Universidad
de La Laguna

Introducción a los códigos geométrico-algebraicos: ataque al criptosistema de McEliece

Introduction to algebraic-geometric codes: attack against McEliece cryptosystem

Laura Anguita Batista

Trabajo de Fin de Grado

Departamento de Matemáticas, Estadística e Investigación Operativa

Sección de Matemáticas

Universidad de La Laguna

La Laguna, 12 de marzo de 2015

Dra. Dña. **Evelia Rosa García Barroso**, con N.I.F. 42.851.422-F profesora Titular de Universidad adscrita al Departamento de Matemáticas, Estadística e Investigación Operativa de la Universidad de La Laguna

C E R T I F I C A

Que la presente memoria titulada:

"*Introducción a los códigos geométrico-algebraicos: ataque al criptosistema de McEliece.*"

ha sido realizada bajo su dirección por Dña. **Laura Anguita Batista**, con N.I.F. 54.059.277-P.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 12 de marzo de 2015

Agradecimientos

A Evelia García Barroso,
por fomentar en mí el deseo de superación,
subiendo siempre el listón un poquito más. Por brindarme
sus conocimientos inculcándome la rigurosidad que le caracteriza.
Por todas esas horas dedicadas a seleccionar
y corregir. Gracias, Evelia.

A Irene Márquez Corbella,
por su necesaria e inestimable ayuda. Es un placer haber contado
con su colaboración para poder desarrollar esta memoria con propiedad.
Por su paciencia en cada consulta. Gracias, Irene.

A Mª Victoria Reyes Sánchez,
por servirme de guía desde que empecé a formar parte
de la ULL. Gracias, Mariví.

A mi familia y amigos,
por la confianza depositada en mí. A todos, gracias.

Resumen

El estudio de los códigos geométrico-algebraicos es una atractiva teoría donde convergen conceptos abstractos de la Teoría de Curvas y problemas concretos de la ingeniería de la transmisión de información.

La memoria se divide en cuatro capítulos. En el primero se presentan los ingredientes necesarios para construir códigos, es decir, familias de palabras formadas por secuencias de símbolos pertenecientes a un conjunto finito. Nos centraremos en el estudio de la capacidad detectora y correctora de errores de un código, donde resulta necesario el cálculo de su distancia mínima. Concluye este primer capítulo con una breve introducción a los dos tipos fundamentales de sistemas criptográficos, esto es, de clave privada y de clave pública, poniendo de manifiesto la diferencia entre el propósito de éstos y la Teoría de Códigos correctores de errores.

A continuación se definen, en el segundo capítulo, los llamados códigos lineales, que no son más que subespacios vectoriales sobre cuerpos finitos. Se estudia cómo el proceso de codificación es sencillo para estos códigos y cómo el cálculo de la distancia mínima precisa un menor número de operaciones que para códigos generales. Se muestran como ejemplo los códigos Reed-Solomon generalizados (GRS). Se presenta un método de decodificación para códigos lineales denominado decodificación por par de códigos correctores (ECP). Por otra parte, siguiendo en la línea de la criptografía, se introduce el criptosistema de clave pública de McEliece, que es uno de los puntos de encuentro de la criptografía y la teoría de códigos. En dicho sistema la clave pública va a ser una matriz generadora de un código lineal que no revele su estructura y la capacidad correctora del mismo.

El capítulo tercero comienza con los conceptos y resultados de Geometría Algebraica necesarios para la construcción de un caso particular de códigos lineales: los códigos geométrico-algebraicos. Se estudia cómo construir dos tipos de los mismos. Los primeros se obtienen como evaluación de funciones del espacio de Riemann-Roch en un conjunto finito de puntos racionales de una curva algebraica proyectiva. Cuando se toma la recta proyectiva, que tiene género cero, se obtienen los códigos GRS. Los segundos se construyen mediante diferenciales en una curva proyectiva. Finalmente se muestra que unos se pueden obtener a partir de los otros.

La memoria concluye con un ataque en tiempo polinomial al criptosistema de McEliece para códigos geométrico-algebraicos, que se basa en la decodificación por ECP.

Palabras clave: código lineal, código geométrico-algebraico, decodificación por pares, criptosistema de McEliece

Abstract

The study of algebraic-geometric codes is an attractive theory where abstract concepts of Curve Theory and concrete problems in the engineering of information transmission meet.

This work is split into four chapters. In the first one we introduce the necessary ingredients for building codes, that is, a family of words formed by sequences of symbols that belong to a finite set. We focus on the study of the capability to detect and correct errors in a code, where it is necessary to calculate the minimum distance. This first chapter ends with a brief introduction to the two basic types of cryptosystems, which are the secret key and the public key, showing the differences between the purposes of Cryptography and the error-correction coding theory.

In the second chapter we define the so-called linear codes, which are vectorial subspaces over finite fields. We show how the coding process is simple for this kind of codes and that the number of operations required to calculate the minimum distance is lower than for general codes. As an example we give the generalized Reed-Solomon codes (GRS). We present a method of decoding for linear codes known as decoding by error correcting pair (ECP). On the other hand, following in the cryptography line, we introduce the McEliece public key cryptosystem, which is a meeting point between cryptography and the coding theory. In this system the public key is a non structured generator matrix of a linear code and its error-correction capability.

The third chapter begins with the necessary concepts and results of Algebraic Geometry to build a specific kind of codes: the algebraic-geometric codes. We study how to build two different kinds of those. The first kind is obtained as an evaluation of functions of Riemann-Roch space in a finite set of rational points of a projective algebraic curve. When we take the projective line, which has genus zero, GRS codes are obtained. The second kind is built by differentials on a projective curve. Finally we prove that ones can be obtained out of the others.

This Degree thesis concludes with a polynomial time attack on the McEliece public key cryptosystem based on algebraic-geometric codes, using ECP decoding method.

Keywords linear code, algebraic-geometric code, error correcting pair, McEliece cryptosystem

Índice general

Motivación y objetivos

Con frecuencia se dice que vivimos en la era numérica. En efecto, gran parte de los datos que son manejados día a día en nuestro entorno están en formato digital, esto es, numérico. No es extraño que uno de los problemas más importantes que genera la transmisión de la información digital sea el de los errores. Una pequeña alteración de la misma puede ocasionar que el mensaje se corrompa. Por tanto, son precisos mecanismos que permitan detectar cuándo se han producido errores y, si es posible, corregirlos recuperando la información original. Con este propósito nacen en los años 50 los códigos correctores de errores.

Este campo es el que motiva la elaboración de este Trabajo de Fin de Grado, ya que la teoría de códigos es hoy en día un área muy activa de las Matemáticas. Ésta forma un extenso y fructífero campo de interacción entre las Matemáticas y las tecnologías de la información, ya que conceptos y resultados abstractos proporcionan soluciones al problema de transmitir información de forma eficiente y segura. Un ejemplo de este fenómeno es el de los códigos cíclicos y BCH presentes en los discos compactos, basados en teoría de cuerpos finitos y conceptos como ideales, raíces de la unidad, etc. Sin embargo, no serán estos códigos, que pueden consultarse en [MC] y en [HF], los que se expongan en esta memoria. Los códigos que trataremos en este trabajo son los obtenidos a partir de curvas algebraicas. Por tanto, en la realización de este Trabajo de Fin de Grado se han afianzado conceptos estudiados en Álgebra lineal, Teoría de Galois, Álgebra Conmutativa, Curvas algebraicas y Análisis complejo a través de una aplicación práctica. Además de estos conocimientos adquiridos en el Grado, ha sido necesaria una introducción a campos de la Geometría Algebraica no estudiados en el mismo.

La posibilidad de aplicar las técnicas de la Geometría Algebraica sobre cuerpos finitos a la construcción de códigos fue introducida por el matemático ruso V. D. Goppa en los años 80. En 1973 había mostrado cómo usar funciones racionales sobre una recta proyectiva para construir ciertos códigos. El siguiente paso fue sustituir la recta proyectiva por una curva arbitraria y habilitar la maquinaria de la Geometría Algebraica para el estudio de los códigos obtenidos.

Otro sector candente en la actualidad es la Criptología. En toda comunicación secreta existe una lucha entre criptógrafos y criptoanalistas de manera que el éxito de unos representa siempre el fracaso de los otros. La criptografía basada en teoría de códigos es una interesante alternativa a los criptosistemas de clave pública basados en teoría de

números, ya que se conjetura que serán seguros ante ataques con ordenadores cuánticos. Unos de los muchos códigos propuestos para este tipo de criptosistemas son los códigos geométrico-algebraicos. Los objetivos de este Trabajo Fin de Grado es el estudio de dichos códigos incluyendo además un ataque al criptosistema de McEliece basado en los mismos publicado en 2014.

Capítulo 1

Introducción a la codificación y a la criptografía

1.1. Códigos correctores de errores

Los canales que usamos para transmitir información pueden distorsionar el mensaje y ocasionar errores en la recepción del mismo. Como respuesta a la necesidad de que la transmisión se realice de forma rápida y segura, los *códigos correctores de errores* tratan de detectar y, si es posible, corregir los errores que se producen en la transmisión de datos de forma que se pueda recuperar la información original. De forma esquemática, se codifica el mensaje, se transmite a través de un canal de comunicaciones, el destinatario recibe el mensaje codificado y se *decodifica* el mensaje recibido.

Se dice que un *alfabeto* es un conjunto finito de símbolos $\mathcal{A}$, que generalmente se identifica con algún conjunto númerico. Un *código* $\mathcal{C}$ es un subconjunto de todas las *palabras* que puedan formarse como secuencia de dichos símbolos. Las palabras de un código pueden ser de longitud variable o fija. En este último caso se hablará de *códigos de bloque* que son los que trataremos en esta memoria. Si $|\mathcal{A}| = q$, el código $\mathcal{C}$ se denominará *q-ario* y se denotará $\mathcal{A}_q$, y si q es primo, o potencia de primo, $\mathcal{A}_q$ se identificará con el cuerpo finito $\mathbb{F}_q$ de q elementos. Esta identificación permitirá aplicar a los problemas de codificación las nociones y propiedades de cuerpos finitos. En particular, si $q = 2$, se dirá que el código es binario.

Por tanto, codificar consiste en asociar de forma inyectiva a cada elemento de $\mathcal{A}_q^k$ uno de $\mathcal{A}_q^n$, donde n será la *longitud* del código. Hay entonces $n-k$ símbolos redundantes, es decir, que no forman parte del mensaje original. Al número $\frac{k}{n}$ se le llama *tasa de transmisión.*

Ejemplo 1.1.1. (Códigos de repetición) *Supongamos que se desea transmitir un mensaje cuyo contenido será Sí o No. La forma más simple es atribuir a cada palabra una palabra binaria, por tanto* $\mathcal{C}_1 = \{0, 1\}$. *Sin embargo, si se produjera un número impar de errores en el canal el receptor no podría darse cuenta. Para evitar esto, la primera idea consiste en doblar el tamaño del mensaje y se obtiene el código* $\mathcal{C}_2 = \{00, 11\}$. *Así, si*

el receptor recibiera la palabra 10 *sabría que no es una palabra del código pero no podría obtener el mensaje original. Si se triplica el mensaje se tiene el código* $\mathcal{C}_3 = \{000, 111\}$ *que permite detectar que, por ejemplo,* 001 *no es una palabra del mismo y además el receptor podría obtener el mensaje original* 000 *suponiendo que el número de errores haya sido mínimo.*

A continuación formalizamos estas ideas.

1.1.1. Detección y corrección de errores

Antes de decodificar es necesario asociar un elemento de $\mathcal{C}$ a cada elemento de $\mathcal{A}_q^n$ que pudiera recibir el receptor.

Definición 1.1.2. *Si* $x, z \in \mathcal{A}_q^n$*, se llama* distancia de Hamming *entre* x *y* z*, y se denota por* $d(x, z)$*, al número de coordenadas distintas que poseen. Así, la* distancia mínima *de un código* C *es*

$$d(\mathcal{C}) := \text{mín}\{d(x, z) : x, z \in \mathcal{C}, x \neq z\}.$$

Proposición 1.1.3. *La distancia de Hamming es una distancia en* $\mathcal{A}_q^n$*.*

Demostración. Si $x, y \in \mathcal{A}_q^n$, entonces $d(x, y) \geq 0$ y $d(x, y) = 0$ si, y solamente si $x = y$. Además, $d(x, y) = d(y, x)$. Consideremos ahora $z \in \mathcal{A}_q^n$ de modo que $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$ y $z = (z_1, \cdots, z_n)$. Definamos los conjuntos

$$T := \{i : x_i \neq z_i\},\ U := \{i : x_i \neq z_i \text{ y } x_i = y_i\},\ V := \{i : x_i \neq z_i \text{ y } x_i \neq y_i\}.$$

Entonces, $d(x, z) = |T| = |U| + |V|$. Dado que $|V| \leq d(x, y)$ y $|U| \leq d(y, z)$ se tiene $d(x, z) \leq d(x, y) + d(y, z)$. □

Dada una palabra $x \in \mathcal{A}_q^n$, el método de *decodificación por mínima distancia* consiste en obtener una palabra del código $c \in \mathcal{C}$ que verifique $d(x, c) = \text{mín}\{d(x, z) : z \in \mathcal{C}\}$.

Definición 1.1.4. *Sean* $s, t \in \mathbb{N}$*. Diremos que la* capacidad detectora *de un código* $\mathcal{C}$ *es* s *o que* $\mathcal{C}$ *es* s-detector*, si* s *es el mayor natural tal que al cometerse un número menor de errores la palabra resultante no pertenece al código. Diremos que la* capacidad correctora *de un código* $\mathcal{C}$ *es* t *o que* $\mathcal{C}$ *es* t-corrector*, si siempre que se cometan a lo sumo* t *errores la decodificación por mínima distancia proporciona la palabra correcta.*

Las siguientes proposiciones ponen de manifiesto que la distancia mínima de un código determina la capacidad detectora y correctora del mismo.

Proposición 1.1.5. *Sean* $\mathcal{C}$ *un código y* $d(\mathcal{C})$ *su distancia mínima. Entonces* $\mathcal{C}$ *es* $(d(\mathcal{C}) - 1)$*-detector.*

Demostración. Sean $c \in \mathcal{C}$ la palabra original y $z \in \mathcal{A}_q^n$ la palabra recibida. Supongamos que z tiene e errores con $e \leq d(\mathcal{C}) - 1$. Por ser $d(\mathcal{C})$ la dístancia mínima de $\mathcal{C}$ se tiene que $z \notin \mathcal{C}$. □

Proposición 1.1.6. *Sean $\mathcal{C}$ un código y $d(\mathcal{C})$ su distancia mínima. Entonces $\mathcal{C}$ es $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$-corrector, donde $\lfloor . \rfloor$ denota la parte entera inferior.*

Demostración. Sean $c \in \mathcal{C}$ la palabra original y $z \in \mathcal{A}_q^n$ la palabra recibida. Supongamos que z tiene e errores con

$$d(c,z) = e \leq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor. \tag{1.1}$$

Entonces, para cada $b \in \mathcal{C}$ se tiene que

$$d(\mathcal{C}) \leq d(b,c) \leq d(b,z) + d(z,c) = d(b,z) + e. \tag{1.2}$$

Por (1.1) y (1.2) se tiene que $2e+1 \leq d(\mathcal{C}) \leq d(b,z)+e$, de donde, $d(b,z) \geq e+1$. Por tanto, c es la única palabra del código que está a distancia e de z. □

Ejemplo 1.1.7. *Sean $\mathcal{C}_1$, $\mathcal{C}_2$ y $\mathcal{C}_3$ como en el Ejemplo 1.1.1. Entonces $d(\mathcal{C}_1) = 1$, $d(\mathcal{C}_2) = 2$ y $d(\mathcal{C}_3) = 3$. Por tanto, tal y como se intuye, no es posible detectar errores en las palabras de $\mathcal{C}_1$. En las palabras de $\mathcal{C}_2$ se puede detectar hasta 1 error pero no puede ser corregido, y en las palabras de $\mathcal{C}_3$ se pueden detectar hasta 2 errores y corregir hasta 1 error.*

1.2. Criptografía versus Teoría de códigos

La criptografía corresponde a la ciencia que estudia cómo proteger información mediante el cifrado. De forma paralela se desarrolla el criptoanálisis, que es la ciencia que estudia cómo romper el cifrado y acceder a la información protegida por él. Por tanto, la Teoría de códigos busca formas eficientes de codificar los datos para que los errores que puedan producirse en el canal de transmisión sean detectados, o incluso corregidos, mientras que en la criptografía el mensaje queda encubierto para que solamente un grupo reducido de receptores sea capaz de descifrarlo.
A grandes rasgos se distinguen dos tipos de sistemas criptográficos; criptografía simétrica o de clave privada y criptografía asimétrica o de clave pública. En la práctica se emplea una combinación de estos dos tipos de criptosistemas, puesto que los criptosistemas asimétricos presentan el inconveniente de ser computacionalmente más costosos que los primeros.

1.2.1. Criptografía simétrica

Es un método criptográfico monoclave, esto es, se usa la misma clave para cifrar y descifrar. El principal problema de este sistema es el necesario intercambio de clave previo a la comunicación y requiere, por tanto, un canal seguro.

1.2.2. Criptografía de clave pública

La ventaja de estos sistemas es que permiten solucionar uno de los problemas de la criptografía clásica, la distribución de las claves secretas a los participantes en la comunicación ya que se trata de sistemas en los que la clave de cifrado y descifrado son distintas. Las dos claves pertenecen al receptor del mensaje. Una de ellas puede hacerse pública sin

que por ello la seguridad de la clave secreta se vea afectada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública de cifrado del receptor, cifra su mensaje con esa clave y el receptor se ocupa de descifrarlo usando su clave oculta.
Una desventaja del cifrado asimétrico respecto al cifrado simétrico es que las claves deben ser de mayor longitud. Es decir, mientras que para algoritmos simétricos se considera segura a día de hoy una clave de 128 bits, para cifrados asimétricos se recomienda actualmente el uso de claves públicas de al menos 1024 bits.
Los sistemas de cifrado de clave pública se basan en *funciones de un sólo sentido*, esto es, funciones cuya computación es fácil en un sentido mientras que su inversión no resulta computacionalmente factible con los medios actuales.
El criptosistema de esta clase más extendido hoy en día es el RSA, que basa su seguridad en la complejidad del problema de la factorización de enteros grandes. Se pueden consultar más detalles del mismo así como el algoritmo de Diffie Hellman y el algoritmo ElGammal en [MC].

A pesar de que el propósito de los códigos correctores y el de los sistemas criptográficos es diferente, existen puntos de encuentro entre ambas teorías como veremos en el siguiente capítulo.

Capítulo 2

Códigos lineales

Dentro de los códigos correctores de errores se encuentran los llamados *códigos lineales*. En este capítulo se estudiará el proceso de codificación así como los parámetros de esta familia de códigos.

2.1. Definición y primeras propiedades

En lo que sigue, supondremos que el cardinal del alfabeto $\mathcal{A}$ es q, siendo q primo o potencia de primo, lo que permite identificar $\mathcal{A}$ con el cuerpo finito de q elementos $\mathbb{F}_q$.

Definición 2.1.1. *Se dice que un subconjunto $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un* [n,k,d]-código lineal q-ario *si $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k, longitud n y distancia mínima d.*

Dado que un código lineal es un subespacio de $\mathbb{F}_q^n$, para describirlo basta con dar una base del mismo. Llamaremos *matriz generatriz* o *generadora* del código $\mathcal{C}$ a la matriz de orden $k \times n$ que tiene por filas los vectores de la base de $\mathcal{C}$ elegida. Así, si G es una matriz generadora del código $\mathcal{C}$ se tiene

$$\mathcal{C} = \{\ aG\ :\ a \in \mathbb{F}_q^k\ \}.$$

Por tanto todo $[n, k, d]$-código lineal q-ario es el conjunto imagen de una aplicación lineal de $\mathbb{F}_q^k$ en $\mathbb{F}_q^n$.

Ejemplo 2.1.2. (Códigos Reed-Solomon generalizados) *Sean $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_q^n$ donde $\alpha_i \neq \alpha_j$ si $i \neq j$, $v = (v_1, \cdots, v_n) \in (\mathbb{F}_q \backslash \{0\})^n$ y k un entero tal que $1 < k < n$. Se define un* código Reed-Solomon generalizado *como*

$$GRS_k(\alpha, v) := \{(v_1 f(\alpha_1), ..., v_n f(\alpha_n))\ :\ f \in L_{k-1}\},$$

donde L_{k-1} denota el $\mathbb{F}_q$-espacio vectorial de dimensión k de polinomios sobre $\mathbb{F}_q$ de grado menor o igual que $k-1$. Consideremos la aplicación

$$\begin{array}{rcl} ev_{\alpha,v} : L_{k-1} & \longrightarrow & F_q^n \\ f & \longrightarrow & (v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)). \end{array}$$

Si $a, b \in \mathbb{F}_q$ *y* $f(x), g(x) \in L_{k-1}$ *se tiene que* $af(x) + bg(x) \in L_{k-1}$. *Además,*

$$ev_{\alpha,v}(af(x) + bg(x)) = a \cdot ev_{\alpha,v}(f(x)) + b \cdot ev_{\alpha,v}(g(x)),$$

de donde la aplicación $ev_{\alpha,v}$ *es lineal y por tanto todo código Reed-Somolon generalizado es lineal, pues* $\mathcal{C} = GRS_k(\alpha, v) = Im(ev_{\alpha,v})$. *Denotaremos la palabra del código* $ev_{\alpha,v}(f(x))$ *por* $f \in \mathcal{C}$.
Sea $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$, $a_i \in \mathbb{F}_q^n$, *tal que* $f \in Ker(ev_{\alpha,v}) = \{f \in L_{k-1} : ev_{\alpha,v}(f(x)) = 0\}$, *es decir,* $v_i f(\alpha_i) = 0$ *para todo* $i = 1, \cdots, n$. *De forma matricial se tiene*

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \end{bmatrix} \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix} = 0.$$

Dado que la matriz asociada es de rango máximo k, *pues es una matriz tipo Vandermonde, tenemos que el sistema homogéneo es compatible determinado y solo admite la solución trivial. Por tanto, la aplicación* $ev_{\alpha,v}$ *es inyectiva. Entonces cualquier base* $\{f_1(x), \cdots, f_k(x)\}$ *de* L_{k-1} *proporciona una base* $\{f_1, \cdots, f_k\}$ *del código* $\mathcal{C}$. *Tomando la base canónica de* L_{k-1}, *esto es,* $\{1, x, \cdots, x^{k-1}\}$, *se tiene que la* i*-ésima fila de la matriz generatriz respecto de dicha base es*

$$ev_{\alpha,v}(x^i) = (v_1\alpha_1^i, \cdots, v_j\alpha_j^i, \cdots, v_n\alpha_n^i),\ 0 \leq i \leq k-1.$$

Por tanto, una matriz generatriz de $GRS_k(\alpha, v)$ *es*

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_j & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_j\alpha_j & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v_1\alpha_1^i & v_2\alpha_2^i & \cdots & v_j\alpha_j^i & \cdots & v_n\alpha_n^i \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_j\alpha_j^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix}.$$

Para determinar la distancia mínima de un código de m palabras y entonces obtener su capacidad detectora y correctora, es necesario evaluar $d(x, y)$ en cada uno de los $\binom{m}{2}$ pares de elementos $x, y \in \mathcal{C}$. Sin embargo, el número de evaluaciones necesario se reduce si el código es lineal.

Definición 2.1.3. *Si* $\mathcal{C}$ *es un código lineal, el* peso *de* $x \in \mathcal{C}$ *es el número de componentes no nulas de* x, *esto es, la distancia de* x *a* $y = 0 \in \mathcal{C}$. *El* peso del código *es* $w(\mathcal{C}) = \text{mín}\{w(x) : x \in \mathcal{C}\}$.

Proposición 2.1.4. *Si* $\mathcal{C}$ *es un código lineal entonces* $w(\mathcal{C}) = d(\mathcal{C})$.

Demostración. Sean $x, y \in \mathcal{C}$. Por ser $\mathcal{C}$ lineal, se tiene que $x - y \in \mathcal{C}$. Además, $d(x, y) = d(x - y, 0) = w(x - y)$, por tanto

$$d(\mathcal{C}) = \text{mín}\{d(x, y) : x, y \in \mathcal{C}\} = \text{mín}\{w(x - y) : x, y \in \mathcal{C}\} = w(\mathcal{C}).$$

□

Como consecuencia, para el cálculo de $d(\mathcal{C})$ con $\mathcal{C}$ lineal, basta con evaluar el peso de las $m - 1$ palabras no nulas del código.

2.2. Generando nuevos códigos

En esta sección se estudiarán dos formas de obtener nuevos códigos a partir de otros existentes.

2.2.1. El código dual

Sea $\mathcal{C}$ un $[n, k, d]$-código lineal. Denotemos por $\cdot$ el producto escalar en $\mathbb{F}_q^n$. El *subespacio ortogonal* a $\mathcal{C}$ es

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

Dicho espacio coincide con las soluciones de un sistema homogéneo cuya matriz asociada H es de rango $n - k$. Dado que $Hx^t = 0$ si, y solamente si, $x \in \mathcal{C}$ y en particular $HG^t = 0$ siendo G la matriz generadora de $\mathcal{C}$, esta matriz H permite controlar si dado un vector éste pertenece o no al código y, por esto, se llama *matriz de control* del código $\mathcal{C}$. Esto motiva la siguiente definición:

Definición 2.2.1. *Sea $\mathcal{C}$ un $[n, k, d]$-código lineal. Se denomina* código dual *de $\mathcal{C}$ al subespacio ortogonal a $\mathcal{C}$.*

Se puede dar una definición del código $\mathcal{C}$ a partir de su matriz de control:

$$\mathcal{C} = \{x \in \mathbb{F}_q^n \text{ tal que } xH^t = 0\} = \{x \in \mathbb{F}_q^n \text{ tal que } Hx^t = 0\}.$$

Asimismo, si G es la matriz generadora de $\mathcal{C}$ entonces

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \text{ tal que } xG^t = 0\} = \{x \in \mathbb{F}_q^n \text{ tal que } Gx^t = 0\}.$$

Ejemplo 2.2.2. *Sea $\mathcal{C}$ un código binario cuya matriz generadora es*

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

Por tanto, $\mathcal{C} = \{x \in \mathbb{F}_2^4 \ : \ x = uG, \ u \in \mathbb{F}_2^3\}$, es decir,

$$\begin{aligned} u_1 + u_3 &= x_1 \\ u_2 + u_3 &= x_2 \\ u_3 &= x_3 \\ u_1 + u_2 + u_3 &= x_4, \end{aligned}$$

de donde se obtiene $x_1 + x_2 + x_3 + x_4 = 0$. *La matriz asociada a este sistema homogéneo es* $H = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$ *y por tanto* $\mathcal{C} = \{x \in \mathbb{F}_2^4 \ : \ xH^t = 0\}$.

El dual de un código dual es el propio código, ya que por definición $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$ y además $dim((\mathcal{C}^\perp)^\perp) = n - (n-k) = k = dim(\mathcal{C})$.
De todo esto se desprende que si G (respectivamente H) es una matriz generadora del código $\mathcal{C}$ (respectivamente de $\mathcal{C}^\perp$), G (respectivamente H) es una matriz de control de $\mathcal{C}^\perp$ (respectivamente de $\mathcal{C}$).

Además, la matriz de control de un código lineal $\mathcal{C}$ proporciona información sobre la distancia mínima de éste.

Proposición 2.2.3. *Sean* $\mathcal{C}$ *un código lineal y* H *una matriz de control de* $\mathcal{C}$. *La distancia mínima* $d(\mathcal{C})$ *es el mayor entero para el que* $d(\mathcal{C}) - 1$ *columnas cualesquiera de* H *son linealmente independientes, es decir,* $d(\mathcal{C}) - 1 = rango(H)$.

Demostración. Denotemos por $h^{(i)}$ a la i-ésima columna de la matriz de control H de $\mathcal{C} \subseteq \mathbb{F}_q^n$, es decir, $H = (h^{(1)}, \cdots, h^{(n)})$. Entonces $Hx^t = x_1h^{(1)} + \cdots + x_nh^{(n)}$ para cualquier $x \in \mathbb{F}_q^n$.
Sean $d(\mathcal{C})$ la distancia mínima de $\mathcal{C}$ y $x \in \mathcal{C}$ un vector de peso $d(\mathcal{C})$. Así,

$$0 = Hx^t = x_1h^{(1)} + \cdots + x_nh^{(n)},$$

donde solo $d(\mathcal{C})$ valores de los x_i son no nulos y por tanto solo $d(\mathcal{C})$ columnas de H aparecen en la igualdad anterior. De aquí se deduce que hay $d(\mathcal{C})$ columnas de H linealmente dependientes. □

Proposición 2.2.4. *Sean* $\mathcal{C}$ *un código lineal y* H *una matriz de control. Entonces* $d(\mathcal{C}) \leq n - k + 1$. *Esta cota se denomina* cota de Singleton *de* $\mathcal{C}$.

Demostración. Basta tener en cuenta que el rango de H es $n - k$, y por la Proposición 2.2.3 se tiene $d - 1 \leq n - k$. □

Proposición 2.2.5. *Todo código Reed-Solomon generalizado* $GRS_k(\alpha, v)$ *alcanza la cota de Singleton.*

Demostración. Sean $h(x) \in L_{k-1}$ un polinomio no nulo y r el número de raíces que $h(x)$ tiene en $\{\alpha_1, \cdots, \alpha_n\}$. El peso de $ev_{\alpha,v}(h(x))$ será

$$\#\{i : v_ih(\alpha_i) \neq 0\} = n - \#\{i : h(\alpha_i) = 0\} = n - r.$$

Dado que $h(x)$ tiene a lo sumo $k-1$ raíces se deduce que $w(ev_{\alpha,v}(h(x))) \geq n - (k-1) = n - k + 1$. Por tanto, $d(\mathcal{C}) = w(\mathcal{C}) \geq n - k + 1$ y oncluimos aplicando la Proposición 2.2.4. □

Proposición 2.2.6. *El código dual de un código Reed-Solomon generalizado* $GRS_k(\alpha, v)$ *es otro código Reed-Solomon generalizado* $GRS_{n-k}(\alpha, v')$.

Demostración. Sea G como en el Ejemplo 2.1.2. Consideremos la matriz H

$$\begin{bmatrix} v'_1 & v'_2 & \cdots & v'_j & \cdots & v'_n \\ v'_1\alpha_1 & v'_2\alpha_2 & \cdots & v'_j\alpha_j & \cdots & v'_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v'_1\alpha_1^i & v'_2\alpha_2^i & \cdots & v'_j\alpha_j^i & \cdots & v'_n\alpha_n^i \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v'_1\alpha_1^{n-k-1} & v'_2\alpha_2^{n-k-1} & \cdots & v'_j\alpha_j^{n-k-1} & \cdots & v'_n\alpha_n^{n-k-1} \end{bmatrix}.$$

Probemos que existe $v' \in (\mathbb{F}_q \backslash \{0\})^n$ tal que $GH^t = 0$ para concluir que el código dual de un código Reed-Solomon generalizado es también un código Reed-Solomon generalizado con el mismo parámetro α y v' como segundo parámetro.
Para cada $i = 0, 1, \cdots, k-1$ y cada $l = 0, 1, \cdots, n-k-1$ necesitamos que el producto escalar de la fila i de G y la fila l de H sea cero, esto es,

$$\sum_{j=1}^{n} v_j v'_j \alpha_j^{i+l} = \sum_{j=1}^{n} v_j v'_j \alpha_j^r, \quad 0 \leq r \leq n-2,$$

o de forma matricial

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \cdots & v_n\alpha_n^{n-2} \end{bmatrix} \begin{bmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_n \end{bmatrix} = 0.$$

Las posibles soluciones $(v'_1, \cdots, v'_n)$ son las palabras no nulas del código $GRS_1(\alpha, v')$. Como la distancia mínima de este último código es n, $(v'_1, \cdots, v'_n) \in (\mathbb{F}_q \backslash \{0\})^n$. □

En general, no es posible determinar la distancia mínima de $\mathcal{C}^\perp$ únicamente en términos de la distancia mínima de $\mathcal{C}$: en el Ejemplo 2.2.2 se tiene $d(\mathcal{C}) = 2$ y $d(\mathcal{C}^\perp) = 4$ en virtud de la Proposición 2.2.3, mientras que en el Ejemplo 2.1.2 se obtiene que $d(\mathcal{C}) = d(\mathcal{C}^\perp) = n - k + 1$ teniendo en cuenta las Proposiciones 2.2.5 y 2.2.6.

2.2.2. El código estrella

Sean $a, b \in \mathbb{F}_q^n$. Se denota por $*$ al producto

$$\begin{array}{rccl} * : \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (a, b) & \longrightarrow & (a_1 b_1, \cdots, a_n b_n). \end{array}$$

En general, dados dos subconjuntos $A, B \subseteq \mathbb{F}_q^n$, se denota $A * B$ al subespacio

$$A * B := \langle \{a * b \ : \ a \in A, b \in B\} \rangle.$$

Escribiremos $A^{(2)}$ para el producto $A * A$.

Ejemplo 2.2.7. *Sean $A = GRS_{t+2}(\alpha, v)$ y $B = GRS_{t+1}(\alpha, w)$. Se tiene que $A * B = GRS_{2t+2}(\alpha, v * w)$. En efecto, consideremos $a \in A$, $b \in B$, entonces $a = vf(\alpha)$ con grado menor o igual que $t+1$ y $b = wg(\alpha)$ con grado menor o igual que t. Por tanto, $a * b = (v * w)(fg)(\alpha)$ con grado menor o igual que $2t+1$ de donde se obtiene el resultado.*

2.3. Relación entre la matriz generadora y la matriz de control

La relación entre una matriz generadora de un código lineal y una matriz de control del mismo se puede expresar en términos de aplicaciones lineales. Sea S_G una aplicación cuya matriz asociada es la matriz generadora G de un $[n, k, d]$-código lineal q-ario y sea H una matriz de control del mismo. Si consideramos la sucesión

$$\mathbb{F}_q^k \xrightarrow{S_G} \mathbb{F}_q^n \xrightarrow{S_{Ht}} \mathbb{F}_q^{n-k},$$

entonces

$$ImS_G = KerS_{H^t}.$$

Por tanto, si conocemos la matriz de control H de un código lineal $\mathcal{C}$ podemos obtener una matriz generadora del código como la matriz que determina el núcleo de la aplicación S_{H^t}. Podemos calcularla mediante operaciones elementales en las columnas de H como pasamos a detallar.
Dado que $HI_n = H$, donde I_n denota la matriz identidad de orden n, se tiene $Ht_c(I_n) = t_c(H)$, siendo t_c la composición de un número finito de transformaciones elementales por columnas. En particular, $rango(t_c(I_n)) = rango(I_n) = n$, por lo que $t_c(I_n)$ es una matriz cambio de base que denotaremos P. Dado que $rango(H) = n-k$, hay k de las n columnas de H que dependen linealmente de las demás. Podemos hacer transformaciones elementales a las columnas de H hasta obtener una matriz que tiene k columnas que son nulas y las correspondientes columnas de la matriz P forman una base de $KerS_H = \mathcal{C}$.

Ejemplo 2.3.1. *Sean $\mathcal{C}$ un código lineal y*

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

una matriz de control de dicho código. La longitud del código es 4, y dado que el rango de H es 2, la dimensión del código es 2. Queremos encontrar una base de $KerS_{H^t}$ donde $S_{H^t} : \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^2$. Haciendo las transformaciones elementales que consisten en restar a la primera columna la tercera y a la segunda columna la cuarta, obtenemos

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

donde P es la matriz que resulta de aplicar las mismas transformaciones elementales a I_4, esto es,

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

Una base de $KerS_{H^t}$ es por tanto $\{(1, 0, 1, 0), (0, 1, 0, 1)\}$ y una matriz generadora de $\mathcal{C}$ es:

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

También se puede obtener una matriz de control de un código lineal $\mathcal{C}$ a partir de una matriz generadora del mismo ya que ésta es la matriz de control de $\mathcal{C}^{\perp}$.

En este caso, si $GP = t_c(G)$ es la matriz que se obtiene al aplicar transformaciones elementales por columnas a la matriz G hasta obtener una matriz de la forma $(I_k|0)$, entonces $P = (T|H^t)$ para cierta matriz T de orden $n \times k$ y se tiene $(I_k|0) = GP = G(T|H^t) = (GT|GH^t) = (GT|0)$. Por tanto $GT = I_k$. A la matriz T se le denomina *matriz pseudoinversa* de G. Esta matriz permite invertir el proceso de codificación y obtener el mensaje original, es decir, antes de añadir los dígitos redundantes. Si $(x_1, \cdots, x_k) \in \mathbb{F}_q^k$ es el mensaje sin codificar y $(y_1, \cdots, y_n) \in \mathbb{F}_q^n$ es el mensaje codificado se tiene que

$$(y_1, \cdots, y_n)T = (x_1, \cdots, x_k)GT = (x_1, \cdots, x_k).$$

Ejemplo 2.3.2. *Sea $\mathcal{C}$ un código binario de dimensión 3 y longitud 4 cuya matriz generadora es*

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

Haciendo las transformaciones elementales que consisten en restar la tercera columna a la cuarta, la primera columna a la tercera y la segunda columna a la cuarta, se obtiene

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

donde P es la matriz que resulta de aplicar dichas transformaciones elementales a la matriz I_4, es decir

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

Por tanto una matriz de control de $\mathcal{C}$ es $H = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}$, mientras que las tres primeras columnas proporcionan una matriz pseudoinversa de G:

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

Se tiene por tanto $GT = I_3$ y $GH^t = 0$.

2.4. Decodificación por par de códigos correctores

En esta sección introducimos la noción de *par de códigos correctores* para un código lineal $\mathcal{C}$, así como un método de decodificación con ellos recogido en [P] alternativo al

método de *decodificación por síndrome* para códigos lineales (ver [RS]), ya que este último no es eficaz desde el punto de vista computacional.

Definición 2.4.1. *Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código lineal. Se dice que un par (A, B) de códigos q-arios de longitud n es un* t-par de códigos correctores *(t-ECP) para $\mathcal{C}$ si se verifica*

1. $(A * B) \subseteq \mathcal{C}^\perp$,
2. $k(A) > t$,
3. $d(B^\perp) > t$,
4. $d(A) + d(\mathcal{C}) > n$.

Ejemplo 2.4.2. *Sean $A = GRS_{t+2}(\alpha, v)$ y $B = GRS_{t+1}(\alpha, w)$ dos códigos Reed-Solomon generalizados. Entonces (A, B) es un t-ECP de $\mathcal{C} = GRS_{2t+2}(\alpha, v * w)^\perp$. Basta comprobar que se verifican las cuatro condiciones de la Definición 2.4.1.*

1. *La inclusión $(A * B) \subseteq \mathcal{C}^\perp$ es consecuencia inmediata del Ejemplo 2.2.7.*
2. *La segunda condición se deduce de la igualdad $k(GRS_{t+2}(\alpha, v)) = t + 2$.*
3. *Por la Proposición 2.2.6 se tiene que $B^\perp = GRS_{n-t-1}(\alpha, w')$, para cierto $w' \in (\mathbb{F}_q \backslash \{0\})^n$. Dado que los códigos Reed-Solomon generalizados alcanzan la cota de Singleton (ver Proposición 2.2.5) concluimos*

$$d(B^\perp) = n - (n - t - 1) + 1 = t + 2 > t.$$

4. *Puesto que $d(A) = n - (t + 2) + 1 = n - t - 1$ y $d(\mathcal{C}) = n - (n - 2t - 2) + 1 = 2t + 3$, entonces $d(A) + d(\mathcal{C}) = n - t - 1 + 2t + 3 = n + t + 2 > n$, pues $t > 0$.*

2.4.1. Algoritmo de decodificación eficiente

En esta sección presentaremos un algoritmo de decodificación eficiente para códigos lineales. Sea $\mathcal{C}$ un código lineal q-ario de longitud n. Supongamos que el emisor envía $c \in \mathcal{C}$ y el receptor recibe la palabra $y \in \mathbb{F}_q^n$. Podemos escribir $y = c + e$, donde $e = (e_1, \cdots, e_n) \in \mathbb{F}_q^n$ es un vector error y supongamos que $w(e) \leq t$. Mostraremos a continuación cómo decodificar y mediante un t-par de códigos correctores para $\mathcal{C}$.

Sea (A, B) es un t-ECP para $\mathcal{C}$. Definimos

$$K_y = \{a = (a_1, \cdots, a_n) \in A \ : \ < y, a * b > = 0 \text{ para todo } b \in B\},$$

donde $< \cdot, \cdot >$ denota el producto escalar usual en $\mathbb{F}_q^n$. Nótese que si $A * B \subseteq \mathcal{C}^\perp$ se tiene $K_y = K_e$, pues $< y, a * b > = < c, a * b > + < e, a * b >$.

Sea J un subconjunto de $\{1, \cdots, n\}$. Definimos

$$A(J) = \{a \in A \ : \ a_j = 0 \text{ para todo } j \in J\}.$$

Denotemos por I el soporte de e, esto es, $I = \{i : e_i \neq 0\}$. Nos interesa obtener $A(I)$, ya que acota las posiciones donde el vector e tiene coordenadas no nulas. Por otra parte, K_y es computable a partir de los datos que tenemos. Se tiene además que

$$A(I) = K_y.$$

En efecto, sea $a \in A(I)$, entonces $< e, a > = 0$ de donde $0 = < e, a * b > = < y, a * b >$, luego $a \in K_y$.
Recíprocamente, sea $a \in K_y$. Dado que $0 = < y, a * b > = < e, a * b > = < e * a, b >$, para cualquier $b \in B$, entonces $e * a \in B^{\perp}$. Pero $w(e * a) \leq w(e) \leq t < d(B^{\perp})$, por tanto $e * a = 0$. De aquí se tiene, en particular, que a_i es nulo en las posiciones donde e_i no lo es, es decir, para todo $i \in I$, luego $a \in A(I)$.

Computamos K_y y tomamos un elemento $a \in K_y = A(I)$ no nulo. Esto es posible ya que $dim(A) > t$. Si $K_y = \{0\}$ la palabra recibida tendría $r > t$ errores ya que $A(I)$ es la intersección de $|I|$ hiperplanos en A y en particular se sabe que $A(I) = K_y$.

Al conjunto de posiciones de a nulas lo denotaremos por J y sabemos que I está contenido en J, ya que las coordenadas de las palabras de A son nulas en las posiciones donde el vector e no lo es.

Sea $\{v_1, \cdots, v_r\}$ una base de $\mathcal{C}^{\perp}$. Consideremos el siguiente sistema de ecuaciones lineales en las variables $x_1, \cdots, x_n$, siendo $x = (x_1, \cdots, x_n)$:

$$\begin{array}{c} < x, v_i > = < y, v_i >, \text{ para todo } i = 1, \cdots, r, \\ x_j = 0, \text{ para } j \notin J. \end{array} \tag{2.1}$$

es decir,

$$\begin{array}{c} < y - x, v_i > = 0, \text{ para todo } i = 1, \cdots, r, \\ x_j = 0, \text{ para } j \notin J. \end{array}$$

El espacio de soluciones será el de los vectores $x \in \mathbb{F}_q^n$ con $x_j = 0$ para $j \notin J$ tales que $y - x \in (\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$, por tanto el vector e es solución. Demostraremos a continuación que es la única. Sea x otra solución del sistema (2.1), entonces el producto escalar $< x - e, v >$ es nulo para todo $v \in \mathcal{C}^{\perp}$, de donde $x - e \in \mathcal{C}$. Además, puesto que x y e son soluciones de (2.1) entonces $w(x - e) \leq |J|$. Dado que $d(A) + d(\mathcal{C}) > n$ se tiene $|J| \leq d(\mathcal{C}) - 1$. En efecto, $|J| = n - |\text{supp } (a)| \leq n - d(A) < d(\mathcal{C})$. Por tanto $w(x - e) \leq d(\mathcal{C}) - 1$. Debe ser entonces $x - e = 0$ y queda probado que el sistema lineal (2.1) tiene al vector error e como única solución.

Concluimos entonces que el método de decodificación por par de códigos correctores se reduce a encontrar explícitamente el error e que lo obtenemos como la única solución del sistema (2.1).

Todo lo recogido en esta sección se resume en el siguiente teorema:

Teorema 2.4.3. *Si (A, B) es un t-par de códigos correctores para $\mathcal{C}$, entonces el siguiente algoritmo corrige t errores con complejidad $O(n^3)$.*

1.1 *Computar* K_y.

1.2 *Si* $K_y = 0$, *entonces ir al paso 3.2*

1.3 *Si* $K_y \neq 0$, *elegir un elemento a no nulo de* K_y. *LLamar* J *al conjunto de posiciones no nulas de* a.

2.1 *Computar el espacio de soluciones de (2.1).*

2.2 *Si (2.1) no tiene solución o tiene varias ir al paso 3.2.*

2.3 *Si (2.1) tiene solución única* x_0, *computar* $w(x_0)$.

2.4 *Si* $w(x_0) > t$, *entonces ir al paso 3.2*

3.1 *La palabra recibida se decodifica como* $y - x_0$. *Ir al paso 4.1*

3.2 *La palabra recibida tiene más de* t *errores.*

4.1 *Fin*

Demostración. Consecuencia de lo expuesto anteriormente salvo la complejidad que detallamos a continuación. En el algoritmo se resuelve un sistema lineal homogéneo de n ecuaciones con n incógnitas para computar K_y. Lo mismo ocurre para el sistema (2.1). Se localizan los ceros de un vector y se calcula el peso de un vector. Todas estas subrutinas tienen complejidad a lo sumo $O(n^3)$. □

2.5. Criptografía basada en códigos. Criptosistema de McEliece

La función unidireccional en un sistema de cifrado de clave pública puede estar basada en códigos correctores de errores.
McEliece introduce el primer criptosistema de clave pública de este tipo. La seguridad de este sistema se basa en la dificultad de decodificar un código lineal cualquiera del que no se conoce su estructura, o equivalentemente encontrar una palabra de peso mínimo si el tamaño del código es suficientemente grande. Por tanto, el criptosistema de McEliece utiliza un código del que se conoce un algoritmo de decodificación eficiente, que será la clave privada, pero enmascarándolo para presentar como clave pública un código general, con el fin de enfrentar al criptoanalista con un problema computacionalmente imposible de resolver a día de hoy.

Sea $\mathcal{F}$ una familia cualquiera de códigos lineales con un algoritmo de decodificación eficiente. Cualquier elemento de esa familia se puede representar por la tripleta $(\mathcal{C}, \mathfrak{A}_\mathcal{C}, t)$ donde $\mathfrak{A}_\mathcal{C}$ denota un algoritmo decodificador para $\mathcal{C} \in \mathcal{F}$ que corrige a lo sumo t errores. Sea $(\mathcal{C}, \mathfrak{A}_\mathcal{C}, t)$ un elemento de $\mathcal{F}$ y G una matriz generadora de $\mathcal{C}$ que no revele su estructura. Entonces la *clave pública* y la *clave secreta* se definen respectivamente por

$$\mathcal{K}_{pub} = (G, t) \text{ y } \mathcal{K}_{sec} = (\mathfrak{A}_\mathcal{C}).$$

Supongamos que $m \in \mathbb{F}_q^k$ es el mensaje a enviar. Se toma un vector error aleatorio $e \in \mathbb{F}_q^n$ con peso a lo sumo t, esto es, $w(e) \leq t$. Entonces $y = mG + e$ es la palabra cifrada.
El receptor obtiene el mensaje original aplicando $\mathcal{K}_{sec}$, es decir, el algoritmo de decodificación.

Capítulo 3

Códigos geométrico-algebraicos

3.1. Curvas algebraicas

En esta sección mostraremos algunos conceptos necesarios para el estudio de los llamados *códigos geométrico-algebraicos*.

Definición 3.1.1. *Sea k un cuerpo. Una* clausura algebraica de k *es un cuerpo K tal que $k \subseteq K$ y que satisface*

- *K es algebraicamente cerrado, es decir, todo polinomio en $K[x]$ tiene al menos una raíz en K, y*
- *Si L es un cuerpo tal que $k \subseteq L \subseteq K$ y L es algebraicamente cerrado, entonces $L = K$.*

Todo cuerpo tiene una única clausura algebraica (pág. 97, [C]) que denotaremos $\overline{k}$. Por ejemplo, $\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{F}}_4 = \overline{\mathbb{F}}_2$ y, en general, $\overline{\mathbb{F}}_{p^n} = \overline{\mathbb{F}}_p$.

De la definición se desprende que dado $f \in k[x]$ de grado n, entonces existen una unidad $u \in (\overline{k})^* := \bar{k}\backslash\{0\}$ y $\alpha_1, ..., \alpha_n \in \bar{k}$ (no necesariamente distintos) tales que $f(x) = u(x - \alpha_1)...(x - \alpha_n)$.

Definición 3.1.2. *Sean k un cuerpo y $f \in k[x, y]$. Llamaremos* curva algebraica afín de ecuación $f(x, y) = 0$ *al conjunto*

$$V_k(f) = C_f(k) := \{(a, b) \in k^2 \ : \ f(a, b) = 0\} \subseteq k^2.$$

Cuando se sobreentienda el cuerpo k, la denotaremos simplemente C_f.

Esta definición se puede generalizar a un número finito de polinomios como sigue:

Definición 3.1.3. *Sea S un subconjunto no vacío del anillo de polinomios $k[x_1, \cdots, x_n]$. Llamaremos* conjunto algebraico afín *de k^n definido por S al conjunto*

$$V_k(S) := \{a \in k^n \ : \ p(a) = 0 \text{ para todo } p \in S\}.$$

Cuando se sobreentienda el cuerpo k, lo denotaremos simplemente $V(S)$.

Definición 3.1.4. *Sea k un cuerpo. Definimos el* plano proyectivo $\mathbb{P}^2(k)$ *como*

$$\mathbb{P}^2(k) := (k^3 \backslash \{(0,0,0)\})/\backsim$$

donde $(X_0, Y_0, Z_0) \backsim (X_1, Y_1, Z_1)$ si y sólo si existe $\alpha \in k^*$ tal que $X_1 = \alpha X_0$, $Y_1 = \alpha Y_0$, y $Z_1 = \alpha Z_0$.

Denotaremos la clase de equivalencia de (X_0, Y_0, Z_0) en $\mathbb{P}^2(k)$ por $(X_0 : Y_0 : Z_0)$.
Recordemos que un polinomio se denomina *homogéneo* si todos sus términos tienen el mismo grado.
Dado que para todo $\alpha \in k^*$ y todo $F \in k[X, Y, Z]$ homogéneo de grado d se tiene

$$F(\alpha X, \alpha Y, \alpha Z) = (\alpha Z)^d f(\alpha X/Z, \alpha Y/Z) = \alpha^d F(X, Y, Z),$$

entonces $F(X_0, Y_0, Z_0) = 0$ si y sólo si $F(\alpha X_0, \alpha Y_0, \alpha Z_0) = 0$ para todo $\alpha \in k^*$. La relación $\backsim$ identifica (X_0, Y_0, Z_0) con $(\alpha X_0, \alpha Y_0, \alpha Z_0)$.

Definición 3.1.5. *Sean k un cuerpo y $F \in k[X, Y, Z]$ un polinomio homogéneo. Se define la* curva proyectiva *determinada por F como*

$$V_k(F) = C_F(k) := \{(a : b : c) \in \mathbb{P}^2(k) \ : \ F(a, b, c) = 0\} \subseteq \mathbb{P}^2(k).$$

La Definición 3.1.3 se puede extender al plano proyectivo.
A toda curva algebraica afín se le puede asociar una curva proyectiva de la forma siguiente:

Definición 3.1.6. *Sean k un cuerpo, $f \in k[x, y]$ de grado d, y $C_f(k)$ la curva asociada a $f(x, y)$. Definimos la* clausura proyectiva *de la curva $C_f(k)$ como $\overline{C}_f(k) := \{(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(k) \ : \ F(X_0, Y_0, Z_0) = 0\}$, donde $F(x, y, z) := z^d f(x/z, y/z) \in k[x, y, z]$ se denomina* homogeneización de f. *Cuando se sobreentienda el cuerpo k, la denotaremos $\overline{C}_f$ en lugar de $\overline{C}_f(k)$.*
Denominamos punto en el infinito *de $\overline{C}_f$ a cualquier punto $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(k)$ tal que $Z_0 = 0$. En otro caso lo llamaremos* punto afín.

De esta definición se desprenden dos observaciones:

- Multiplicando por una unidad de k, podemos suponer que al menos una de las coordenadas de todo punto en $\mathbb{P}^2(k)$ es 1.
- $f(x_0, y_0) = 0$ si y sólo si $F(x_0, y_0, 1) = 0$.

Sea f un polinomio (no necesariamente homogéneo), llamaremos *multiplicidad* de un punto P en f, y lo denotaremos $m_f(P)$, a la multiplicidad de P como cero de f. Cuando se sobreentienda el polinomio f, se denotará simplemente $m(P)$.

Definición 3.1.7. *Sea C_f una curva algebraica afín. Diremos que C_f es* irreducible *si tener $C_f = C_{f_1} \cup C_{f_2}$, donde C_{f_i} son curvas algebraicas afines, implica $C_{f_1} = \emptyset$ o $C_{f_2} = \emptyset$. Análogamente, si C_F es una curva algebraica proyectiva diremos que C_F es* irreducible *si tener $C_F = C_{F_1} \cup C_{F_2}$, donde C_{F_i} son curvas algebraicas proyectivas, implica $C_{F_1} = \emptyset$ o $C_{F_2} = \emptyset$.*

Sea Y un subconjunto de k^2. Definimos el conjunto

$$I(Y) := \{f \in k[x,y] \ : \ f(a,b) = 0, \text{ para todo } (a,b) \in Y\}.$$

De forma análoga, asociamos a $Y \subseteq \mathbb{P}^2(k)$ el conjunto

$$I(Y) := \{F \in k[X,Y,Z] \ : \ F \text{ homogéneo y } F(a,b,c) = 0 \text{ para todo } (a:b:c) \in Y\}.$$

Proposición 3.1.8. *$I(Y)$ es un ideal del anillo de polinomios.*

Demostración. Supongamos $Y \subseteq k^2$. Como el polinomio nulo se anula en cualquier punto de k^2, $0 \in I(Y)$. Sean $p, q \in I(Y)$ y $(a,b) \in Y$, entonces $p(a,b) - q(a,b) = 0 - 0 = 0$, de donde $p - q \in I(Y)$. Finalmente, sea $h \in k[x,y]$ se tiene que $p(a,b)h(a,b) = 0h(a,b) = 0$ y por tanto $ph \in I(Y)$. Se demuestra de forma análoga para $Y \subseteq \mathbb{P}^2(k)$. □

Nótese que el ideal $I(Y)$ está finitamente generado ya que el anillo de polinomios con coeficientes en un cuerpo es un anillo noetheriano.

Proposición 3.1.9. *Sean C y C' dos curvas algebraicas. Entonces $I(C \cup C') = I(C) \cap I(C')$.*

Demostración. Sea $f \in I(C \cup C')$, entonces para todo $a \in C \cup C'$ se tiene que $f(a) = 0$. En particular, si $a \in C \subseteq C \cup C'$, $f(a) = 0$, es decir, $f \in I(C)$. Análogamente, $f \in I(C')$ y concluimos que $f \in I(C) \cap I(C')$.
Recíprocamente, sea $f \in I(C) \cap I(C')$. Entonces $f \in I(C)$ y $f \in I(C')$. Así, para todo $c \in C \cup C'$ se tiene $f(c) = 0$ luego $f \in I(C \cup C')$. □

Definición 3.1.10. *Se dice que un ideal I de $k[x,y]$ es* primo *si dado $fg \in I$ entonces $f \in I$ o bien $g \in I$.*

Proposición 3.1.11. *Una curva algebraica (afín o proyectiva) C es irreducible si, y solamente si, $I(C)$ es un ideal primo.*

Demostración. Supongamos que $I(C)$ no es un ideal primo. Sean $f, g \notin I(C)$ tales que $fg \in I(C)$. Entonces se tiene que $f(a)g(a) = 0$, para todo $a \in C$. Además, existen $b_1, b_2 \in C$ tales que $f(b_1) \neq 0$ y $g(b_2) \neq 0$. Dado que $fg \in I(C)$, se deduce que $V(I(C)) \subseteq V(fg) = V(f) \cup V(g)$, es decir, $C \subseteq C_f \cup C_g$. Por tanto, $C = C \cap (C_f \cup C_g) = (C \cap C_f) \cup (C \cap C_g)$. Ahora bien, $C \cap C_f$ es distinto de C porque $b_1 \in C$ y $b_1 \notin C_f$. Análogamente, $C \cap C_g$ es también distinto de C, luego C no es irreducible.
Recíprocamente, supongamos que $C = C_1 \cup C_2$, donde $C_i \neq C$. En virtud de la Proposición 3.1.9, obtenemos que $I(C) = I(C_1 \cup C_2) = I(C_1) \cap I(C_2)$, de donde $I(C) \subsetneq I(C_i)$. Además $I(C) \subsetneq I(C_i)$ puesto que $C_i \neq C$. Por tanto existen polinomios $f_i \in I(C_i) \backslash I(C)$ y por ser $I(C_i)$ ideal, $f_1 f_2 \in I(C_i)$ y consecuentemente $f_1 f_2 \in I(C_1) \cap I(C_2) = I(C)$, lo que está en contradicción con la hipótesis de que $I(C)$ es primo. □

Sea C una curva algebraica (afín o proyectiva). Dos polinomios que se diferencian en un elemento de $I(C)$ tienen el mismo valor en cada punto de C. Por tanto, sus clases coinciden en el anillo cociente $k[x,y]/I(C)$.

Definición 3.1.12. *El anillo $k[x,y]/I(C)$ se denomina* anillo de coordenadas *de C y lo denotamos $k[C]$.*

Si C es irreducible el anillo de coordenadas es un *dominio de integridad*, es decir, si $f, g \in k[C]$ son tales que $fg = 0$, entonces necesariamente $f = 0$ o bien $g = 0$. Por tanto, podemos construir su cuerpo de fracciones que denotamos $\mathcal{F}(C)$. A continuación definimos

$$k(C) := \left\{ \frac{G(X,Y,Z)}{H(X,Y,Z)} \ : \ G, H \in \mathcal{F}(C) \text{ homogéneos del mismo grado} \right\} \cup \{0\}.$$

A los elementos de $k(C)$ los denominamos *funciones racionales*. Nótese que $k(C)$ es un k-espacio vectorial siendo $\cdot$ la restricción a $k \times k(C)$ del producto en $\mathcal{F}(C)$, esto es,

$$\begin{array}{rcl} \cdot : k \times k(C) & \longrightarrow & k(C) \\ (\lambda, \frac{g}{h}) & \longrightarrow & \lambda \frac{g}{h}. \end{array}$$

Cuando C es una curva proyectiva se tiene la igualdad $\mathcal{F}(C) = k(C)$ (ver página 7 de [H-vL-P]).

Teorema 3.1.13. (Teorema de Bézout) *Si $g, h \in k[x,y]$ son polinomios de grado d y e respectivamente sin componentes en común, entonces C_f y C_g tienen a lo sumo $d \cdot e$ puntos de intersección. Además, $\overline{C}_f(\overline{k})$ y $\overline{C}_g(\overline{k})$ se intersectan exactamente en $d \cdot e$ puntos de $\mathbb{P}^2(\overline{k})$ (contando multiplicidades).*

Demostración. Ver Lemma 14.4 y Theorem 14.7 de [G]. □

3.1.1. Singularidades y género de una curva

Las curvas que usaremos en la teoría de códigos geométrico-algebraicos serán las llamadas *lisas* o no singulares, que definimos a continuación.
Sean k un cuerpo y $f \in k[x,y]$. Si $k = \mathbb{R}$ o $\mathbb{C}$, definimos mediante el concepto de límite la derivada parcial de f con respecto a x que denotamos f_x. Si k es un cuerpo de característica $p > 0$, la definición usual de límite no tiene sentido. Sin embargo, podemos definir, para $f \in \mathbb{F}_q[x,y]$, las *derivadas parciales formales* siguiendo las reglas de derivación usuales.

Definición 3.1.14. *Sean k un cuerpo y $f \in k[x,y]$. Un* punto singular *de C_f es un punto $(x_0, y_0) \in k \times k$ tal que $f(x_0,y_0) = f_x(x_0,y_0) = f_y(x_0,y_0) = 0$. La curva C_f es* lisa *si no tiene puntos singulares. Análogamente, si $F(x,y,z)$ es un polinomio homogéneo entonces $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(k)$ es un* punto singular *de C_F si $F(X_0,Y_0,Z_0) = F_X(X_0,Y_0,Z_0) = F_Y(X_0,Y_0,Z_0) = F_Z(X_0,Y_0,Z_0) = 0$. La curva C_F es* lisa *si no tiene puntos singulares.*

Ejemplo 3.1.15. *Llamamos* curva de Klein *a la curva definida por $F = 0$ donde F es el polinomio homogéneo $X^3Y + Y^3Z + Z^3X \in \mathbb{F}_q[X,Y,Z]$. En general, se define la curva $\mathcal{K}_m$ por la ecuación*

$$X^M Y + Y^M Z + Z^M X = 0.$$

Supongamos que $m^2 - m + 1$ y q son primos entre sí. Las derivadas parciales de la ecuación son $mX^{m-1}Y + Z^m$, $mY^{m-1}Z + X^m$ y $mZ^{m-1}X + Y^m$. Supongamos que (x:y:z) es un

punto singular de la curva $\mathcal{K}_m$. Si m es divisible por la característica de $\mathbb{F}_q$, entonces $x^m = y^m = z^m = 0$, de donde $x = y = z = 0$, que es una contradicción.
Si m y q son coprimos, entonces

$$x^m y = -m y^m z = m^2 z^m x, \tag{3.1}$$

de donde

$$(m^2 - m + 1) z^m x = x^m y + y^m z + z^m x = 0.$$

Dado que $m^2 - m + 1$ es coprimo con la característica de $\mathbb{F}_q$, se tiene que $z = 0$ o bien $x = 0$. Si $z = 0$, por (3.1) se tiene que $x^m = -m y^{m-1} z = 0$ y $y^m = -m z^{m-1} x = 0$, luego $x = y = z = 0$. Análogamente se llega a la misma contradicción si $x = 0$. Por tanto $\mathcal{K}_m$ es lisa si $m^2 - m + 1$ y q son primos entre sí.

Nota 3.1.16. *En la Definición 3.1.14, la hipótesis $F(X_0, Y_0, Z_0) = 0$ no es necesaria. Si se tiene que $F_X(X_0, Y_0, Z_0) = F_Y(X_0, Y_0, Z_0) = F_Z(X_0, Y_0, Z_0) = 0$ entonces, por el Lema de Euler (Lemma 10.8, [G]), se concluye que $F(X_0, Y_0, Z_0) = 0$.*

En general, si $f \in k[x, y]$ es un polinomio de grado d tal que la curva $\overline{C}_f$ es lisa, se define el *género de C_f* (o de $\overline{C}_f$) como

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

Esta igualdad también se conoce como la *fórmula de Plücker*. Aunque el género de una curva singular también se puede definir, no lo necesitamos en esta memoria.

3.1.2. Puntos y funciones racionales y divisores de curvas

Definición 3.1.17. *Sean k un cuerpo y C_F una curva proyectiva plana. Para cualquier cuerpo K tal que $k \subseteq K$, diremos que un punto $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(K)$ es un* K-punto racional *en C_F si $F(X_0, Y_0, Z_0) = 0$. Denotaremos el conjunto de todos los K-puntos racionales de $C_F(k)$ por $C_F(K)$.*

Ejemplo 3.1.18. *Sea $\mathcal{K}_3$ la curva de Klein definida por $F = 0$ donde F es el polinomio homogéneo $X^3Y + Y^3Z + Z^3X \in \mathbb{F}_2[X, Y, Z]$. Los puntos racionales en $\mathbb{F}_2$ son $(1 : 0 : 0)$, $(0 : 1 : 0)$ y $(0 : 0 : 1)$. Además, hay dos $\mathbb{F}_4$-puntos racionales que son $(1 : 1 + \alpha : \alpha)$ y $(1 : \alpha : 1 + \alpha)$ siendo $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, donde $\alpha^2 = 1 + \alpha$.*

Definición 3.1.19. *Sea C_F una curva proyectiva definida sobre $\mathbb{F}_q$. Un* divisor *D en C_F es una suma formal $D = \sum_Q n_Q Q$, donde $n_Q \in \mathbb{Z}$, con $n_Q \neq 0$ para un número finito de Q, siendo cada Q un punto racional en C_F. Se dice que D es* efectivo *si $n_Q \geq 0$ para cualquier Q y escribimos $D \geq 0$. Definimos el* grado *del divisor D como* $\deg(D) = \sum n_Q$. *Finalmente, se define el* soporte *del divisor D como* $\operatorname{supp} D = \{Q : n_Q \neq 0\}$.

Definimos, en el conjunto de los divisores de una curva, la siguiente relación de orden parcial: dados dos divisores $D_1 = \sum_Q n_Q Q$ y $D_2 = \sum_P n_P P$, decimos que $D_1 \leq D_2$ si $n_Q \leq n_P$ para cualquier punto racional en C_F.

Podemos dotar al conjunto de divisores de una curva de estructura de grupo abeliano con la suma formal.
Sean $C = C_F(\mathbb{F}_q)$ y $C' = C_G(\mathbb{F}_q)$ curvas proyectivas definidas por dos polinomios homogéneos F y G de grado d y e respectivamente. Si las curvas no tienen componentes en común, el Teorema de Bézout garantiza $d \cdot e$ puntos de intersección $\{P_1, \cdots, P_n\}$ en $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ contando multiplicidades y se tiene

$$m(P_1) + \cdots + m(P_r) = d \cdot e, \quad 1 \leq r \leq d \cdot e.$$

Ejemplo 3.1.20. (Divisor intersección) *Llamamos* divisor intersección *de C y C' a*

$$\sum_{P_i \in C \cap C'} m(P_i) P_i,$$

siendo $m(P_i)$ la multiplicidad de P_i como cero de la curva $C \cap C'$. Por abuso de lenguaje denotaremos $C \cap C'$ a dicho divisor.

Ejemplo 3.1.21. *Sea C la curva de Klein del Ejemplo 3.1.18. Consideremos $P_1 = (0:0:1)$, $P_2 = (0:1:0)$ y L la recta de ecuación $X = 0$. Entonces L intersecta a la curva C en los puntos P_1 y P_2. Además, P_1 es un punto de multiplicidad 3 y P_2 es de multiplicidad 1 como puntos de $C \cap L$. Por tanto $C \cap L = 3P_1 + P_2$.*

De ahora en adelante, para simplificar notación, denotaremos C a una curva proyectiva plana lisa sobre el cuerpo $\mathbb{F}_q$ determinada por el polinomio homogéneo $F \in \mathbb{F}_q[X, Y, Z]$ que supondremos irreducible en $\mathbb{F}_q$, y por lo tanto la curva que determina también lo es.

Definición 3.1.22. *Sean C una curva sobre $\mathbb{F}_q$ y $f := g/h \in \mathbb{F}_q(C)$. Definimos el* divisor de f *como* $\operatorname{div}(f) := \sum_P m(P)P - \sum_Q m(Q)Q$, *siendo $\sum_P m(P)P$ el divisor intersección $C \cap C_g$ y $\sum_Q m(Q)Q$ el divisor intersección $C \cap C_h$.*

Consideremos la aplicación:

$$\begin{array}{rcl} v_P : \mathbb{F}_q(C) & \longrightarrow & \mathbb{Z} \\ & & \\ f = \frac{g}{h} & \longrightarrow & v_P(f) = \begin{cases} m_g(P) & \text{si } P \text{ es cero de } f, \\ -m_h(P) & \text{si } P \text{ es polo de } f, \\ 0 & \text{en otro caso,} \end{cases} \end{array}$$

siendo $m_g(P)$ (respectivamente $m_h(P)$) la multiplicidad de P en la curva C_g (respectivamente en C_h).
Obsérvese que v_P verifica

(i) $v_P(\lambda f) = v_P(f)$, para todo $\lambda \in \mathbb{F}_q^n \backslash \{0\}$,

(ii) $v_P(fg) = v_P(f) + v_P(g)$ y

(iii) $v_P(f + g) \geq \min\{v_P(f), v_P(g)\}$.

En particular, v_P es una *valoración discreta.*

Nota 3.1.23. *Podemos reescribir el divisor de f como*

$$\text{div } (f) = \sum_{P \in C} v_P(f)P.$$

Por tanto, se tiene que si $f, f' \in \mathbb{F}_q(C)$ *entonces*

(a) $\text{div } (\lambda f) = \text{div } (f)$, *para todo* $\lambda \in \mathbb{F}_q \backslash \{0\}$,

(b) $\text{div } (ff') = \text{div } (f) + \text{div } (f')$.

(c) $\text{div } (f+g) \geq \text{mín}\{\text{div } (f), \text{div } (g)\}$.

De la Definición 3.1.22 se desprende que div (f) determina los ceros y polos de f y cuáles son sus multiplicidades como tales.

Definición 3.1.24. *El divisor de una función racional se denomina* divisor principal. *Se dice que dos divisores* D *y* D' *son* linealmente equivalentes *si, y solo si,* $D - D'$ *es un divisor principal.*

El divisor de f no depende del representante de f escogido.

Nota 3.1.25. *El signo del grado de* div (f) *determina si* f *tiene más ceros que polos o viceversa. Obsérvese además que si* $k = \overline{k}$ *entonces* $\deg(\text{div } (f)) = 0$ *pues* $\deg(C \cap C_g) = \deg(C \cap C_h) = d \cdot e$.

3.1.3. El espacio de Riemann-Roch

Sea $D = \sum n_P P$ un divisor de C. El divisor D selecciona un número finito de puntos P, y les asocia un determinado entero n_P. Vamos a estudiar cuándo existe una función racional cuyos ceros sean, precisamente, los puntos escogidos, y con multiplicidades no inferiores a n_P.

Definición 3.1.26. *Sea* D *un divisor de una curva proyectiva plana lisa* C *definida sobre el cuerpo* $\mathbb{F}_q$. *Denominamos* espacio de funciones racionales *asociados a* D *a*

$$L(D) := \{f \in \mathbb{F}_q(C) \ : \ \text{div } (f) \geq -D\} \cup \{0\}.$$

Este espacio también se conoce como *espacio de Riemann-Roch.*
Nótese que div $(f) \geq -D$ equivale a que div $(f) + D$ es efectivo.

Proposición 3.1.27. $L(D)$ *es un* $\mathbb{F}_q$*-espacio vectorial de dimensión finita.*

Demostración. Probemos que es un subespacio vectorial de $\mathbb{F}_q(C)$. Sean $f, f' \in L(D)$. En virtud de la Nota 3.1.23 se tiene $\lambda f \in L(D)$, para cualquier $\lambda \in \mathbb{F}_q \backslash \{0\}$. Además, div $(f) + D \geq 0$ y div $(f') + D \geq 0$ de donde div $(f + f') + D \geq 0$ aplicando de nuevo la Nota 3.1.23. □

Nótese que si $D = -P$, entonces $L(D)$ es el conjunto de funciones racionales que tienen al menos un cero en P y ningún polo. La única función que verifica esto es la idénticamente nula, que está en $L(D)$ por definición. En general se tiene el siguiente resultado:

Lema 3.1.28. *Si* $\deg(D) < 0$ *entonces* $L(D) = \{0\}$.

Demostración. Si $\deg(D) < 0$, entonces se tendrá $\deg(\text{div }(f) + D) < 0$ para cualquier $f \in \mathbb{F}_q(C)$, luego $f \notin L(D)\backslash\{0\}$. □

Agrupando los coeficientes positivos y negativos del divisor D, podemos escribir $D = D_{pos} - D_{neg}$ y ahora D_{pos} y D_{neg} son divisores efectivos. Además, reescribimos div $(f) =$ (ceros de f) − (polos de f). Por lo tanto, div $(f) + D = D_{pos} -$ (polos de f) + (ceros de f) $- D_{neg}$. De aquí se deduce la idea de que $f \in \mathbb{F}_q$ está en $L(D)$ si y sólo si f tiene *suficientes ceros y no demasiados polos.*

El siguiente teorema es un resultado clásico que relaciona los ceros y los polos de una función. En particular, fijados dónde están los ceros y los polos y de qué orden son, el teorema nos da la dimensión del espacio de funciones que satisfacen esa condición.

Teorema 3.1.29. (Teorema de Riemann-Roch) *Sean C una curva proyectiva plana lisa de género g definida sobre $\mathbb{F}_q$ y D un divisor en C. Entonces*

$$\dim L(D) \geq \deg(D) - g + 1. \tag{3.2}$$

Además, si $\deg(D) > 2g - 2$*, entonces se obtiene la igualdad en (3.2).*

Demostración. Ver Theorem 1.4.2 de [L-W-X]. □

3.1.4. Diferenciales en una curva

Sea C una curva irreducible lisa con cuerpo de funciones $\mathbb{F}_q(C)$.

Definición 3.1.30. *Sea U un espacio vectorial sobre $\mathbb{F}_q(C)$. Se denomina* derivación *a toda $\mathbb{F}_q$-aplicación lineal $D : \mathbb{F}_q(C) \longrightarrow U$ que satisface la* regla del producto

$$D(fg) = fD(g) + gD(f).$$

El conjunto de todas las derivaciones $D : \mathbb{F}_q(C) \longrightarrow U$ se denotará $Der(C, U)$. En particular, si $U = \mathbb{F}_q(C)$ dicho conjunto se denotará $Der(C)$.

La suma de dos derivaciones $D_1, D_2 \in Der(C, U)$ se define como $(D_1 + D_2)(f) = D_1(f) + D_2(f)$. El producto de $D \in Der(C, U)$ con $f \in \mathbb{F}_q(C)$ se define $(fD)(g) = fD(g)$. Así, $Der(C, U)$ es un espacio vectorial sobre $\mathbb{F}_q(C)$, con las operaciones suma y producto antes definidas.

Se llama *parámetro local en un punto P* a toda función racional cuya valoración en P es 1. El siguiente teorema (ver Theorem 2.42 de [H-vL-P]) nos permite determinar una base de $Der(C)$.

Teorema 3.1.31. *Sea t un parámetro local en un punto P. Entonces existe una única derivación $D_t : \mathbb{F}_q(C) \longrightarrow \mathbb{F}_q(C)$ tal que $D_t(t) = 1$. Además, $Der(C)$ tiene dimensión uno sobre $\mathbb{F}_q(C)$ y D_t es una base del mismo para todo parámetro local t.*

Definición 3.1.32. *Se denomina* forma diferencial racional *o* diferencial *en C a toda $\mathbb{F}_q(C)$-aplicación lineal de $Der(C)$ en $\mathbb{F}_q(C)$. El conjunto de todas las formas diferenciales racionales en C se denota $\Omega(C)$.*

Obsérvese que $\Omega(C)$ es el espacio vectorial dual de $Der(C)$.

Consideremos la aplicación

$$d : \mathbb{F}_q(C) \longrightarrow \Omega(C),$$

donde se define, para $f \in \mathbb{F}_q(C)$, la diferencial $df : Der(C) \to \mathbb{F}_q(C)$ como $df(D) = D(f)$ para todo $D \in Der(C)$. Se tiene que d es una derivación.

Teorema 3.1.33. *El espacio $\Omega(C)$ es un $\mathbb{F}_q(C)$-espacio vectorial de dimensión 1 y dt es una base para cualquier punto P con parámetro local t.*

Demostración. Ya que $\Omega(C)$ es el espacio vectorial dual de $Der(C)$ se tiene que $\Omega(C)$ es un espacio vectorial sobre $\mathbb{F}_q(C)$ y $dim(\Omega(C)) = dim(Der(C)) = 1$. Por tanto, para obtener una base basta encontrar un vector en $\Omega(C)$ no nulo. Se tiene que $dt \in \Omega(C)$ y $dt(D_t) = D_t(t) = 1$ de donde se concluye el resultado. □

Deducimos del Teorema 3.1.33 que fijados un punto P y un parámetro local t_P, toda diferencial ω se escribe de forma única como $\omega = f_P dt_P$, donde f_P es una función racional. Usando la siguiente definición es posible determinar cuándo ω tiene un cero o un polo y de qué orden.

Definición 3.1.34. *Sea ω una diferencial en C. La* valoración *de ω en P se define como $v_P(\omega) = v_P(f_P)$. La forma diferencial ω se denomina* regular *si no tiene polos, es decir, si f_P no los tiene.*

El divisor de una diferencial se define de forma análoga al divisor de una función racional:

Definición 3.1.35. *Se llama* divisor *de una diferencial ω, y se denota* div (ω) *a*

$$\text{div } (\omega) = \sum_{P \in C} v_P(\omega) P.$$

Esta definición es consistente ya que solo un número finito de coeficientes en div (ω) son no nulos.

Se llama *divisor canónico* a todo divisor $W =$ div (ω), donde $\omega \in \Omega(C)$. Si ω' es cualquier otra diferencial no nula de $\Omega(C)$, entonces $\omega' = f\omega$ para cierta función racional f. Si $W' =$ div (ω') se tiene que W y W' son linealmente equivalentes. Por tanto, los divisores canónicos forman una clase de equivalencia lineal que por abuso de lenguaje también denotaremos W.
La siguiente definición no depende de la elección del parámetro local t.

Definición 3.1.36. *Sean P un punto en C, t un parámetro local en P y $\omega = fdt$ la representación de ω. La función racional f admite desarrollo en serie de Laurent $\sum_i a_i t^i$. Definimos el* residuo *de ω en P, y lo denotamos $Res_P(\omega)$, como a_{-1}.*

El siguiente resultado clásico en la teoría de curvas algebraicas se conoce como el *Teorema de los residuos* que enunciamos a continuación:

Teorema 3.1.37. *Si ω es una diferencial en una curva lisa proyectiva C, entonces*

$$\sum_{P \in C} Res_P(\omega) = 0.$$

Teorema 3.1.38. (Riemann-Roch generalizado) *Sean C una curva proyectiva lisa sobre $\mathbb{F}_q$ de género g, D un divisor en C y W un divisor canónico en C. Entonces*

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

(ii) $dim(L(W)) = g$.

Demostración. Ver Riemann-Roch Theorem (página 210) y Corollary 1 de [F]. □

El Teorema 3.1.38 nos permite determinar el grado de un divisor canónico.

Corolario 3.1.39. *Para cualquier divisor canónico W se tiene* $\deg(W) = 2g - 2$.

Demostración. La dimensión del espacio $L(0)$ es 1. Por tanto, sustituyendo W en D y aplicando (ii) del Teorema 3.1.38 en (i) de dicho teorema se tiene el resultado. □

Introducimos a continuación una generalización de la Definición 3.1.26.

Definición 3.1.40. *Sea D un divisor en la curva C. Definimos*

$$\Omega(D) = \{\omega \in \Omega(C) \ : \ \text{div } (\omega) - D \geq 0\}.$$

Obsérvese que $\Omega(D)$ es un espacio vectorial sobre $\mathbb{F}_q$. La conexión entre los espacios introducidos en las Definiciones 3.1.26 y 3.1.40 se muestra en el siguiente resultado.

Teorema 3.1.41. *Sea $W = \text{div } (\omega)$ un divisor canónico. Se tiene $dim(\Omega(D)) = dim(L(W - D))$.*

Demostración. La aplicación $\varphi : L(W - D) \to \Omega(D)$ definida como $\varphi(f) = fw$ es un isomorfismo. □

3.2. Códigos geométrico-algebraicos: definición y propiedades

En esta sección siempre trabajaremos con el cuerpo finito $\mathbb{F}_q$ y la letra k denotará un entero positivo.

Definición 3.2.1. *Sean C una curva proyectiva plana lisa, $\mathcal{P} = \{P_1, ..., P_n\}$ un conjunto de $\mathbb{F}_q-$puntos racionales en C y D un divisor en C tal que $\mathcal{P} \cap \text{supp } D = \emptyset$ con $\deg(D) < n$. El código geométrico-algebraico asociado a C, $\mathcal{P}$ y D es*

$$\mathcal{C}(C, \mathcal{P}, D) := \{(f(P_1), ..., f(P_n)) \ : \ f \in L(D)\} \subset \mathbb{F}_q^n.$$

Obsérvese que $\mathcal{C}(C, \mathcal{P}, D)$ es la imagen de la *aplicación evaluación*

$$\begin{array}{rcl} ev_{\mathcal{P}} : L(D) & \longrightarrow & F_q^n \\ f & \longrightarrow & ev_{\mathcal{P}}(f) = (f(P_1), ..., f(P_n)). \end{array}$$

Dado que la aplicación evaluación es lineal, $\mathcal{C}(C, \mathcal{P}, D)$ es un código lineal de longitud n.

Proposición 3.2.2. *La aplicación evaluación*

$$\begin{array}{rcl} ev_{\mathcal{P}} : L(D) & \longrightarrow & F_q^n \\ f & \longrightarrow & ev_{\mathcal{P}}(f) = (f(P_1), ..., f(P_n)). \end{array}$$

es inyectiva.

Demostración. Probemos que el núcleo de $ev_{\mathcal{P}}$ es trivial. Supongamos $ev_{\mathcal{P}}(f) = 0$. Entonces $f(P_1) = ... = f(P_n) = 0$, por lo tanto el coeficiente de cada P_i en div (f) es al menos 1. Ya que $\mathcal{P} \cap \text{supp } D = \emptyset$ tenemos que div $(f) + D - P_1 - ... - P_n \geq 0$, es decir, $f \in L(D - P_1 - \cdots - P_n)$. Dado que $\deg(D) < n$, entonces el divisor $D - P_1 - \cdots - P_n$ tiene grado negativo, y deducimos del Lema 3.1.28 que $L(D - P_1 - \cdots - P_n) = \{0\}$, luego $f = 0$ y se tiene el resultado. □

Corolario 3.2.3. *La dimensión del código $\mathcal{C}(C, \mathcal{P}, D)$ coincide con la dimensión del espacio vectorial $L(D)$.*

Demostración. Consecuencia inmediata de la Proposición 3.2.2. □

Teorema 3.2.4. *Sea C una curva proyectiva plana lisa de género g definida sobre $\mathbb{F}_q$. Sea $\mathcal{P} \subset C(\mathbb{F}_q)$ un conjunto de n $\mathbb{F}_q$-puntos racionales distintos en C y sea D un divisor en C tal que $\mathcal{P} \cap \text{supp } D = \emptyset$ con $2g-2 < \deg(D) < n$. Entonces el código geométrico-algebraico $\mathcal{C}(C, \mathcal{P}, D)$ es lineal de longitud n, dimensión $k = \deg(D) - g + 1$ y distancia mínima d, donde $d \geq n - \deg(D)$.*

Demostración. Sabemos que el código geométrico-algebraico $\mathcal{C}(C, \mathcal{P}, D)$ es lineal de longitud n y, por el Corolario 3.2.3, de dimensión igual a la dimensión de $L(D)$. Por el Teorema de Riemann-Roch tenemos que $dim(L(D)) = \deg(D) - g + 1$.
Para finalizar la demostración nos queda probar la cota sobre la distancia mínima. Sea $ev_{\mathcal{P}}(f) = (f(P_1), ..., f(P_n)) \in \mathcal{C}$ una palabra de peso mínimo d. Entonces $ev_{\mathcal{P}}(f)$ tiene exactamente d coordenadas no nulas. Supongamos, sin pérdida de generalidad, que $f(P_{d+1}) = ... = f(P_n) = 0$. En particular, div $(f) + D - P_{d+1} - ... - P_n \geq 0$ de donde $f \in L(D - P_{d+1} - ... - P_n)$. Además, dado que f es no nula se tiene que, en virtud del Lema 3.1.28 el divisor $D - P_{d+1} - ... - P_n$ tiene grado no negativo. Por tanto, $\deg(D) - (n - d) \geq 0$ y tenemos el resultado.

□

Proposición 3.2.5. *Los códigos Reed-Solomon generalizados son códigos geométrico-algebraicos.*

Demostración. Sea $GRS_k(\alpha, v)$ con matriz generadora

$$G = \begin{bmatrix} v_1 & v_2 & \cdots & v_j & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_j\alpha_j & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v_1\alpha_1^i & v_2\alpha_2^i & \cdots & v_j\alpha_j^i & \cdots & v_n\alpha_n^i \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_j\alpha_j^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix} \in \mathcal{M}_{k\times n}(\mathbb{F}_q).$$

Consideremos la curva proyectiva $C = \mathbb{P}^1$ dada por $z = 0$. Esta curva tiene género 0 y sus puntos son de la forma $(x : y)$. Sea $P_\infty = (1, 0)$ y $P_j = (a_j : 1)$ para todo $j = 1, \cdots, n$, donde $a_j \in \mathbb{F}_q$. Definimos $\mathcal{P} = \{P_1, \cdots, P_n\}$ y $D = (k-1)P_\infty$. Entonces, $dim(L(E)) = \deg(E) + 1 - g = k$ para $\deg(E) = k - 1 > 2g - 2$, y una base de $L(E)$ viene dada por

$$B_1 = \left\{1, \frac{x}{y}, \frac{x^2}{y^2}, \cdots, \frac{x^{k-1}}{y^{k-1}}\right\}.$$

Entonces el código $\mathcal{C} = (C, \mathcal{P}, E)$ tiene a G como matriz generadora con $v_i = 1$ para $i = 1, \cdots, n$.
Sea g un polinomio tal que $g(P_j) = v_j$ y consideremos $D := (k-1)P_\infty - \text{div }(g)$. Teniendo en cuenta la Nota 3.1.25 concluimos que $\deg(D) = k - 1$ y D es linealmente equivalente con $E = (k-1)P_\infty$. Además,

$$\begin{aligned} gL(E) &= \{gf \in \mathbb{F}_q(C) : \text{div }(f) + E \geq 0\} \cup \{0\} \\ &= \{gf \in \mathbb{F}_q(C) : \text{div }(f) + \text{div }(g) + D \geq 0\} \cup \{0\} \\ &= \{gf \in \mathbb{F}_q(C) : \text{div }(gf) + D \geq 0\} \cup \{0\} \\ &\subseteq \{h \in \mathbb{F}_q(C) : \text{div }(h) + D \geq 0\} \cup \{0\} = L(D). \end{aligned}$$

Por otro lado, por el Teorema de Riemann-Roch se tiene que $dim(L(D)) = k = dim(L(E)) = dim(gL(E))$ de donde $L(D) = L(E)$. Por tanto, una base de $L(D)$ viene dada por

$$B_2 = \left\{g, g\frac{x}{y}, g\frac{x^2}{y^2}, \cdots, g\frac{x^{k-1}}{y^{k-1}}\right\}.$$

Si D tiene soporte disjunto con $\mathcal{P}$, entonces el código $\mathcal{C}(C, \mathcal{P}, D)$ tiene a G como matriz generadora ya que $v_j = g(P_j)$ para $j = 1, \cdots, n$. □

Hemos definido los códigos geométrico-algebraicos a partir de las funciones racionales en $L(D)$. Podemos definir otra clase de códigos geométrico-algebraicos mediante diferenciales.

Definición 3.2.6. *El código lineal $\mathcal{C}^*(C, \mathcal{P}, E)$ de longitud n sobre $\mathbb{F}_q$ es la imagen de la aplicación lineal $\alpha^* : \Omega(E - D_\mathcal{P}) \to \mathbb{F}_q^n$ definida como*

$$\alpha^*(\mu) := (Res_{P_1}(\mu), \cdots, Res_{P_n}(\mu)),$$

donde $D_\mathcal{P} = P_1, \cdots, P_n$.

Teorema 3.2.7. *El código $\mathcal{C}^*(C,\mathcal{P},E)$ tiene dimensión $k^* = n - \deg(E) + g - 1$.*

Demostración. Por el Teorema 3.1.41 se tiene que $dim(\Omega(E - D_{\mathcal{P}})) = dim(L(W - E + D_{\mathcal{P}}))$. Dado que $\deg(E) < n$ se deduce que $\deg(W-E+D_{\mathcal{P}}) = 2g-2-\deg(E)+n > 2g-2$. Luego, en virtud del Teorema de Riemann-Roch, $dim(L(W - E + D_{\mathcal{P}})) = n - \deg(E) + g - 1$. La dimensión de $\mathcal{C}^*(C,\mathcal{P},E)$ se concluye tiendo en cuenta que la aplicación α^* es inyectiva. □

Teorema 3.2.8. *Los códigos $\mathcal{C}(C,\mathcal{P},E)$ y $\mathcal{C}^*(C,\mathcal{P},E)$ son códigos duales.*

Demostración. Aplicando el Corolario 3.2.3 y el Teorema 3.2.7 se tiene que $k+k^* = n$. Por tanto es suficiente tomar una palabra de cada código y probar que el producto escalar de ambas es nulo. Sean $f \in L(E)$ y $\mu \in \Omega(E-D_{\mathcal{P}})$. Sabemos que f no tiene polos en P_i. Dado que $\Omega(E-D_{\mathcal{P}})$ es un $\mathbb{F}_q(C)$-espacio vectorial se tiene que $f\mu \in \Omega(E-D_{\mathcal{P}})$ y por tanto sus únicos posibles polos son en tal caso los puntos P_i de orden a lo sumo 1. Si $\mu = gdt$ entonces $f\mu = fgdt$ y $Res_{P_i}(f\mu) = Res_{P_i}(fg) = f(P_i)Res_{P_i}(g) + g(P_i)Res_{P_i}(f) = f(P_i)Res_{P_i}(g)$ pues $Res_{P_i}(f) = 0$ para $i = 1,\cdots,n$. Aplicando el Teorema de los Residuos se tiene que $0 = \sum_i^n Res_{P_i}(f\mu) = \sum_i^n f(P_i)Res_{P_i}(\mu) = (f(P_1),\cdots,f(P_n))(Res_{P_1}(\mu),\cdots,Res_{P_n}(\mu))$. □

Los códigos geométrico-algebraicos definidos mediante el espacio de Riemann-Roch se conocen como *códigos geométrico-algebraicos Reed-Solomon*. Los que se construyen a través de diferenciales se denominan *códigos geométrico-algebraicos Goppa*. Gracias al siguiente resultado (Theorem 2.72 de [H-vL-P]) se puede suponer, sin pérdida de generalidad, que un código geométrico-algebraico es del tipo Reed-Solomon.

Teorema 3.2.9. *Sea C una curva proyectiva lisa definida sobre $\mathbb{F}_q$. Sea $\mathcal{P} = \{P_1,\cdots,P_n\}$ un conjunto de n puntos racionales y consideremos el divisor $D_{\mathcal{P}} = P_1+\ldots+P_n$. Entonces existe una forma diferencial ω con polos simples en P_i tal que $Res_{P_i}(\omega) = 1$ para todo $i = 1,\cdots,n$. Además*

$$\mathcal{C}^*(C,\mathcal{P},E) = \mathcal{C}(C,\mathcal{P},W + D_{\mathcal{P}} - E)$$

para cualquier divisor E que tenga soporte disjunto con $D_{\mathcal{P}}$, donde W es el divisor de ω.

Teorema 3.2.10. *El código $\mathcal{C}^*(C,\mathcal{P},E)$ tiene distancia mínima $d^* \geq \deg(E) - 2g + 2$.*

Demostración. En virtud de la Proposición 3.2.9 se tiene $\mathcal{C}^*(C,\mathcal{P},E) = \mathcal{C}(C,\mathcal{P},W+D_{\mathcal{P}}-E)$. Dado que $\deg(W+D_{\mathcal{P}}-E) = 2g-2+n-\deg(E)$, el resultado se concluye del Teorema 3.2.4. □

A modo de resumen recogemos los parámetros de un código geométrico-algebraico Reed-Solomon que serán últiles en el siguiente capítulo. Sea $\mathcal{C}(C,\mathcal{P},E)$ un código geométrico-algebraico Reed-Solomon. Se tiene:

1. Si $\deg(E) < n$ entonces
   - $k(\mathcal{C}) \geq \deg(E) - g + 1$ (Corolario 3.2.3),
   - $d(\mathcal{C}) \geq n - \deg(E)$ (Teorema 3.2.4).

Si además $2g-2 < \deg(E)$ se tiene $k(\mathcal{C}) = \deg(E) - g + 1$ (Corolario 3.2.3).

2. Si $\deg(E) > 2g-2$
   - $k(\mathcal{C}^\perp) \geq n - (\deg(E) - g + 1) = n - \deg(E) + g - 1$ (Teoremas 3.2.7 y 3.2.8),
   - $d(\mathcal{C}^\perp) \geq \deg(E) - 2g + 2$ (Teoremas 3.2.8 y 3.2.10).

   Si además $n > \deg(E)$ se tiene $k(\mathcal{C}^\perp) = n - \deg(E) + g - 1$.

3.3. Par de códigos correctores para un código geométrico-algebraico

Dada una curva C consideremos dos divisores E y F de la misma. Recordemos que $L(E)$ y $L(F)$ son subespacios vectoriales de $\mathbb{F}_q(C)$. Sea $L(E) \cdot L(F) := \{a \cdot b \ : \ a \in L(E),\ b \in L(F)\}$. Denotemos por $< L(E) \cdot L(F) >$ al subespacio generado por $L(E) \cdot L(F)$. Se tiene:

Teorema 3.3.1. *Sean E y F dos divisores en la curva C tales que $deg(E) \geq 2g$ y $deg(F) \geq 2g+1$, entonces*

$$< L(E) \cdot L(F) > = L(E+F)$$

Demostración. Ver Theorem 6 de [M]. □

Proposición 3.3.2. *Si E, F son dos divisores en la curva C con soporte disjunto a $D_P := P_1 + \cdots + P_n$, entonces*

$$\mathcal{C}(C, \mathcal{P}, E) * \mathcal{C}(C, \mathcal{P}, F) \subseteq \mathcal{C}(C, \mathcal{P}, E+F). \tag{3.3}$$

Si además $deg(E) \geq 2g$ y $deg(F) \geq 2g+1$, entonces se da la igualdad en (3.3).

Demostración. Sean $a = ev_{\mathcal{P}}(f) \in \mathcal{C}(C, \mathcal{P}, E)$ con $f \in L(E)$ y $b = ev_{\mathcal{P}}(g) \in \mathcal{C}(C, \mathcal{P}, F)$ con $g \in L(F)$, entonces se tiene que div $(f) \geq -E$ y div $(g) \geq -F$ de donde div $(fg) \geq -E-F$ y $fg \in L(E+F)$. Por tanto, $a * b = ev_{\mathcal{P}}(fg) \in \mathcal{C}(C, \mathcal{P}, E+F)$.

Para demostrar la igualdad, basta aplicar el Teorema 3.3.1. □

Corolario 3.3.3. *Sean E, F dos divisores en la curva C con soporte disjunto a $D_P := P_1 + \cdots + P_n$. Si $\deg(F) \geq 2g$ y $deg(E) \leq n-3$ entonces*

$$\Big(\mathcal{C}(C, \mathcal{P}, F) * (\mathcal{C}(C, \mathcal{P}, E))^\perp\Big)^\perp = \mathcal{C}(C, \mathcal{P}, E-F).$$

Demostración. Sean $A = \mathcal{C}(C, \mathcal{P}, F)$ y $B = \mathcal{C}(C, \mathcal{P}, E)$. Por el Teorema 3.2.9 se tiene que $B^\perp = \mathcal{C}(C, \mathcal{P}, E')$ con $E' = D_{\mathcal{P}} + W - E$, donde W es un divisor canónico en C. Por tanto, en virtud del Corolario 3.1.39, se tiene que $\deg(E') = n - \deg(E) + 2g - 2 \geq 2g+1$. Aplicando la Proposición 3.3.2 y el Teorema 3.2.9 se tiene que $A * B^\perp = \mathcal{C}(C, \mathcal{P}, D_{\mathcal{P}} + W - E + F) = \mathcal{C}(C, \mathcal{P}, E-F)^\perp$. □

Teorema 3.3.4. *Sean* $\mathcal{C} = \mathcal{C}(C, \mathcal{P}, E)^{\perp}$, $A = \mathcal{C}(C, \mathcal{P}, F)$, $B = \mathcal{C}(C, \mathcal{P}, E - F)$. *Si* $t^* = \left\lfloor \frac{d^*-1-g}{2} \right\rfloor$ *donde* d^* *es la distancia mínima del código* $\mathcal{C}$ *y se verifica que*

$$d(\mathcal{C}^{\perp}) = deg(E) - 2g + 2 \tag{3.4}$$

y

$$n > deg(F) = t + g, \tag{3.5}$$

entonces (A, B) *es un t-ECP de* $\mathcal{C}$.

Demostración. Aplicando la Proposición 3.3.2 se tiene que $A * B \subseteq \mathcal{C}^{\perp}$.
Por el Corolario 3.2.3 y aplicando (3.5) se obtiene $k(A) \geq t + 1 > t$.
Sabemos que

$$t^* = \left\lfloor \frac{d^* - 1 - g}{2} \right\rfloor = \left\lfloor \frac{\deg(E) - 2g + 2 - 1 - g}{2} \right\rfloor = \left\lfloor \frac{\deg(E) - 3g + 1}{2} \right\rfloor,$$

entonces $\deg(E - F) = \deg(G) - \deg(F) = \deg(E) - (t + g) = \deg(E) - 2t + t - g = \deg(E) - \deg(E) + 3g - 1 + t - g = 2g - 1 + t > 2g - 2 + t > 2g - 2$.
Por tanto, en virtud del Teorema 3.2.8, $d(B^{\perp}) \geq \deg(E-F)-2g+2 > t+2g-2-2g+2 = t$.
Finalmente, $d(A) + d(\mathcal{C}) \geq n - \deg(F) + \deg(E) - 2g = \deg(E - F) - 2g + 2 + n > n$, pues $\deg(E - F) > -2g + 2$. □

Corolario 3.3.5. *Sea* B *como en el Teorema 3.3.4, entonces si* $A = (B * \mathcal{C}(C, \mathcal{P}, E)^{\perp})^{\perp}$ *se tiene que* (A, B) *es un t-ECP de* $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$.

Demostración. Consecuencia inmediata del Corolario 3.3.3 y el Teorema 3.3.4. □

Capítulo 4

Ataque al criptosistema de McEliece

En este capítulo se presenta un ataque en tiempo polinomial para el criptosistema de clave pública de McEliece basado en códigos geométrico-algebraicos, recogido en [C-MC-P]. Se denotará por $\mathcal{P} = (P_1, P_2, \ldots, P_n)$ una n-upla de $\mathbb{F}_q$-puntos racionales distintos en C, donde C denota una curva proyectiva lisa en $\mathbb{F}_q$ de género g y E un $\mathbb{F}_q$-divisor de grado $m \in \mathbb{Z}$, cuyo soporte es disjunto a $D_{\mathcal{P}} := P_1 + \cdots + P_n$.

4.1. Cifrado de McEliece con códigos geométrico-algebraicos

Sabemos que la clave pública del criptosistema de McEliece es un par formado por una matriz generadora G y la capacidad correctora t del código lineal. En esta sección presentaremos el cifrado de McEliece basado en códigos geométrico-algebraicos, en particular $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$. El hecho de partir de un código dual no resta generalidad a la construcción ya que el código dual de un código geométrico-algebraico es otro código geométrico-algebraico (Teorema 3.2.8).
Tomaremos

$$t = \left\lfloor \frac{d^* - g - 1}{2} \right\rfloor$$

donde $d^* = m - 2g + 2$ se denomina *distancia mínima designada* del código $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$. Esta capacidad correctora, que es la capacidad de corrección real de un código lineal menos $\frac{g}{2}$, es razonable pues los algoritmos de decodificación para códigos geométrico-algebraicos que se conocían hasta el año 1993 solo permitían corregir hasta esa cota (Algoritmo de Skiribogatov-Vladut). Sin embargo, en 1993 Feng-Rao presenta el primer algoritmo que permite corregir hasta la mitad de la distancia mínima. Consideremos,

$$\mathcal{K}_{pub} := (G, t), \text{ con } t = \left\lfloor \frac{d^* - g - 1}{2} \right\rfloor. \tag{4.1}$$

Nota 4.1.1. *Asumimos $t>0$, es decir, que el código corrige al menos un error. De esto y*

de (4.1) se tiene

$$\deg(E) = m > 3g - 1.$$

4.2. Antes del ataque

El ataque consistirá en computar un t-ECP para decodificar $\mathcal{C} = \mathcal{C}(C, \mathcal{P}, E)^{\perp}$.
Recordemos que la clave pública del criptosistema de McEliece es una matriz generadora G y la capacidad correctora t del código $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$.
Sea E tal que

$$\frac{n}{2} - 2 > \deg(E) \geq 2g + 1. \tag{4.2}$$

En particular si $n \geq 2$ entonces $\deg(E) < \frac{n}{2} - 2 \leq n - 3$.

Lema 4.2.1. *Sea $\mathcal{C} = \mathcal{C}(C, \mathcal{P}, F)$ donde F es un divisor en C tal que $\deg(F) \geq 2g + 1$. Entonces*

$$\deg(E) = k(\mathcal{C}^{(2)}) - k(\mathcal{C}) \quad y \quad g = k(\mathcal{C}^{(2)}) - 2k(\mathcal{C}) + 1,$$

donde $\mathcal{C}^{(2)} = \mathcal{C} * \mathcal{C}$.

Demostración. En virtud de la Proposición 3.3.2 se tiene que $\mathcal{C}^{(2)} = \mathcal{C}(C, \mathcal{P}, 2F)$. Aplicando el Teorema de Riemann-Roch se deduce que $k(\mathcal{C}) = \deg(F) - g + 1$ y $k(\mathcal{C}^{(2)}) = \deg(2F) - g + 1$, de donde $\deg(E) = k(\mathcal{C}^{(2)}) - k(\mathcal{C})$ y consecuentemente $g = k(\mathcal{C}^{(2)}) - 2k(\mathcal{C}) + 1$. □

El Lema 4.2.1 nos permite determinar el divisor E y el género de la curva C del código secreto $\mathcal{C} = \mathcal{C}(C, \mathcal{P}, E)^{\perp}$. En efecto, las dimensiones de $\mathcal{C}$ y $\mathcal{C}^{(2)}$ son conocidas. Además, podemos escribir $\mathcal{C} = \mathcal{C}(C, \mathcal{P}, E)^{\perp} = \mathcal{C} = \mathcal{C}(C, \mathcal{P}, F)$ donde $F = W + D_{\mathcal{P}} - E$. Dado que $\deg \leq n - 3$ se tiene $\deg(F) \geq 2g + 1$ y estamos en condiciones de aplicar el Lema 4.2.1 que determina $\deg(F)$ y g. Finalmente, el valor de $\deg(E)$ se concluye teniendo en cuenta que $\deg(F) = 2g - 2 + n - \deg(E)$.

El Corolario 3.3.5 nos dice que es suficiente computar un código del tipo $\mathcal{C}(C, \mathcal{P}, E - F)$ con $\deg(F) = t + g$ para determinar un t-ECP del código $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$. Esto es equivalente a encontrar una matriz generadora de dicho código $\mathcal{C}(C, \mathcal{P}, E - F)$. Presentaremos en la siguiente sección un método en tiempo polinomial para computar dicha matriz generadora.

Consideremos la sucesión de códigos

$$(\mathcal{B}_i := \mathcal{C}(C, \mathcal{P}, E - iP_1))_{i \in \mathbb{N}}$$

donde $\mathcal{P} = (P_1, ..., P_n)$. Dado que $L(E - (i+1)P_1) \subseteq L(E - iP_1)$ se tiene que $\mathcal{B}_{i+1} \subseteq \mathcal{B}_i$. Entonces dado un elemento $c \in \mathcal{B}_i$, existe una $f \in L(E - iP_1)$ tal que $ev_{\mathcal{P}}(f) = c$ y por tanto div $(f) \geq -E + iP_1$.

Nota 4.2.2. *Para $i \geq 1$, el código $\mathcal{B}_i$ es* degenerado, *es decir $P \cap \text{supp}\ (E - iP_1) \neq \emptyset$.*

Obsérvese que el código $\mathcal{B}_0$ es el código dual del código secreto $\mathcal{C}(C,\mathcal{P},E)^{\perp}$ cuya matriz generadora es pública, luego la matriz generadora de $\mathcal{B}_0$ es la matriz de control de $\mathcal{C}(C,\mathcal{P},E)^{\perp}$, que se puede hallar por eliminación gaussiana. Además, para calcular $\mathcal{B}_1$ basta darse cuenta de que sus palabras son las de $\mathcal{B}_0$ cuya primera coordenada es nula. Haciendo eliminación gaussiana en la matriz generadora de $\mathcal{B}_0$ tenemos la de $\mathcal{B}_1$. En conclusión, los códigos $\mathcal{B}_0$ y $\mathcal{B}_1$ son conocidos.

4.3. El ataque

En esta sección computamos una matriz generadora del código $\mathcal{C}(C,\mathcal{P},E-F)$ con $\deg(F)=t+g$ para determinar un t-ECP del código $\mathcal{C}(C,\mathcal{P},E)^{\perp}$.

Proposición 4.3.1. *Si* $\frac{n}{2}-1>\deg(E)>2g+2$ *entonces*

$$\mathcal{B}_2=\{z\in\mathcal{B}_1 \text{ tal que } z*\mathcal{B}_0\subseteq\mathcal{B}_1^{(2)}=\mathcal{B}_1*\mathcal{B}_1\}.$$

Demostración. Sea $z\in\mathcal{B}_2\subseteq\mathcal{B}_1$, tenemos que probar que $z*\mathcal{B}_0\subseteq\mathcal{B}_1^{(2)}=\mathcal{C}(C,\mathcal{P},2E-2P_1)$, donde la última igualdad se obtiene de la Proposición 3.3.2 . Aplicando nuevamente esta proposición se tiene que $\mathcal{C}(C,\mathcal{P},E-2P_1)*\mathcal{C}(C,\mathcal{P},E)\subseteq\mathcal{C}(C,\mathcal{P},2E-2P_1)$ y se concluye el resultado.

Probemos que no existe $z\in\mathcal{B}_1\backslash\mathcal{B}_2$ tal que $z*\mathcal{B}_0\subseteq\mathcal{B}_1^{(2)}$. Supongamos por reducción al absurdo que un tal z existe. Entonces para cierta $f\in L(E-P_1)\backslash L(E-2P_1)$ tenemos que $ev_{\mathcal{P}}(f)=z$, esto es, div $(f)\geq -E+P_1$ y div $(f)\not\geq -E+2P_1$ y por tanto P_1 es un cero de orden 1 de f, es decir,

$$v_{P_1}(f)=1. \tag{4.3}$$

Dado que existen funciones en $L(E)$ que no se anulan en P_1 se tiene $\mathcal{B}_1\subsetneq\mathcal{B}_0$. Esto es equivalente a la existencia de $g\in L(E)\backslash L(E-P_1)$ tal que $ev_{\mathcal{P}}(g)\in\mathcal{B}_0\backslash\mathcal{B}_1$ y por tanto $v_{P_1}(g)$ no puede tomar valores positivos ya que de ser así P_1 sería un cero de g. Además, por ser $g\in L(E)$ se tiene div $(g)+E\geq 0$ y dado que $D_{\mathcal{P}}\cap E=\emptyset$ se deduce que $v_{P_1}(g)$ no toma valores negativos. Por tanto

$$v_{P_1}(g)=0. \tag{4.4}$$

Dado que $z*\mathcal{B}_0\subseteq\mathcal{B}_1^{(2)}$ entonces $ev_{\mathcal{P}}(fg)=ev_{\mathcal{P}}(f)*ev_{\mathcal{P}}(g)=z*ev_{\mathcal{P}}(g)\in\mathcal{B}_1^{(2)}=\mathcal{C}(C,\mathcal{P},2E-2P_1)$ y dado que div $(fg)\geq -2E+2P_1$ se tiene $v_{P_1}(fg)\geq 2$. Sin embargo de (4.3) y (4.4) se tiene

$$v_{P_1}(fg)=v_{P_1}(f)+v_{P_1}(g)=1,$$

que es una contradicción. □

La Proposición 4.3.1 se generaliza en el siguiente teorema:

Teorema 4.3.2. *Si* $i\geq 1$ *y* $\frac{n}{2}+i-2>\deg(E)>(2g+1)+i$ *entonces*

$$\mathcal{B}_{i+1}=\{z\in\mathcal{B}_i \text{ tal que } z*\mathcal{B}_{i-1}\subseteq\mathcal{B}_i^{(2)}=\mathcal{B}_i*\mathcal{B}_i\}.$$

Demostración. Dado que $\deg(E) - i \geq 2g + 1$, aplicando la Proposición 3.3.2 obtenemos la inclusión hacia la derecha.
Para demostrar la igualdad supongamos por reducción al absurdo que existe $z \in \mathcal{B}_i \backslash \mathcal{B}_{i+1}$ tal que $z * \mathcal{B}_{i-1} \subseteq \mathcal{B}_i^{(2)}$. Entonces podemos encontrar $f \in L(E - iP_1) \backslash L(E - (i+1)P_1)$ tal que $ev_{\mathcal{P}}(f) = z$ y $g \in L(E - (i-1)P_1) \backslash L(E - iP_1)$ tal que $ev_{\mathcal{P}}(g) \in \mathcal{B}_{i-1} \backslash \mathcal{B}_i$. De esto se tiene $v_{P_1}(f) = i$ y $v_{P_1}(g) = i - 1$ y por tanto $v_{P_1}(fg) = 2i - 1$. Por otro lado, dado que $z * \mathcal{B}_{i-1} \subseteq \mathcal{B}_i^{(2)}$ entonces $ev_{\mathcal{P}}(fg) \in \mathcal{B}_i^{(2)}$, de donde div $(fg) \geq -2E + 2iP_1$ y se tiene $v_{P_1}(fg) \geq 2i$ llegando a una contradicción. □

Resumiendo, podemos computar un subcódigo $\mathcal{C}(C, \mathcal{P}, E - F)$ de $\mathcal{C}(C, \mathcal{P}, E)$ para cierto divisor F con $\deg(F) = t + g$. Sin embargo, dado que el soporte de F no es disjunto con el de $\mathcal{P}$, el código $\mathcal{C}(C, \mathcal{P}, E - F)$ es degenerado y no puede usarse el Corolario 3.3.5 para la construcción de un ECP. A continuación se explica cómo hallar otro código $\mathcal{C}(C, \mathcal{P}, E - F')$, donde F' es linealmente equivalente con F, es decir, $F' = F + \text{div } (h)$ para cierta función racional h, tal que el soporte de F' es disjunto con el de $\mathcal{P}$. En particular, tomaremos $F = (t + g)P_1$ luego $F' = (t + g)P_1 + \text{div } (h)$.

Por tanto, vamos a estudiar cómo hallar una matriz generadora del código

$$\mathcal{C}(C, \mathcal{P}, E - (t + g)P_1 - \text{div } (h))$$

conociendo una matriz generadora de $\mathcal{B}_{t+g}$ y otra de $\mathcal{B}_{t+g+1}$.
Obsérvese que para todo $i \geq 1$ las palabras de $\mathcal{B}_i$ tienen primera coordenada nula ya que las de $\mathcal{B}_1$ la tienen y $\mathcal{B}_i \subset \mathcal{B}_1$ para todo $i \geq 2$.

Teorema 4.3.3. *Sea G una matriz generadora de $\mathcal{B}_{t+g}$ de la forma*

$$G = \left(\begin{array}{c|c} 0 & c_1 \\ \hline (0) & G_1 \end{array} \right),$$

donde $c_1 \in \mathbb{F}_q^{n-1}$ y $(\ 0 \mid c_1 \ ) \in \mathcal{B}_{t+g} \backslash \mathcal{B}_{t+g+1}$ y $(\ (0) \mid G_1 \ )$ es una matriz generadora de $\mathcal{B}_{t+g+1}$. Entonces, existe una función racional h en C tal que la matriz

$$G' = \left(\begin{array}{c|c} 1 & c_1 \\ \hline (0) & G_1 \end{array} \right)$$

es una matriz generadora de $\mathcal{C}(C, \mathcal{P}, E - (t + g)P_1 - \text{div } (h))$.

Demostración. Queremos hallar una matriz generadora de $\mathcal{C}(C, \mathcal{P}, E - (t+g)P_1 - \text{div } (h))$, lo que equivale a encontrar una base de dicho código. Por un lado se tiene, aplicando el Teorema de Riemann-Roch, que la dimensión del código $\mathcal{B}_{t+g+1}$ es una menos que la de $\mathcal{C}(C, \mathcal{P}, E - (t + g)P_1 - \text{div } (h))$.

Probaremos a continuación que $\mathcal{B}_{t+g+1} \subseteq \mathcal{C}(C, \mathcal{P}, E - (t+g)P_1 - \text{div } (h))$. En efecto, si $\phi \in L(E - (t + g + 1)P_1)$ entonces div $(\phi) + E - (t + g + 1)P_1 = \text{div } (\phi) + E - F - P_1 \geq 0$. Además, div $(\phi) + E - (t+g)P_1 - \text{div } (h) = \text{div } (\phi) + E - F' \geq \text{div } (\phi) + E - F - P_1$ ya que $F' = F + \text{div } (h)$ con $P_1 \notin \text{supp } (\text{div } (h))$. En consecuencia, $\phi \in L(E - (t+g)P_1 - \text{div } (h))$.

Además las filas de $((0) \mid G_1)$ forman una base S de $\mathcal{B}_{t+g+1}$. Basta completar dicha base con un vector linealmente independiente con ella. Por tanto, basta con encontrar $\phi \in L(E-(t+g)P_1 - \text{div}\,(h))$ tal que $ev_{\mathcal{P}}(\phi)$ sea linealmente independiente con los vectores de la base S. Dado que todos los vectores de S tienen primera coordenada nula, es suficiente con que $ev_{\mathcal{P}}(\phi)$ tenga la primera coordenada no nula. Sea $f \in L(E-(t+g)P_1)\backslash L(E-(t+g+1)P_1)$ tal que $(0 \mid c_1) = (f(P_1), \cdots, f(P_n))$. Entonces, $v_{P_1}(f) = t+g$. Aplicando Theorem 1.3.1 de [S] se tiene que existe una función racional $h \in \mathbb{F}_q(C)$ tal que

(i) $h(P_i) = 1$ para todo $i = 2, \cdots, n$.

(ii) $v_{P_1}(h) = -t-g$ y $hf(P_1) = 1$.

Se tiene por (ii) que $hf \in L(E-(t+g)P_1 - \text{div}\,(h))$. Además

$$ev_{\mathcal{P}}(hf) = ev_{\mathcal{P}}(h) * ev_{\mathcal{P}}(f) = (hf(P_1), \cdots, hf(P_n)) = (1 \mid c_1),$$

de donde se concluye el resultado considerando $\phi = hf$. □

Por tanto, podemos sintetizar el ataque en el siguiente esquema:

- **Paso 1:** Hallar los valores de g y $\deg(E)$.
- **Paso 2:** Obtener las matrices generadoras de los códigos $\mathcal{B}_0$ y $\mathcal{B}_1$ por eliminación gaussiana.
- **Paso 3:** Para $i = 2, \cdots, t+g+1$, computar $\mathcal{B}_i$ usando $\mathcal{B}_{i-1}$ y $\mathcal{B}_{i-2}$ en el Teorema 4.3.2.
- **Paso 4:** Utilizar $\mathcal{B}_{t+g}$ y $\mathcal{B}_{t+g+1}$ para hallar una matriz de un código no degenerado $\mathcal{B}' = \mathcal{C}(C, \mathcal{P}, E-(t+g)P_1 - \text{div}\,(h))$.
- **Paso 5:** Utilizar $\mathcal{B}'$ en el Corolario 3.3.5 para obtener un ECP del código $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$.

Nota 4.3.4. *El número de iteraciones puede reducirse teniendo en cuenta que si* $\frac{n}{2} + i - 2 > m \geq 2g + \left\lfloor \frac{i+1}{2} \right\rfloor + 1$, *entonces*

$$\mathcal{B}_i = \{z \in \mathcal{B}_{\lfloor (i+1)/(2) \rfloor} \text{ y } z * \mathcal{B}_0 \subseteq \mathcal{B}_{\lfloor i/2 \rfloor} * \mathcal{B}_{\lfloor (i+1)/2 \rfloor}\}.$$

Nota 4.3.5. *El ataque se aplica bajo la hipótesis* $\frac{n}{2} - 2 > \deg(E)$. *Esta condición puede ser debilitada considerando subcódigos de* $\mathcal{C}(C, \mathcal{P}, E)^{\perp}$. *Los detalles se pueden consultar en [C-MC-P].*

Capítulo 5

Conclusiones

Dentro de los códigos lineales, los códigos geométrico-algebraicos, objeto de estudio de esta memoria, forman una familia de códigos para los que existen algoritmos de decodificación eficientes que corrigen un número de errores muy próximo a la capacidad correctora real de un código lineal.

Sin embargo, su estructura hace que esta familia de códigos no sea una buena opción de cara a la Criptografía tal y como evidencia el ataque al criptosistema de McEliece basado en ellos. La clave de su vulnerabilidad reside en el hecho de que el cuadrado de un código geométrico-algebraico, a diferencia de otros códigos, permite obtener información de los mismos, en particular, el grado del divisor y el género de la curva utilizados.

Bibliografía

[C-MC-P] A. Couvreur, I. Márquez Corbella, R. Pellikaan, *A polynomial time attack against Algebraic Geometry code based public key crypto systems.* IEEE International Symposium on Information Theory (ISIT). pp. 1446 - 1450. IEEE, 24/01/2014.

[C] David A. Cox, *Galois Theory.* Wiley-Interscience, (2004)

[F] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry.* Addison-Wesley, (1989).

[G] C.G. Gibson, *Elementary Geometry of Algebraic Curves. An Undergraduate Introduction.* Cambridge : University press, (1998)

[HF] R. M. Hernández Falcón, *Introducción a la teoría de códigos: códigos cíclicos.* Trabajo Fin de Grado, ULL (2014).

[H-vL-P] T. Høholdt, J. H. van Lint, R. Pellikaan, *Algebraic geometry codes.* In the Handbook of Coding Theory, vol. I, (1998), 871-961.

[MC] I. Márquez Corbella, *Introducción a los aspectos geométrico-algebraicos de la teoría de códigos.* Trabajo académicamente dirigido (Universidad de La Laguna), Junio 2008.

[M] D. Mumford, *Varieties Defined by Quadratic Equations.* Questions on Algebraic Varieties. C.I.M.E. Summer Schools Volume 51, 1970, pp. 29-100.

[L-W-X] S. Ling, H. Wang, C. Xing, *Algebraic curves in cryptography.* CRC Press, (2013).

[P] R. Pellikaan, *On the efficient decoding of algebraic-geometric codes.* In *Eurocode '92 (Udine, 1992)*, volume 339 of *CISM Courses and Lectures*, pages 231-253. Springer, Vienna, 1993.

[RS] M. V. Reyes Sánchez, Notas sobre códigos correctores. Matemáticas de las comunicaciones. Máster en Matemáticas Avanzadas y Aplicaciones, ULL, Febrero 2013.

[S] H. Stichtenoth, *Algebraic function fields and codes,* volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

Introduction to algebraic-geometric codes: attack against McEliece cryptosystem

Laura Anguita Batista

Introduction to coding theory

As a response to the need of information transmision being fast and secure, the error correction coding theory tries to detect and correct errors that could have ocurred during the process of data transmision.
We say that a code $\mathcal{C}$ is a family of words formed by sequences of symbols that belong to a finite set.
The parameters of a code $\mathcal{C}$ are the length, which is the number of symbols that form each word, and minimum distance, that is

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

where $d(x,z)$ denotes the Hamming distance.
A code $\mathcal{C}$ detects $d(\mathcal{C})-1$ errors and corrects $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ errors.

Cryptography versus coding theory

Sometimes we want to protect the information that we send in order to let only a small group of receptors understand it. This is the Cryptography purpose. At large scale we can distinguish two kinds of cryptosystems.

- **Secret key cryptosystem**
  The same key is used to encrypt and decrypt.
- **Public key cryptosystem**
  The key to encrypt and to decrypt are not the same. Both keys belong to the transmitter. One of them is public and the other one is secret, which can't be deducted from the first of them.

Linear codes

Let $\mathbb{F}_q$ be the finite field with q elements. We say that $\mathcal{C}$ is a $[n,k,d]_q$-linear code if $\mathcal{C}$ is a k dimensional $\mathbb{F}_q$-vectorial space of length n and minimum distance d. Let G be a matrix which has the k vectors of a basis of $\mathcal{C}$ as its rows. Then

$$\mathcal{C} = \{\ aG\ :\ a \in \mathbb{F}_q^k\ \}$$

and we call this matrix generator matrix.
Let $\mathcal{C}^\perp$ be the orthogonal subspace of $\mathcal{C}$. We say $\mathcal{C}^\perp$ is the dual code of $\mathcal{C}$. If H is a generator matrix of $\mathcal{C}^\perp$ we have

$$\mathcal{C} = \{x \in \mathbb{F}_q^n\ :\ xH^t = \mathbf{0}\},$$

so that we call H parity check matrix of $\mathcal{C}$. We define the star code of two given codes as

$$A * B := \langle \{a * b\ :\ a \in A, b \in B\} \rangle,$$

where

$$\begin{aligned} * : \mathbb{F}_q^n \times \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ (a,b) &\longrightarrow (a_1b_1, \cdots, a_nb_n). \end{aligned}$$

We denote $\mathcal{C} * \mathcal{C} = \mathcal{C}^{(2)}$ and call it the square of the code $\mathcal{C}$.

Decoding method based on error correcting pair

Let A and B be linear codes. We say that (A,B) is an t-error correcting pair if they verify the following:

- $(A * B) \subseteq \mathcal{C}^\perp$,
- $dim(A) > t$,
- $d(B^\perp) > t$,
- $d(A) + d(\mathcal{C}) > n$.

There exists a decoding method for linear codes based on t-error correcting pair that corrects t errors with complexity $O(n^3)$.

McEliece cryptosystem

McEliece cryptosystem is one of the public key cryptographic system where the one directional function, which is a function that is easy to compute to one side but computionally imposible to the other one, is based on coding theory. The public key is a pair formed by a generator matrix of a linear code and its corrector capability.

Algebraic-geometric codes

Algebraic-geometric (AG) codes are linear codes based on curve theory. Let C be a projective smooth curve, $\mathcal{P} = \{P_1, ..., P_n\}$ a set of $\mathbb{F}_q$−rational points on C and $E = \sum_i n_{Q_i} Q_i$ a divisor on C that verifies $\mathcal{P} \cap \operatorname{supp} E = \emptyset$, where $\operatorname{supp} E = \{Q_i\ :\ n_{Q_i} \neq \mathbf{0}\}$, and $\mathbf{deg}(E) < n$. We define two kinds of AG codes.

- **AG Reed-Solomon codes**
  Let $L(E)$ be the Riemann-Roch space asociated to the divisor E. The algebraic-geometric code asociated to C, $\mathcal{P}$ and E is

$$\mathcal{C}(C,\mathcal{P},E) := \{(f(P_1), ..., f(P_n))\ :\ f \in L(E)\} \subset \mathbb{F}_q^n.$$

- **AG Goppa codes**
  The linear code $\mathcal{C}^*(C,\mathcal{P},E)$ of length n over $\mathbb{F}_q$ is the image of the linear map $\alpha^* : \Omega(E - D_\mathcal{P}) \to \mathbb{F}_q^n$ defined by

$$\alpha^*(\mu) := (Res_{P_1}(\mu), \cdots, Res_{P_n}(\mu)),$$

where $D_\mathcal{P} = P_1 + \ldots + P_n$, $\Omega(E - D_\mathcal{P})$ is the vectorial subspace of differentials asociated to the divisor $E - D_\mathcal{P}$ and $Res_{P_i}(\mu)$ denotes the residue of ω in the point P_i.
The codes $\mathcal{C}(C,\mathcal{P},E)$ and $\mathcal{C}^*(C,\mathcal{P},E)$ are dual codes.
We can consider, without losing generality, that every algebraic-geometric code is an algebraic-geometric Reed-Solomon code because

$$\mathcal{C}^*(C,\mathcal{P},E) = \mathcal{C}(C,\mathcal{P},W + D_\mathcal{P} - E)$$

for any canonical divisor W, where D_P has support disjoint from the support of E.

Attack against McEliece public key cryptosystem

We present a polynomial time attack against McEliece public key cryptosystem based on algebraic-geometric codes. The attack consists on finding an t-error correcting pair for a code of the form $\mathcal{C}(C,\mathcal{P},E)^\perp$. We summarize it in the following steps:

- Compute $\mathbf{deg}(E)$ and the genus of C and call it g.
- Consider the sequence of codes

$$(\mathcal{B}_i := \mathcal{C}(C,\mathcal{P},E - iP_1))_{i \in \mathbb{N}}$$

  and compute the generator matrix of $\mathcal{B}_{t+g+1}$.
- Obtain a matrix of a code from the ones of $\mathcal{B}_{t+g}$ and $\mathcal{B}_{t+g+1}$ tal que .
- Use this matrix to find an t-error correcting pair from the properties of the star operation $*$ of algebraic-geometric codes.

Conclusions

Among the linear codes, the algebraic-geometric codes form a family of codes for which exist eficient decoding algorithms that correct a number of error close to the real correct capability of a linear code. However, their structure is the reason why this family of codes is not a good choice facing the Cryptography as the attack on McEliece cryptosystem based on them shows. The key to its vulnerability lies in the fact that the square of an algebraic-geometric code, as opposing to other codes, allows to gather information of them, in particular, the degree of the divisor and the genus of the curve.

- A. Couvreur, I. Márquez Corbella, R. Pellikaan, *A polynomial time attack against Algebraic Geometry code based public key crypto systems*. IEEE International Symposium on Information Theory (ISIT). pp. 1446 - 1450. IEEE, 24/01/2014.
- T. Høholdt, J. H. van Lint, R. Pellikaan, *Algebraic geometry codes*. In the Handbook of Coding Theory, vol. I, (1998), 871-961.

alu0100624984@ull.edu.es