:

Lema 4.2.4. *Cualquier matriz de* $\mathrm{PGL}_2(\mathbb{F}_q)$ *que fija el punto* 0 *puede escribirse de la forma:*

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}. \tag{4.2}$$

Demostración. Consideremos la matriz $A = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ tal que $A^{-1}0 = 0$, entonces tenemos que

$$0 = A^{-1}0 = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} 0 = \frac{d'0 - b'}{-c'0 + a'} = \frac{-b'}{a'},$$

de donde obtenemos que $a' \neq 0$ y $b' = 0$. Así, obtenemos que

$$A = \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix},$$

con $a' \neq 0$. Por lo tanto podemos ver que otra manera de expresar A en $\mathrm{PGL}_2(\mathbb{F}_q)$ es $(a')^{-1}A$, obteniendo así

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix},$$

donde $c = (a')^{-1}c'$ y $d = (a')^{-1}d'$. □

Probaremos ahora que un código sigma-cíclico racional asociado a una matriz de la forma (4.2) coincide con otro código sigma-cíclico racional asociado a una matriz que fija el punto ∞.

Para esto vamos a necesitar la siguiente $\mathbb{F}_q$-base de $\mathcal{L}(rP_\beta)$:

$$B_\beta = \left\{1, \frac{1}{x-\beta}, \frac{1}{(x-\beta)^2}, \ldots, \frac{1}{(x-\beta)^r}\right\}$$

donde $\beta \in \mathbb{F}_q$. Tenemos el siguiente lema:

Lema 4.2.5. *Si $\beta \in \mathbb{F}_q$ y $r \geq 0$, entonces B_β y $\tilde{B}_\beta$ son bases de $\mathcal{L}(rP_\beta)$, donde*

$$B_\beta = \left\{1, \frac{1}{x-\beta}, \frac{1}{(x-\beta)^2}, \ldots, \frac{1}{(x-\beta)^r}\right\}$$

para todo $\beta \in \mathbb{F}_q$ y

$$\tilde{B}_\beta = \begin{cases} \left\{ \frac{1}{(x-\beta)^r}, \frac{x}{(x-\beta)^r}, \frac{x^2}{(x-\beta)^r}, \ldots, \frac{x^r}{(x-\beta)^r} \right\}, & \beta \neq 0, \\ \left\{ \frac{1}{x^r}, \frac{x+1}{x^r}, \frac{(x+1)^2}{x^r}, \ldots, \frac{(x+1)^r}{x^r} \right\}, & \beta = 0. \end{cases}$$

Demostración. Notar que $\ell(rP_\beta) = \deg(rP_\beta) + 1 - g = r + 1$, pues el género g de $\mathbb{F}_q(x)$ es cero. Además:

$$\begin{aligned} \mathcal{L}(rP_\beta) &= \{z \in \mathbb{F}_q(x) \ : \ (z) \geq -rP_\beta\} \cup \{0\} \\ &= \{z \in \mathbb{F}_q(x) \ : \ \nu_P(z) \geq 0 \ \forall \ P \neq P_\beta, \nu_{P_\beta}(z) \geq -r\} \cup \{0\} \\ &= \{z \in \mathbb{F}_q(x) \ : \ \nu_P(z) \geq 0 \ \forall \ P \neq P_\beta, P \neq P_\infty, \nu_{P_\infty}(z) \geq 0, \nu_{P_\beta}(z) \geq -r\} \cup \{0\} \\ &= \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}_q(x) \ : \ \deg g \geq \deg f, \ g(x) = (x-\beta)^j, 0 \leq j \leq r \right\} \cup \{0\} \\ &= \left\{ \frac{f(x)}{(x-\beta)^r} \in \mathbb{F}_q(x) \ : \ \deg f \leq r \right\} \cup \{0\}. \end{aligned}$$

Con esta descripción, $f(x)$ solamente puede ser un polinomio de grado a lo sumo r, y obtenemos la base $\tilde{B}_\beta$.

La base B_β es menos evidente que $\tilde{B}_\beta$, pero se obtiene observando que cualquier combinación lineal toma la forma:

$$a_0 + a_1 \frac{1}{x-\beta} + \cdots + a_r \frac{1}{(x-\beta)^r} = \frac{a_0(x-\beta)^r + a_1(x-\beta)^{r-1} + \cdots + a_r}{(x-\beta)^r}.$$

Como B_β y $\tilde{B}_\beta$ tienen $r+1$ elementos y generan a $\mathcal{L}(rP_\beta)$, concluimos que son bases. $\square$

Con el siguiente resultado podremos reducir nuestro estudio al caso (iii), y clasificar según clases de equivalencia solamente los códigos sigma-cíclicos racionales de un punto de la forma $\mathcal{C}_{\mathcal{L}}(D, rP_\infty)$.

Proposición 4.2.6. *Sea*

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q),$$

de orden n. Entonces

$$\begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q),$$

es de orden n, fija el punto ∞ y

$$\mathcal{C}\left(\left(\begin{smallmatrix} 1 & 0 \\ c & d \end{smallmatrix}\right), \alpha, 0, r\right) = \mathcal{C}\left(\left(\begin{smallmatrix} d & c \\ 0 & 1 \end{smallmatrix}\right), \alpha^{-1}, \infty, r\right).$$

En otras palabras, dado un código AG sigma-cíclico racional sobre $\mathbb{F}_q$ de la forma $\mathcal{C}_{\mathcal{L}}(D, rP_0)$, existe un divisor D' de $\mathbb{F}_q(x)$ tal que

$$\mathcal{C}_{\mathcal{L}}(D, rP_0) = \mathcal{C}_{\mathcal{L}}(D', rP_\infty).$$

Demostración. Sean

$$A = \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix}.$$

Notemos que $|A| = |B|$ pues

$$A^j = \begin{pmatrix} 1 & 0 \\ c(1 + d + \cdots + d^{j-1}) & d^j \end{pmatrix} \quad \text{y} \quad B^j = \begin{pmatrix} d^j & c(1 + d + \cdots + d^{j-1}) \\ 0 & 1 \end{pmatrix}.$$

Consideremos las órbitas $[\alpha]_A = \{\alpha_1, \ldots, \alpha_n\}$ y $[\alpha^{-1}]_B = \{\theta_1, \ldots, \theta_n\}$ con $\theta_1 = \alpha^{-1}$. Sean

$$M_1 = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \ldots & \frac{1}{\alpha_n} \\ \frac{1}{\alpha_1^2} & \frac{1}{\alpha_2^2} & \ldots & \frac{1}{\alpha_n^2} \\ \vdots & \vdots & & \vdots \\ \frac{1}{\alpha_1^r} & \frac{1}{\alpha_2^r} & \ldots & \frac{1}{\alpha_n^r} \end{pmatrix} \quad \text{y} \quad M_2 = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \theta_1^2 & \theta_2^2 & \ldots & \theta_n^2 \\ \vdots & \vdots & & \vdots \\ \theta_1^r & \theta_2^r & \ldots & \theta_n^r \end{pmatrix}.$$

Tenemos que M_2 es una matriz generadora del código $\mathcal{C}(B, \alpha^{-1}, \infty, r)$ y, usando la base B_β con $\beta = 0$, también tenemos que M_1 es una matriz generadora del código $\mathcal{C}(A, \alpha, 0, r)$.

Si vemos que $\theta_i = \alpha_i^{-1}$ para $i = 1, \ldots, n$, entonces $M_1 = M_2$ y habremos probado que los códigos indicados son iguales. Procedemos por inducción: por definición, tenemos que $\theta_1 = \alpha^{-1} = \alpha_1^{-1}$. Supongamos ahora que $\theta_i = \alpha_i^{-1}$. Entonces

$$\begin{aligned}\theta_{i+1} = B^{-1}\theta_i = \begin{pmatrix} 1 & -c \\ 0 & d \end{pmatrix} \cdot \theta_i &= \frac{\theta_i - c}{d} \\ &= \frac{\alpha_i^{-1} - c}{d} \\ &= \frac{1 - c\alpha_i}{d\alpha_i}.\end{aligned}$$

Además

$$\alpha_{i+1} = A^{-1} \cdot \alpha_i = \begin{pmatrix} d & 0 \\ -c & 1 \end{pmatrix} \cdot \alpha_i = \frac{d\alpha_i}{-c\alpha_i + 1}.$$

Luego $\theta_{i+1} = \alpha_{i+1}^{-1}$, como queríamos ver. □

Consideraremos ahora el caso (iii). Los automorfismos de $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ que fijan el lugar P_∞ están representados por matrices de $\mathrm{PGL}_2(\mathbb{F}_q)$ que fijan el punto $\infty \in \mathbb{P}^1(\mathbb{F}_q)$. Sabemos que tales matrices son de la forma

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Observación 4.2.7. La matriz $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_q)$ puede escribirse en $\mathrm{PGL}_2(\mathbb{F}_q)$ como una matriz de la forma $\left(\begin{smallmatrix} 1 & -b' \\ 0 & a' \end{smallmatrix}\right)$ donde $b' = -ba^{-1}$ y $a' = da^{-1}$. Mediante estos representantes de matrices en $\mathrm{PGL}_2(\mathbb{F}_q)$ que fijan el punto $\infty \in \mathbb{P}^1(\mathbb{F}_q)$ de la forma $A = \left(\begin{smallmatrix} 1 & -b \\ 0 & a \end{smallmatrix}\right)$ vamos a obtener expresiones más sencillas de las potencias de A^{-1} y de ciertas matrices generadoras para el código $\mathcal{C}(A, \alpha, \infty, r)$. Notemos que en tal caso, un representante de A^{-1} es

$$A^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

En primer lugar, vamos a determinar la longitud n de $\mathcal{C} = \mathcal{C}(A, \alpha, \infty, r)$ en relación a la matriz A, y luego vamos a determinar condiciones bajo las cuales se obtienen códigos equivalentes.

Recordemos que la longitud n de $\mathcal{C}$ es $|A|$, el orden de A en $\mathrm{PGL}_2(\mathbb{F}_q)$. Pero $|A| = |A^{-1}|$. Veamos entonces qué podemos decir de $|A^{-1}|$, y por lo tanto de la longitud del código a estudiar.

Lema 4.2.8. *Sean* $A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$*, con* $A \neq I$*, y* $p = \mathrm{Char}(\mathbb{F}_q)$*, entonces el orden de* $A^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ *en* $\mathrm{PGL}_2(\mathbb{F}_q)$ *es:*

$$|A^{-1}| = \begin{cases} p, & si\ a = 1 \\ |a|, & si\ a \neq 1 \end{cases}$$

donde $|a|$ *es el orden de* a *en el grupo multiplicativo* $\mathbb{F}_q^*$*.*

Demostración. Consideremos primero el caso en que $a = 1$ (y como $A \neq I$, $b \neq 0$). Basta notar que

$$(A^{-1})^m = \begin{pmatrix} 1 & mb \\ 0 & 1 \end{pmatrix},$$

por lo que $(A^{-1})^m = I$ si y solo si $p|m$. Luego $|A| = p$ pues es el menor entero divisible por p.

Supongamos ahora que $a \neq 1$. En este caso,

$$(A^{-1})^m = \begin{pmatrix} a^m & b\frac{a^m-1}{a-1} \\ 0 & 1 \end{pmatrix}.$$

De aquí, tomando $m = |a|$ podemos deducir que $(A^{-1})^m = I$ y como $|a|$ es el menor entero tal que $a^{|a|} = 1$ tenemos que $|A^{-1}| = |a|$. □

A continuación, probaremos un resultado técnico que vamos a necesitar para encontrar una expresión adecuada de la matriz generadora de $\mathcal{C}(A, \alpha, \infty, r)$, que nos permita obtener conclusiones acerca de la equivalencia de ciertos códigos.

Lema 4.2.9. *Sean* $I \neq A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$ *una matriz de orden* n*,* $\alpha \in \mathbb{F}_q$ *tal que* $A^{-1}\alpha \neq \alpha$ *y consideremos* $\alpha_1 = \alpha$ *y* $\alpha_{i+1} = A^{-1}\alpha_i$ *para* $1 \leq i \leq n-1$*. Entonces para todos* $1 \leq j' < j \leq n$ *se cumple que*

$$\alpha_j - \alpha_{j'} = (a\alpha + b - \alpha)a^{j'-1} \sum_{i=0}^{j-j'-1} a^i.$$

Demostración. Notemos que $A^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ y:

$$\begin{aligned} \alpha_1 &= \alpha \\ \alpha_2 &= a\alpha + b \\ \alpha_3 &= a^2\alpha + b(a+1) \\ \alpha_4 &= a^3\alpha + b(a^2+a+1) \\ &\vdots \end{aligned}$$

En general, para $1 \leq j \leq n$ tenemos que $\alpha_j = a^{j-1}\alpha + b\sum_{i=0}^{j-2} a^i$, considerando que si $j = 1$ el conjunto sobre el que sumamos es vacío y esa suma da cero.

Sean $1 \leq j' < j \leq n$, entonces:

$$\begin{aligned} \alpha_j - \alpha_{j'} &= a^{j-1}\alpha + b\sum_{i=0}^{j-2} a^i - a^{j'-1}\alpha - b\sum_{i=0}^{j'-2} a^i \\ &= a^{j'-1}\alpha(a^{j-j'} - 1) + b\sum_{i=j'-1}^{j-2} a^i \\ &= a^{j'-1}\alpha(a^{j-j'} - 1) + b\sum_{i=0}^{j-j'-1} a^{i+j'-1} \\ &= a^{j'-1}\alpha(a^{j-j'} - 1) + ba^{j'-1}\sum_{i=0}^{j-j'-1} a^i \\ &= a^{j'-1}\left[\alpha(a-1)\left(\sum_{i=0}^{j-j'-1} a^i\right) + b\sum_{i=0}^{j-j'-1} a^i\right] \\ &= (a\alpha + b - \alpha)a^{j'-1}\sum_{i=0}^{j-j'-1} a^i, \end{aligned}$$

como queríamos demostrar. □

Con el fin de demostrar que ciertos códigos sigma-cíclicos son equivalentes, recordemos algunos hechos que usaremos para tal fin:

1. Si $G = rP_\infty$, $\mathcal{L}(G) = \{f(x) \in \mathbb{F}_q[x] \ : \ \deg f \leq r\} \cup \{0\}$. Además, una base de $\mathcal{L}(G)$ es $\{1, x, x^2, \ldots, x^r\}$.

2. Si $D = P_1 + \cdots + P_n$, entonces para cada i se tiene que $P_i = P_{x-\alpha_i}$, donde $A^{-1}\alpha_1 \neq \alpha_1$ y $\alpha_{i+1} = A^{-1}\alpha_i$ para $1 \leq i \leq n-1$.

3. $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) = \mathcal{C}(A, \alpha_1, \infty, r)$ es un $[n, k]$-código cíclico con $n = |A|$ y $k = r + 1$. Según la conveniencia, usaremos tanto r como k. Una matriz generadora para $\mathcal{C}$ es:

$$M = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ & & \vdots & \\ \alpha_1^r & \alpha_2^r & \dots & \alpha_n^r \end{pmatrix}.$$

4. Dos $[n, k]$-códigos son iguales si sus matrices generadoras poseen la misma forma reducida por renglones.

5. Notar que toda submatriz cuadrada de M de tamaño $k \times k$ es una matriz de Vandermonde. Si V es la matriz de Vandermonde generada por $\alpha_1, \dots, \alpha_k$, entonces

$$\det(V) = \prod_{\substack{j', j=1 \\ j'<j}}^{n} (\alpha_j - \alpha_{j'}).$$

   En particular, podemos escribir $M = (V|U)$, donde V es de tamaño $k \times k$ y U es de tamaño $k \times (n - k)$. De aquí, $V^{-1}M = (I|W)$ con $W = V^{-1}U$.

Vamos a mostrar que, fijada la dimensión k y fijado $a \in \mathbb{F}_q^*$, todos los códigos sigma-cíclicos generados por matrices de la forma $A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix}$ de longitud $|A|$ son equivalentes. En el caso de $a = 1$ se descarta obviamente el caso $b = 0$.

Proposición 4.2.10. *Sean* $I \neq A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$ *una matriz de orden* n, $\alpha \in \mathbb{F}_q$ *tal que* $A^{-1} \cdot \alpha \neq \alpha$ *y consideremos* $\alpha_1 = \alpha$ *y* $\alpha_{i+1} = A \cdot \alpha_i$ *para* $1 \leq i \leq n - 1$. *Si* $1 \leq k \leq n - 1$, *entonces todos los* $[n, k]$*-códigos sigma-cíclicos que puedo generar con matrices de la forma de* A *fijado el valor de* a *son iguales , independientemente de los valores de* b *y* α. *En otras palabras,*

$$\mathcal{C}\left(\begin{pmatrix} 1 & -b_1 \\ 0 & a \end{pmatrix}, \alpha_1, \infty, r\right) = \mathcal{C}\left(\begin{pmatrix} 1 & -b_2 \\ 0 & a \end{pmatrix}, \gamma_1, \infty, r\right),$$

siempre que $\begin{pmatrix} 1 & -b_i \\ 0 & a \end{pmatrix} \neq I$ *para* $i = 1, 2$, $A^{-1}\alpha_1 \neq \alpha_1$ *y* $A^{-1}\gamma_1 \neq \gamma_1$.

Demostración. Vamos a demostrar que todas las matrices generadoras dentro de las posibles tienen la misma forma reducida, independientemente de b y α.

Consideremos la matriz generadora, recordando que como $G = rP_\infty$, entonces $k = r+1$.

$$M = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_k & \alpha_{k+1} & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_k^2 & \alpha_{k+1}^2 & \dots & \alpha_n^2 \\ \vdots & & & & & & \vdots \\ \alpha_1^r & \alpha_2^r & \dots & \alpha_k^r & \alpha_{k+1}^r & \dots & \alpha_n^r \end{pmatrix} = \left(V_{k\times k} | U_{k\times(n-k)}\right)$$

Como vimos anteriormente, podemos encontrar la forma reducida de M multiplicando a izquierda por V^{-1}: $V^{-1}M = (I|W)$ con $W = V^{-1}U$. En principio, las entradas de la matriz W podrían depender de a, b y α, es decir que $W = W(a, b, \alpha)$. Nuestro objetivo es mostrar que $W = W(a)$. Sean U_j y W_j las columnas j-ésimas de U y W respectivamente. Luego, $V^{-1}U_j = W_j$ y por lo tanto $VW_j = U_j$. Ésta última ecuación matricial representa un sistema de ecuaciones compatible determinado (pues $\det(V) \neq 0$) del cual podemos encontrar las incognitas w_i^j utilizando la regla de Cramer. En tal caso, obtenemos que

$$w_i^j = \frac{\det(V_i)}{\det(V)},\ 1 \leq i \leq k,$$

donde V_i es también una matriz de Vandermonde que se obtiene de reemplazar la columna i-ésima de V por U_j. Notemos que:

$$V = \begin{pmatrix} 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_{i-1} & \alpha_i & \alpha_{i+1} & \dots & \alpha_k \\ \alpha_1^2 & \dots & \alpha_{i-1}^2 & \alpha_i^2 & \alpha_{i+1}^2 & \dots & \alpha_k^2 \\ \vdots & & & & & & \vdots \\ \alpha_1^r & \dots & \alpha_{i-1}^r & \alpha_i^r & \alpha_{i+1}^r & \dots & \alpha_k^r \end{pmatrix},\ V_i = \begin{pmatrix} 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_{i-1} & \alpha_j & \alpha_{i+1} & \dots & \alpha_k \\ \alpha_1^2 & \dots & \alpha_{i-1}^2 & \alpha_j^2 & \alpha_{i+1}^2 & \dots & \alpha_k^2 \\ \vdots & & & & & & \vdots \\ \alpha_1^r & \dots & \alpha_{i-1}^r & \alpha_j^r & \alpha_{i+1}^r & \dots & \alpha_k^r \end{pmatrix}$$

Podemos ver que V es la matriz de Vandermonde generada por $\alpha_1, \dots, \alpha_k$ y V_i es la matriz de Vandermonde generada por $\beta_1, \dots, \beta_k$, donde $\beta_\ell = \alpha_\ell$ para todo $\ell \neq i$ y $\beta_i = \alpha_j$.

Luego, sabiendo que $j \geq k$, tenemos que:

$$\det(V_i) \ = \ \prod_{\substack{\ell',\ell=1 \\ \ell'<\ell}}^{k} (\beta_\ell - \beta_{\ell'})$$

$$
\begin{aligned}
&= \prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'}) \prod_{\ell=i+1}^{k} (\alpha_\ell-\alpha_j) \prod_{\ell=1}^{i-1} (\alpha_j-\alpha_\ell)\\
&= \left(\prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'})\right)\left((-1)^{k-i}\prod_{\substack{\ell=1\\ \ell\neq i}}^{k} (\alpha_j-\alpha_\ell)\right)\\
&= (-1)^{k-i}\prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'}) \prod_{\substack{\ell=1\\ \ell\neq i}}^{k} (\alpha_j-\alpha_\ell)
\end{aligned}
$$

y similarmente:

$$
\det(V) = \prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'}) \prod_{\ell=i+1}^{k} (\alpha_\ell-\alpha_i) \prod_{\ell=1}^{i-1} (\alpha_i-\alpha_\ell)
$$

Luego, obtenemos lo siguiente:

$$
\begin{aligned}
w_i^j &= \frac{\det(V_i)}{\det(V)}\\
&= \frac{(-1)^{k-i}\displaystyle\prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'}) \prod_{\substack{\ell=1\\ \ell\neq i}}^{k} (\alpha_j-\alpha_\ell)}{\displaystyle\prod_{\substack{1\le \ell'<\ell\le k\\ \ell,\ell'\neq i}} (\alpha_\ell-\alpha_{\ell'}) \prod_{\ell=i+1}^{k} (\alpha_\ell-\alpha_i) \prod_{\ell=1}^{i-1} (\alpha_i-\alpha_\ell)}\\
&= \frac{(-1)^{k-i}\displaystyle\prod_{\substack{\ell=1\\ \ell\neq i}}^{k} (\alpha_j-\alpha_\ell)}{\displaystyle\prod_{\ell=i+1}^{k} (\alpha_\ell-\alpha_i) \prod_{\ell=1}^{i-1} (\alpha_i-\alpha_\ell)}\\
&= (-1)^{k-i}\prod_{\ell=1}^{i-1}\frac{(\alpha_j-\alpha_\ell)}{(\alpha_i-\alpha_\ell)} \prod_{\ell=i+1}^{k}\frac{(\alpha_j-\alpha_\ell)}{(\alpha_\ell-\alpha_i)}
\end{aligned}
$$

Así, por el Lema 4.2.9 obtenemos que

$$
\begin{aligned}
w_i^j &= (-1)^{k-i}\prod_{s=1}^{i-1}\frac{(a\alpha+b-\alpha)a^{s-1}\sum_{t=0}^{j-s-1}a^t}{(a\alpha+b-\alpha)a^{s-1}\sum_{t=0}^{i-s-1}a^t} \prod_{s=i+1}^{k}\frac{(a\alpha+b-\alpha)a^{s-1}\sum_{t=0}^{j-s-1}a^t}{(a\alpha+b-\alpha)a^{i-1}\sum_{t=0}^{s-i-1}a^t}\\
&= (-1)^{k-i}\prod_{s=1}^{i-1}\frac{\sum_{t=0}^{j-s-1}a^t}{\sum_{t=0}^{i-s-1}a^t} \prod_{s=i+1}^{k} a^{s-i}\frac{\sum_{t=0}^{j-s-1}a^t}{\sum_{t=0}^{s-i-1}a^t}
\end{aligned}
$$

$$= (-1)^{k-i} \prod_{s=i+1}^{k} a^{s-i} \prod_{s=1}^{i-1} \frac{\sum_{t=0}^{j-s-1} a^t}{\sum_{t=0}^{i-s-1} a^t} \prod_{s=i+1}^{k} \frac{\sum_{t=0}^{j-s-1} a^t}{\sum_{t=0}^{s-i-1} a^t},$$

es decir

$$w_i^j = (-1)^{k-i} a^{\frac{1}{2}(k-i)(k-i+1)} \prod_{s=1}^{i-1} \frac{\sum_{t=0}^{j-s-1} a^t}{\sum_{t=0}^{i-s-1} a^t} \prod_{s=i+1}^{k} \frac{\sum_{t=0}^{j-s-1} a^t}{\sum_{t=0}^{s-i-1} a^t}.$$

Por lo tanto las entradas w_i^j de W solo dependen de a, es decir que $W = W(a)$, como queríamos demostrar. □

El resultado anterior establece que para cualquier matriz

$$A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q),$$

de orden $n > 1$ existen dos posibilidades: si $a \neq 1$,

$$\mathcal{C}(A, \alpha, \infty, r) = \mathcal{C}(D(1, a), \gamma, \infty, r)$$

donde

$$D(1, a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix},$$

y si $a = 1$

$$\mathcal{C}(A, \alpha, \infty, r) = \mathcal{C}(T, \gamma, \infty, r),$$

donde

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{4.3}$$

En el caso $a \neq 1$, tenemos que $1 \in \mathbb{F}_q$ no es un punto fijo de $D(1, a)$ y entonces

$$\mathcal{C}(A, \alpha, \infty, r) = \mathcal{C}(D(1, a), 1, \infty, r).$$

En el caso $a = 1$ el único punto fijo de T es ∞. Luego

$$\mathcal{C}(A, \alpha, \infty, r) = \mathcal{C}(T, 1, \infty, r).$$

Notemos que, si la longitud es $p = \mathrm{Char}(\mathbb{F}_q)$, existe un único tipo de códigos sigma-cíclicos racionales de la forma $\mathcal{C}_\mathcal{L}(D, rP_\infty)$: aquellos de la forma $\mathcal{C}(T, \alpha, \infty, r)$, pues ningún elemento de $\mathbb{F}_q^*$ puede tener orden p.

Veremos a continuación que, salvo equivalencias, existe un único código sigma-cíclico racional de la forma $\mathcal{C}_\mathcal{L}(D, rP_\infty)$ de una longitud y una dimensión dadas.

Proposición 4.2.11. *Sea $c \in \mathbb{F}_q$ un elemento de orden n en el grupo multiplicativo $\mathbb{F}_q^*$. Para cualquier matriz*

$$A = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q),$$

de orden n y cualquier $\alpha \in \mathbb{F}_q$ tal que $A^{-1}\alpha \neq \alpha$ se cumple que

$$\mathcal{C}(A, \alpha, \infty, r) \sim \mathcal{C}(D(1, c), 1, \infty, r),$$

si $a \neq 1$, y

$$\mathcal{C}(A, \alpha, \infty, r) = \mathcal{C}(T, 1, \infty, r),$$

si $a = 1$, donde T está dada por (4.3).

En otras palabras, sea $c \in \mathbb{F}_q$ de orden $n \neq \mathrm{Char}(\mathbb{F}_q)$ en el grupo multiplicativo $\mathbb{F}_q^*$. Si sucede que $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ es de orden n y

(a) $\sigma(P_\infty) = P_\infty$,

(b) $\sigma(P_i) = P_{i+1}$ *para* $1 \leq i \leq n-1$ *y* $\sigma(P_n) = P_1$ *donde* $P_1, \ldots, P_n$ *son lugares racionales de* $\mathbb{F}_q(x)$,

entonces

$$\mathcal{C}_{\mathcal{L}}(P_1 + \cdots + P_n, rP_\infty) \sim \mathcal{C}(D(1, c), 1, \infty, r).$$

Más aún, si $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ es de orden $p = \mathrm{Char}(\mathbb{F}_q)$ y las condiciones (a) y (b) se cumplen para $n = p$, entonces

$$\mathcal{C}_{\mathcal{L}}(P_1 + \cdots + P_p, rP_\infty) = \mathcal{C}(T, 1, \infty, r).$$

Demostración. La afirmación para el caso $a = 1$ ya ha sido probada. Para el caso $a \neq 1$, basta demostrar que si a_1 y a_2 son dos elementos de orden n en el grupo multiplicativo $\mathbb{F}_q^*$, entonces

$$\mathcal{C}(D(1, a_1), 1, \infty, r) \sim \mathcal{C}(D(1, a_2), 1, \infty, r).$$

Sea $i = 1, 2$. Notemos que

$$D(1, a_i)^{-1} = \begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix},$$

y una matriz generadora para $\mathcal{C}(D(1,a_i),1,\infty,r)$ es de la forma

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & a_i & a_i^2 & \dots & a_i^{(n-1)} \\ 1 & a_i^2 & a_i^4 & \dots & a_i^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_i^{(k-1)} & a_i^{2(k-1)} & \dots & a_i^{(k-1)(n-1)} \end{pmatrix}$$

Ahora bien, la segunda fila es justamente el subgrupo cíclico de $\mathbb{F}_q^*$ generado por a_i, es decir

$$\langle a_i \rangle = \left\{1, a_i, a_i^2, \dots, a_i^{n-1}\right\}.$$

Como a_1 y a_2 tienen el mismo orden, tenemos que $\langle a_1 \rangle = \langle a_2 \rangle$ ([4, Teorema 7, pag. 58]). Esto significa que la matriz genrdora de $\mathcal{C}(D(1,a_1),1,\infty,r)$ puede obtenerde de la matriz generadora de $\mathcal{C}(D(1,a_2),1,\infty,r)$ mediante permutación de columnas.

Por lo tanto, $\mathcal{C}(D(1,a_1),1,\infty,r) \sim \mathcal{C}(D(1,a_2),1,\infty,r)$. □

Si utilizamos los resutados que hemos desarrollado hasta aquí en esta sección, estamos en condiciones de enunciar uno de los resultados mas importantes de esta tesis.

Teorema 4.2.12. *Salvo equivalencias, para cada par $[n,k]$ de longitud y dimensión posibles, existe un único código sigma-cíclico racional sobre $\mathbb{F}_q$, de la forma $\mathcal{C}_\mathcal{L}(D,rP_\beta)$, para algún $\beta \in \mathbb{P}^1(\mathbb{F}_q)$.*

Demostración. El resultado es consecuencia directa de las Proposiciones 4.2.3, 4.2.6 y 4.2.11. □

4.3. Equivalencia monomial en el caso $G \neq rP_\beta$

En la sección previa solamente consideramos códigos $\mathcal{C}_\mathcal{L}(D,G)$, con $G = rP$, para algún lugar racional P. Ahora trataremos el caso en que $\deg G > 1$.

Como un primer acercamiento a comprender los códigos de interés en esta sección, podemos ver que, en realidad, cada código $\mathcal{C}_\mathcal{L}(D,G)$ de longitud $n < q+1$ se corresponde mediante equivalencia con un código de la forma $\mathcal{C}_\mathcal{L}(D,rP)$, para algún lugar racional P.

Proposición 4.3.1. *Sean $P_1, \ldots, P_n$ lugares racionales distintos, con $n < q+1$, y D, G divisores tales que $D = P_1 + \cdots + P_n$ y $\nu_G(P_i) = 0$ para todo i, con $0 < \deg G < n$, entonces existen un lugar racional $P \notin \{P_1, \ldots, P_n\}$ y un entero r tales que*

$$\mathcal{C}_{\mathcal{L}}(D, G) \sim \mathcal{C}_{\mathcal{L}}(D, rP).$$

Demostración. En primer lugar, como $n < q+1$, y $\mathbb{F}_q(x)$ posee $q+1$ lugares racionales, sabemos que existe un lugar racional $P \notin \{P_1, \ldots, P_n\}$. Además, por la Proposición 2.3.2, sabemos que la dimensión del código $\mathcal{C}_{\mathcal{L}}(D, G)$ es $k = 1 + \deg G$. Consideremos el divisor $G' = (k-1)P$, entonces resulta que $\deg(G' - G) = 0$.

Por el Teorema 1.5.17, obtenemos que $\ell(G' - G) = 1$. Luego, $G' - G$ es un divisor de grado 0 y dimensión 1. Así, por el Corolario 1.4.10, obtenemos que $G' - G$ es un divisor principal, o dicho de otra manera, que $G' \sim G$, es decir que son divisores equivalentes.

Luego, por la Proposición 2.2.14 de [16] tenemos que $\mathcal{C}_{\mathcal{L}}(D, G) \sim_S \mathcal{C}_{\mathcal{L}}(D, G')$. Como $\sim_S$ es una equivalencia más fuerte que $\sim$, obtenemos que $\mathcal{C}_{\mathcal{L}}(D, G) \sim \mathcal{C}_{\mathcal{L}}(D, G')$, con $G' = (k-1)P$. □

Si consideramos códigos sigmá-cíclicos provenientes de automorfismos que dejan fijo al menos un lugar racional, la proposición anterior nos brinda lo siguiente:

Corolario 4.3.2. *Sea $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ tal que $\sigma(P) = P$ para al menos un lugar racional P y sea G cualquier divisor fijo por σ de grado r. Sea $D = P_1 + \cdots + P_n$ un divisor formado por lugares racionales que σ mueve cíclicamente. Entonces*

$$\mathcal{C}_{\mathcal{L}}(D, G) \sim \mathcal{C}_{\mathcal{L}}(D, rP).$$

Demostración. Es consecuencia directa de la Proposición 4.3.1. □

Consideremos ahora códigos racionales sigma-cíclicos de longitud $q+1$ sobre $\mathbb{F}_q$.

Sean $P_1, P_2, \ldots, P_{q+1}$ todos los lugares racionales de $\mathbb{F}_q$ y sean $\sigma_1, \sigma_2 \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$ dos automorfismos que mueven cíclicamente los $q+1$ lugares en algún orden. Como podemos intercambiar posiciones en palabras código para obtener códigos equivalentes, podemos suponer que $\sigma_j(P_i) = P_{i+1 \ \mathrm{mód}\ q+1}$ para todos j, i. Por el mismo motivo, podemos asumir por ejemplo que $P_{q+1} = P_\infty$, el polo de x.

Sea $D = P_1 + \cdots + P_{q+1}$ y supongamos que $\sigma_j \in \mathrm{Aut}_{D,G_j}(\mathbb{F}_q(x))$ para cada j, con divisores G_1, G_2 que sean del mismo grado, digamos $\deg G_1 = \deg G_2 = r$. Así, podemos construir dos códigos sigma-cíclicos $\mathcal{C}_j = \mathcal{C}_\mathcal{L}(D, G_j)$, para $j = 1, 2$.

Ahora bien, notemos que el divisor $G' = rP_\infty$ es un divisor de grado r, y entonces $G' - G_j$ es un divisor de grado 0. Usando el Teorema 1.5.17 y el Corolario 1.4.10, obtenemos que $G' \sim G_j$ para cada j, y por transitividad en la relación de equivalencia obtenemos que $G_1 \sim G_2$. Luego, por el Corolario 4.1.10, obtenemos que $\mathcal{C}_1 \sim \mathcal{C}_2$.

Con lo anterior, hemos demostrado:

Proposición 4.3.3. *Fijada la dimensión, todos los códigos sigma-cíclicos de longitud $q+1$ son equivalentes.*

Además, utilizando el mismo argumento, obtenemos el siguiente resultado que abarca automorfismos que no fijan ningún lugar racional.

Proposición 4.3.4. *Sean $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$, $\alpha \in \mathbb{P}^1(\mathbb{F}_q)$ tal que $A^{-1}\alpha \neq \alpha$, donde A es la matriz asociada a σ y D el divisor que surge de considerar los lugares asociados a la órbita $[\alpha]_A$. Si G_1, G_2 son dos divisores del mismo grado, tales que $\nu_{P_i}(G_j) = 0$ para todos i, j, y $\sigma(G_j) = G_j$ para cada j, entonces los códigos sigma-cíclicos resultan equivalentes, es decir:*

$$\mathcal{C}_\mathcal{L}(D, G_1) \sim \mathcal{C}_\mathcal{L}(D, G_2).$$

Hasta el momento, somos capaces de determinar que, fijadas la longitud n y la dimensión k, existe un único código sigma-cíclico, salvo equivalencias, en los siguientes casos:

- cuando el automorfismo asociado fija algún lugar racional,
- y cuando $n = q + 1$.

Así, resulta que no hemos abordado aún el caso en que ningún lugar racional queda fijo y $n < q + 1$, es decir que $n | q + 1$.

Motivados por entender o conjeturar cuántos códigos sigma-cíclicos no equivalentes existen de aquellos que no están comprendidos en los resultados teóricos, realizamos experimentos numéricos para comprobar computacionalmente equivalencia de códigos sigma-cíclicos generados con divisores $G = Q$, donde Q es un lugar no racional de $\mathbb{F}_q(x)$, y

la longitud n es un divisor propio de $q+1$. Además, resumimos en una tabla las cantidades de códigos distintos y de códigos no equivalentes que existen, de dimensión 3, para los valores indicados de q y n. Vale la pena destacar que, cuando se indique, la cantidad de códigos no equivalentes puede referirse a que son no equivalentes por permutaciones, pues la complejidad computacional para determinar equivalencia monomial no siempre nos permite analizarla. En cambio, contamos con rutinas optimizadas para determinar rápidamente equivalencia permutacional.

1. Fijado q, construimos el cuerpo finito $\mathbb{F}_q$, el anillo de polinomios con coeficientes en $\mathbb{F}_q$ y el cuerpo de funciones racionales sobre $\mathbb{F}_q$.

2. Formamos PMI_2, el conjunto de los polinomios mónicos irreducibles de grado 2, el cual sirve para construir el subconjunto IMS del conjunto $\mathrm{GL}_2(\mathbb{F}_q)$. IMS contiene a las matrices de $\mathrm{GL}_2(\mathbb{F}_q)$ que no fijan lugar racional alguno.

3. PMI_2 también es utilizado para considerar lugares de grado 2 en el cuerpo de funciones, y obtener códigos de dimensión $k = 3$.

4. Si queremos considerar lugares de grado $k-1$, para un entero k fijo, determinamos el conjunto PMI_{k-1} de polinomios mónicos irreducibles de grado $k-1$ sobre $\mathbb{F}_q$, con el fin de estudiar códigos de dimensión k.

5. Calculamos los órdenes de las matrices de IMS como elementos de $\mathrm{PGL}_2(\mathbb{F}_q)$, y consideramos el conjunto N de todos los órdenes n que cumplen que $n < q+1$ y $n|q+1$ (divisores propios de $q+1$).

6. Para cada $n \in N$, realizamos lo siguiente (notar que en este paso ya quedan fijos n y k, que son la longitud y la dimensión de los códigos que vamos a construir):

   a) Definimos una lista MATGEN en la cual pondremos las matrices generadoras de códigos de longitud n y dimensión k.

   b) Para cada matriz $A \in$ IMS de orden n, calculamos sus órbitas y los lugares de grado $k-1$ que fija el automorfismo σ asociado a A. Para cada órbita $[\alpha]_A$ y cada lugar fijo Q, obtenemos la matriz generadora M del código $\mathcal{C}_{\mathcal{L}}(D, G)$,

donde D es el divisor obtenido de la órbita $[\alpha]_A$ y $G = Q$. Agregamos la matriz M a la lista MATGEN.

c) Buscamos las formas reducidas por filas de todas las matrices de MATGEN, para ver cuántos códigos diferentes, pero quizás equivalentes, hay. Recordemos que si dos matrices distintas tienen la misma reducción, entonces los códigos generados son exactamente el mismo código.

d) Comparamos todos los códigos asociados a las matrices de MATGEN para descartar aquellas matrices que generan códigos equivalentes por permutaciones, y contamos la cantidad de códigos no equivalentes por permutaciones obtenida.

e) Si existe un único código no equivalente por permutaciones, entonces existe un único código no equivalente en el sentido monomial. Si no, es decir, si hay más de un código no equivalente por permutaciones, debemos chequear si son o no monomialmente equivalentes.

f) Si sucede que existe más de un código monomialmente no equivalente, imprimimos las matrices generadoras de los mismos.

g) Dependiendo de los valores de q y n, puede suceder que no podamos chequear equivalencia monomial, ya que no existe una rutina para ello, y nuestro algortimo lo hace por fuerza bruta. En tales casos nos quedamos con las matrices de los códigos no equivalentes por permutaciones.

Debido a la diferencia de complejidad computacional que surge dependiendo de si q es o no un número primo, hemos escrito dos algoritmos. Tales algoritmos pueden encontrarse en el siguiente enlace:

https://github.com/cabanagusti/Algoritmos-de-Tesis-Cabana.git

A continuación, resumimos en una tabla la información obtenida, trabajando con divisores $G = Q$ para lugares Q de grado 2, por lo que los códigos serán de dimensión 3.

q	n	Cantidad de códigos distintos	Cantidad de códigos no equivalentes
7	4	1	1
9	5	20	2
11	4	1	1
	6	1	1
13	7	3	1
17	6	1	1
	9	3	1
19	4	1	1
	5	2	1
	10	2	1
23	4	1	1
	6	1	1
	8	2	1
	12	2	1
25	13	156	2 no equivalentes por permutaciones
27	4	28	2
	7	84	2 no equivalentes por permutaciones
	14	84	2 no equivalentes por permutaciones
29	5	2	1
	6	1	1
	10	2	1
	15	4	1
31	4	1	1
	8	2	1
	16	4	1

Ahora, listaremos las matrices generadoras de códigos no equivalentes en los casos en los que hay más de un código no equivalente. Denotaremos con I a la matriz identidad de orden 3.

- $\mathbb{F}_9 = \mathbb{F}_3[a]$ con a raíz de $y^2 + 2y + 2$ y $n = 5$. Hay 2 códigos monomialmente no equivalentes, con matrices generadoras de la forma $M = (I|M_1)$:

$$M_1 = \begin{pmatrix} 2 & 2a \\ a+1 & 2a+2 \\ 2a+1 & 2a+2 \end{pmatrix} \text{ y } M_1 = \begin{pmatrix} 2a & 1 \\ a & 0 \\ 1 & 0 \end{pmatrix}.$$

- $\mathbb{F}_{25} = \mathbb{F}_5[a]$ con a raíz de y^2+4y+2 y $n = 13$. Hay 2 códigos no equivalentes por permutaciones, con matrices generadoras de la forma $M = (I|M_1)$, donde M_1 es cualquiera de las siguientes:

$$\begin{pmatrix} 3a+1 & a+4 & 1 & 4a+2 & 4 & 2a+4 & 4 & 4a+2 & 1 & a+4 \\ 4a+1 & 4a+1 & 0 & 1 & a+2 & 2 & 2a & 3a+2 & 2a & 2 \\ 3a+4 & 1 & 0 & a+3 & 4a & 3a & 3a+2 & 3a+2 & 3a & 4a \end{pmatrix},$$

$$\begin{pmatrix} 4a+2 & a+1 & 4a+1 & 3a & a+4 & a+3 & a+4 & 3a & 4a+1 & a+1 \\ 3a+3 & 2 & 4a+1 & 3a+1 & 2a+1 & a & 3a+4 & a+2 & a+1 & a+3 \\ 3a+1 & 4a+3 & 2a+4 & 4a & 2a+1 & 3a+3 & a+3 & a+4 & 4 & 3a+2 \end{pmatrix}.$$

- $\mathbb{F}_{27} = \mathbb{F}_3[a]$ con a raíz de $y^3 + 2y + 1$ y $n = 4$. Hay 2 códigos monomialmente no equivalentes, con matrices generadoras:

$$\begin{pmatrix} 1 & 0 & 0 & a^2+2a+2 \\ 0 & 1 & 0 & a^2+a \\ 0 & 0 & 1 & a^2+2 \end{pmatrix} \text{ y } \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- $\mathbb{F}_{27} = \mathbb{F}_3[a]$ con a raíz de $y^3 + 2y + 1$ y $n = 7$. Hay 2 códigos no equivalentes por permutaciones, con matrices generadoras de la forma $M = (I|M_1)$:

$$M_1 = \begin{pmatrix} 2a^2+a+1 & a & 2a^2+2a+2 & a \\ a^2+a+2 & a^2+2a+2 & 2a^2+2 & 2a+2 \\ a+1 & 2a^2+2 & 2a^2+a & 2 \end{pmatrix} \text{ y}$$

$$M_1 = \begin{pmatrix} a+1 & 2a^2+a+1 & 1 & 2a^2+a+1 \\ a^2+2a+2 & a^2+2a+2 & 0 & 1 \\ 2a^2+1 & 1 & 0 & a^2+2a+2 \end{pmatrix}.$$

- $\mathbb{F}_{27} = \mathbb{F}_3[a]$ con a raíz de $y^3 + 2y + 1$ y $n = 14$. Hay 2 códigos no equivalentes por permutaciones, con matrices generadoras de la forma $M = (I|M_1|M_2)$:

$$M_1 = \begin{pmatrix} a^2+2 & a^2+a+2 & 1 & 2a^2+2a & 2a^2 & 2 \\ 2a^2+2a+1 & 2a^2+2a+1 & 0 & 1 & a^2+2a+2 & 2a^2+a \\ a+1 & 1 & 0 & a^2+a & a+2 & a^2+2a+2 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 2 & 2a^2 & 2a^2+2a & 1 & a^2+a+2 \\ 2a^2+a+1 & 2a & 2a & 2a^2+a+1 & 2a^2+a \\ a^2+2a+1 & a^2+a+1 & a^2+2a+1 & a^2+2a+2 & a+2 \end{pmatrix}$$

y

$$M_1 = \begin{pmatrix} a+2 & 2a^2+a+1 & 2a^2+1 & 2a^2+2a+1 & a^2+2a \\ 2a^2+2a+1 & 2a^2+1 & a^2+2a+1 & 2a^2+a+1 & 2 \\ a^2+1 & 2a^2+2a+2 & a+2 & 2a^2+2 & 2a^2+a+2 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} a^2+2 & a^2+2 & a^2+2a & 2a^2+2a+1 & 2a^2+1 & 2a^2+a+1 \\ a^2+2 & a^2 & 2a^2+a+2 & 2a^2+2 & a+2 & 2a^2+2a+2 \\ a^2 & a^2+2 & 2 & 2a^2+a+1 & a^2+2a+1 & 2a^2+1 \end{pmatrix}.$$

La evidencia computacional parece sugerir que la cantidad de códigos sigma-cíclicos es baja, aún en los casos que no pudimos desarrollar teóricamente.

Conclusiones y trabajo futuro

La presente tesis se enmarcó dentro de la teoría de códigos, más precisamente estudiamos códigos algebraico-geométricos cíclicos y logramos avances originales significativos para comprender propiedades estructurales de estos códigos, especialmente dentro de los códigos algebraico-geométricos racionales.

En primera instancia, encontramos condiciones para construir códigos algebraico-geométricos cíclicos en el contexto de cuerpos de funciones algebraicas sobre cuerpos finitos, $F/\mathbb{F}_q$, mediante el uso del grupo de automorfismos $\mathrm{Aut}_{\mathbb{F}_q}(F)$. Para ello, diseñamos el método sigma, que nos permitió construir tales códigos, a los que nombramos códigos sigma-cíclicos, y desarrollamos ejemplos de aplicación del método.

Además de considerar dichas construcciones en cuerpos de funciones, desarrollamos resultados y ejemplos de códigos algebraico-geométricos cíclicos construidos en extensiones F'/F de cuerpos de funciones, lo que puede ser de suma importancia al momento de intentar construir sucesiones de códigos cíclicos.

Finalmente, focalizamos nuestro estudio en códigos algebraico-geométricos cíclicos racionales, es decir, aquellos construidos sobre cuerpos de funciones racionales $F = \mathbb{F}_q(x)$. En este contexto, logramos clasificar una familia de códigos sigma-cíclicos muy usada en la literatura, mediante la denominada equivalencia monomial. Además, realizamos ejemplos computacionales para contemplar aquellos casos no abordados teóricamente.

Los resultados más importantes que hemos podido demostrar, son los siguientes:

- Lema 3.1.5: Sean $P_1, \ldots, P_n$ lugares racionales diferentes de un cuerpo de funciones F sobre $\mathbb{F}_q$, y G un divisor tal que $\nu_{P_i}(G) = 0$ para todo $i = 1, \ldots, n$. Consideremos $D = P_1 + \cdots + P_n$ y supongamos que existe $\sigma \in \mathrm{Aut}_{D,G}(F)$ tal que

$$\sigma(P_1) = P_2,\ \ldots,\ \sigma(P_{n-1}) = P_n,\ \sigma(P_n) = P_1.$$

Entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código AG cíclico, el orden de σ como elemento de $\mathrm{Aut}_{\mathbb{F}_q}(F)$ es divisible por n y además n es el menor entero positivo que satisface $\sigma^n(P_1) = P_1$.

- Proposición 3.4.1: Sean F'/F una extensión cíclica de grado m de cuerpos de funciones sobre $\mathbb{F}_q$. Sea P un lugar de F y sean $P_1, \ldots, P_n$ todos los lugares de F' que están arriba de P. Entonces n divide a m y para cualquier generador σ de $\mathrm{Gal}(F'/F)$ tenemos que la órbita de P_1 es

$$[P_1]_\sigma = \{P_1, \ldots, P_n\}.$$

  Más aún, sea $Q \neq P$ un lugar de F y sea $G = Q_1 + \cdots + Q_k$ un divisor de F' formado por todos los lugares de F' que están arriba de Q. Entonces $\sigma(G) = G$ y $\mathrm{sop}(G) \cap \mathrm{sop}(D) = \emptyset$, donde $D = P_1 + \cdots + P_n$. En particular, si cada P_i es racional, entonces $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código sigma-cíclico.

- Corolario 3.4.4: Sea F'/F una extensión de Galois de grado n de cuerpos de funciones sobre $\mathbb{F}_q$. Sean $P_1, \ldots, P_n$ diferentes lugares de F'. Supongamos que (3.5) se cumple con los lugares $P_1, \ldots, P_n$ para algún $\sigma \in \mathrm{Gal}(F'/F)$. Entonces la extensión F'/F es cíclica, σ genera a $\mathrm{Gal}(F'/F)$, y existe un lugar $P \in \mathbb{P}(F)$ que se descompone en F' en los lugares $P_1, \ldots, P_n$. Recíprocamente, si F'/F es cíclica y algún lugar $P \in \mathbb{P}(F)$ se descompone en F' en los lugares $P_1, \ldots, P_n$, entonces (3.5) se cumple para esos lugares y cualquier generador σ de $\mathrm{Gal}(F'/F)$.

- Teorema 3.4.6: Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ que contiene al cuerpo de funciones racionales $\mathbb{F}_q(x)$. Sean $P_1, \ldots, P_n$ diferentes lugares de F. Sea $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(F)$ un automorfismo de orden m que satisface (3.5). Entonces:

  1. n divide a m.

  2. Existen un divisor k de n, un entero positivo d que divide tanto a m/k como a n y un cuerpo de funciones E sobre $\mathbb{F}_q$ tales que $\mathbb{F}_q(x) \subset E \subset F$ y F/E es cíclica. Además, existen lugares $Q_1, \ldots, Q_d$ de E que se descomponen completamente en F en los lugares $P_1, \ldots, P_n$.

3. Sean $y \in F$ tal que $F = \mathbb{F}_q(x, y)$ y $G = \langle \sigma \rangle$ el subgrupo generado por σ de $\mathrm{Aut}_{\mathbb{F}_q}(F)$. Si sucede que $\alpha x + y \notin F^G$ para todo $\alpha \in \mathbb{F}_q$, entonces la extensión cíclica F/E obtenida en el inciso anterior cumple que $E \subsetneq F$.

- Teorema 3.5.1: Si $u \in \mathcal{L}(G)$ y $\deg u \leq \frac{r}{\deg L}$, existe $u_L \in \mathcal{L}(G)$ que satisface (3.10).
- Corolario 3.5.3: Si $\deg L = 1$, para cada $u \in \mathcal{L}(G)$ existe $u_L \in \mathcal{L}(G)$ que satisface (3.10). En consecuencia, $\mathcal{C}$ es cíclico.
- Proposición 3.5.6: Sea $\sigma \in \mathrm{Aut}(F)$ tal que $\sigma(P_i) = P_{i-1 \mod n}$ y $\sigma(G) = G$. Si $u \in \mathcal{L}(G)$ y $\deg u_L < n$, entonces $u_\sigma = u_L$, donde $u_\sigma = \sigma^{-1}(u)$.
- Teorema 4.2.12: Salvo equivalencias, para cada par $[n, k]$ de longitud y dimensión posibles, existe un único código sigma-cíclico racional sobre $\mathbb{F}_q$, de la forma $\mathcal{C}_{\mathcal{L}}(D, rP_\beta)$, para $\beta \in \mathbb{P}^1(\mathbb{F}_q)$.

Vale la pena mencionar que estudiar códigos algebraico-geométricos cíclicos es muy interesante porque hay mucho aún por investigar. Una lista no exhaustiva de problemas que queremos resolver en el futuro es la siguiente:

- Obtener otra manera sistemática de construir códigos AG cíclicos, sin usar automorfismos.
- Estudiar la ramificación de lugares en una torre de cuerpos de funciones con la intención de construir un código AG cíclico en cada paso de la torre y analizar los parámetros relativos de tal sucesión de códigos.
- Lograr una clasificación completa de códigos sigma-cíclicos racionales.
- Utilizar una combinación del método sigma con el polinomio interpolador de Lagrange para estudiar códigos AG en cuerpos de funciones no racionales.

Bibliografía

[1] N. Aydin, J. Lambrinos, and O. VandenBerg. On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes. *Des. Codes Cryptogr.*, 87(10):2199–2212, 2019.

[2] G. Cabaña, M. Chara, R. Podestá, and R. Toledano. On cyclic algebraic-geometry codes. *Finite Fields Appl.*, 82:Paper No. 102064, 2022.

[3] M. Chara, R. Podestá, and R. Toledano. Block transitive codes attaining the Tsfasman-Vladut-Zink bound. *Des. Codes Cryptogr.*, 88(6):1227–1253, 2020.

[4] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[5] K. Guenda and T. A. Gulliver. On the equivalence of cyclic and quasi-cyclic codes over finite fields. *J. Algebra Comb. Discrete Struct. Appl.*, 4(3):261–269, 2017.

[6] D. Hachenberger, H. Niederreiter, and C. Xing. Function-field codes. *Appl. Algebra Engrg. Comm. Comput.*, 19(3):201–211, 2008.

[7] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[8] A. López, D. Maisner, E. Nart, and X. Xarles. Orbits of Galois invariant n-sets of $\mathbb{P}^1$ under the action of PGL_2. *Finite Fields Appl.*, 8(2):193–206, 2002.

[9] A. López and E. Nart. Classification of Goppa codes of genus zero. *J. Reine Angew. Math.*, 517:131–144, 1999.

[10] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[11] Y. Manin. What is the maximum number of points on a curve over $\mathbf{F}_2$? *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):715–720 (1982), 1981.

[12] C. Munuera and R. Pellikaan. Equality of geometric Goppa codes and equivalence of divisors. *J. Pure Appl. Algebra*, 90(3):229–252, 1993.

[13] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[14] H. Stichtenoth. On automorphisms of geometric Goppa codes. *J. Algebra*, 130(1):113–121, 1990.

[15] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound. *IEEE Trans. Inform. Theory*, 52(5):2218–2224, 2006.

[16] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[17] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[18] M. Tsfasman, S. Vlăduţ, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[19] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991. Translated from the Russian by the authors.

Índice alfabético