Universidad de Valladolid

Facultad de Ciencias

Grado en Matemáticas

Semigrupos numéricos, códigos AG en un punto y pesos de Hamming Generalizados

---

Autor: Jorge Angulo Rodriguez

Director: Diego Ruano Benito

Índice general

A Diego Ruano y José Ignacio Farrán, por la dirección y consejos.
A Pedro A. García-Sánchez, por mandarme su libro y ayudarme con la parte de GAP.
A Inés.

Introducción

Abstract

En este Trabajo de Fin de Grado vamos a introducir los conceptos básicos sobre semigrupos numéricos y el concepto de ideal de un semigrupo. Veremos la relación existente entre semigrupos numéricos y códigos algebraico geométricos en un punto (en particular, a través del semigrupo de Weierstrass). Los códigos AG en un punto son un tipo de códigos correctores AG, por lo que introduciremos los conceptos fundamentales de la teoría de códigos correctores y la teoría de códigos AG, así como las nociones necesarias de geometría algebraica. Generalizaremos el concepto de peso de Hamming (propio de la teoría de códigos correctores) y veremos cómo tiene aplicaciones a criptografía, en el problema de "wire-tap channel II".

Introdución

El primer capítulo está dedicado a los semigrupo numéricos, uno de los principales objetos de estudio del trabajo, y a conceptos asociados, como género, lagunas, conductor, etc. Un semigrupo numérico contiene, salvo un conjunto finito, todos los números naturales. A los elementos de dicho conjunto se los conoce como lagunas, y al cardinal del conjunto como género. Una forma de expresar un semigrupo es mediante un conjunto finito de generadores, A. En cuyo caso, todo elemento, x, del semigrupo se puede expresar como $x = \sum_{i=1}^{|A|} n_i a_i$, para ciertos $n_i \in \mathbb{N} \cup \{0\}$. Equivalentemente, si se conocen las lagunas, se conoce el semigrupo, pero conocer las lagunas no es un problema sencillo. De hecho, dar una formula cerrada para la mayor de las lagunas (el número de Fröbenius), en función de los generadores, es un problema abierto (Problema Fröbenius). Veremos que, para el caso especial, con dos generadores, es posible dar solución a este problema.

Existen otras alternativas, en base a otros conceptos que introduciremos (como la sucesión ν), que permiten caracterizar el semigrupo. En el Trabajo de Fin de Grado de informática, entro en más detalle en estas caracterizaciones desde el punto de vista computacional [13], implementando en GAP, como algoritmos, las caracterizaciones de un semigrupo a partir de la

sucesiones ν y τ, y la operación $\oplus$, siguiendo las descripciones de Maria Bras-Amorós en [4]. El objetivo final es expandir la librería GAP, "NumericalSpgs" [7], con funciones implementadas por mi.

El segundo capítulo está dedicado al concepto de ideal, un concepto típico de la teoría de anillos, pero que se puede generalizar a los semigrupos numéricos. Distinguimos un tipo especial de ideal, que estudiaremos por separado, cuando un ideal está estrictamente contenido en el semigrupo, que denominamos ideal propio. El objetivo principal del capitulo es estudiar la descomposición en irreducibles (para ambos tipos de ideal). Así, establecemos la base teórica, para en el TFG de informática poder implementar en GAP algoritmos de descomposición en irreducibles, que se incorporarán a la biblioteca "NumericalSpgs". En el contexto del trabajo, los conjuntos $D(x)$, que son fundamentales en el estudio de ideales propios irreducibles, jugarán un papel importante en el estudio de códigos en un punto, pues se usan para definir las sucesiones ν. En los textos de semigrupos los ideales no son tratados con frecuencia, pero recientemente P.A. García-Sánchez ha publicado un libro en el que dedica un capítulo al estudio de ideales [2]. También me he basado en el artículo [3].

El tercer capítulo trata la teoría de códigos correctores, tanto para introducir los conceptos necesarios para capítulos posteriores, como para estudiar los códigos correctores como tal. Los códigos correctores se estudian en el contexto de transmisión de información, donde se plantea una situación de comunicación entre emisor y receptor, a través de un canal con "ruido". Esto significa que, al transmitir información, se pueden producir errores, que pueden hacer que el mensaje resulte ininteligible para el receptor. Si introducimos redundancia en el mensaje es posible que, aunque sucedan errores, el receptor sea capaz de reconstruir el mensaje original pese a los errores. Por ejemplo, en una conversación, es posible no escuchar cierta palabra en una frase, pero deducirla por el contexto. A grandes rasgos, esta es la idea detrás de los códigos correctores; extender el mensaje, añadiendo redundancia, para poder corregir errores.

Las herramientas que estudiaremos para transmitir mensajes resistentes a errores son códigos correctores lineales. El problema se plantea como uno de codificación, donde consideramos el mensaje como un vector, $\mathbf{m}$, en un espacio vectorial de dimensión k, sobre un cuerpo finito, $\mathbb{F}_q$. Conceptualmete, puede pensarse en el mensaje como una secuencia de bits (aunque estudiamos el problema para q arbitrario). Así, codificar el mensaje $\mathbf{m}$, consiste en multiplicarlo, como vector, por una matriz, llamada matriz generatriz, que define el código. La imagen es un vector, $\mathbf{c}$, de longitud $n \geq k$ (ocupando "más espacio", pues se ha introducido redundancia). Cuando hablamos de código lineal, nos referimos al conjunto de todas las posibles "palabras" codificadas (vectores imagen), que constituye un subespacio vectorial de dimensión k de $\mathbb{F}_q^n$. Al transmitir el mensaje codificado, $\mathbf{c}$, si se producen errores, la información que llega al receptor

es $\mathbf{y} \in \mathbf{F}_q^n$, $\mathbf{y} \neq \mathbf{c}$. La diferencia entre el mensaje original y el modificado se denomina vector de error, $\mathbf{e}$. Así, al receptor le llega $\mathbf{y} = \mathbf{m} + \mathbf{e}$. Para recuperar el mensaje original, deberá realizar la tarea de decodificación y corrección de errores.

Obtener un algoritmo de decodificación eficiente, en general, no es sencillo, y es uno de los motivos por los que se estudian familias particulares de códigos correctores, donde se puede usar la información adicional para obtener un algoritmo rápido. Es deseable poder corregir el máximo número posible de errores, que se pueda decodificar de forma eficiente y que el mensaje codificado no tenga una longitud mucho mayor que el original, para tener baja redundancia. Estudiaremos este tipo de características en los códigos, así como algoritmos de codificación. En general, es difícil dar un algoritmo eficiente. En el capítulo 3 veremos algoritmos genéricos, aplicables a todos código lineal, mientras que en los capítulos 4 y 5 veremos algoritmos específicos a las familias de códigos estudiadas.

La distancia mínima (denotada por d) es de particular interés, pues conocerla permite saber la capacidad correctora de un código (el número máximo de errores que el código puede corregir), y viene dada por la expresión $\lfloor \frac{d-1}{2} \rfloor$. Como veremos, conocer la distancia mínima puede no ser sencillo, y por ello se recurre a cotas inferiores.

Otra aplicación de los códigos correctores es el problema "wire-tap channel II"[17] [1]. Nos encontramos ante un problema de criptografía en el que, al mandar un mensaje, un espía puede obtener información parcial del mismo, pudiendo leer cualesquiera μ bits del mensaje. Se plantea codificar el mensaje sin usar una clave, eligiendo una codificación tal que el espía tenga que tener acceso al mayor número posible de bits, μ, para poder deducir información útil sobre el mensaje original. Se puede usar un código lineal para este propósito, en cuyo caso, a partir del concepto de peso de Hamming generalizado, podemos dar cotas sobre la cantidad de información que, del mensaje original, el espía es capaz de deducir. El uso de un código corrector para este propósito permite proteger el mensaje frente a ruido y un espía a la vez.

Los dos últimos capítulos se centran en el estudio en detalle de unas familias de códigos lineales, códigos algebraico geométricos y códigos algebraico geométricos en un punto (un caso especial de los primeros).

En el cuarto capítulo introduciremos los conceptos necesarios de geometría algebraica para poder definir estos códigos, los códigos algebraico geométricos (o AG). Estos códigos surgen como resultado de evaluar funciones racionales, con un número de polos y ceros acotados, en un conjunto de puntos de una curva algebraica, de forma que dichas evaluaciones constituyan un espacio vectorial. En este capítulo, estudiaremos la familia de códigos AG, de forma ge-

neral, y daremos resultados sobre la longitud y la distancia mínima. Para los códigos AG, no es fácil calcular la distancia mínima, por lo que se trabaja a menudo con cotas inferiores, que permiten estimar el mínimo número de errores que el código es capaz corregir. Estudiaremos resultados que nos permitan obtener tales cotas. Así mismo, describiremos un algoritmo de decodificación, basado en los conceptos de síndrome y función localizadora de errores.

Los códigos en un punto resultan de particular interés por su relación con los semigrupos numéricos, por ello serán el objeto principal de estudio del último capítulo. Se definen a partir de curvas que presentan polos en un único punto. Vemos que, dada una curva con esta propiedad, es posible definir un semigrupo numérico, el semigrupo de Weierstrass. Esto nos permite aplicar conceptos de semigrupos en el estudio. Uno de los resultados que veremos, que ilustra esta conexión entre semigrupos y códigos en un punto, es que, el género del semigrupo de Weierstrass y el género de la curva que lo define, son el mismo.

Asociados al semigrupo de Weierstrass, introduciremos una serie de conceptos, como la sucesión ν y la operación $\oplus$, que serán útiles en el estudio de los códigos en un punto. La primera aplicación de los mismo es a un algoritmo de decodificación. El algoritmo que estudiaremos se basa en un sistema de votación (Berlekamp–Massey–Sakata [11]), en el cual, mediante dicho sistema de votación, se construye una función localizadora de errores.

Al igual que el capítulo 4, nos interesa el estudio de cotas para la distancia mínima y, a través del semigrupo de Weierstrass, es posible definir las distancias de Feng-Rao y de Feng-Rao generalizadas, que son instrumentales para dar dichas cotas.

Veremos también que las distancias de Feng-Rao guardan relacionar con los pesos de Hamming generalizados, y que podemos usarlas para acotarlos; obteniendo así una aplicación final de estos conceptos al problema de “wire-tap channel II”. Estas distancias de Feng-Rao son también objeto de estudio del TFG de informática.

Capítulo 1

Introducción a semigrupos numéricos

Los semigrupos, en particular los semigrupos numéricos, son uno de los conceptos fundamentales de este trabajo, por ello en este capítulo realizaremos una introducción de algunos de los conceptos más básicos sobre semigrupos.

Definición 1.1: Sea $\mathbb{N}_0$ el conjunto delos números naturales con el 0.

- Un **semigrupo** es un par $(S, +)$, donde S es un conjunto y $+$ es una operación binaria y asociativa en S.
  Además, en este trabajo consideraremos que, siempre que no se especifique lo contrario, dicha operación es conmutativa. En general denotaremos por S a los semigrupos conmutativos (omitiendo también la operación en la notación).

- Trataremos, principalmente, con los semigrupos numéricos, es decir, semigrupos cuyos elementos son números naturales y donde la operación " $+$ " es la suma habitual. Dicha operación tiene elemento unitario 0. Pediremos como requisito que el cero forme parte del semigrupo. Consideramos además los semigrupos con la propiedad adicional de tener complemento finito en $\mathbb{N}_0$. Es decir, $S \subseteq \mathbb{N}_0$ es **un semigrupo numérico** si:

  1. $0 \in S$
  2. Si $\forall s, s' \in S$, entonces $(s + s') \in S$
  3. $|\mathbb{N}_0 \setminus S| < \infty$

Ejemplos 1.1:

- Los números naturales con la suma habitual $(\mathbb{N}, +)$ son un semigrupo.

- También podemos ver un ejemplo usando la librería "NumericalSgps"para el sistema GAP:

```
gap> s1 := NumericalSemigroup("generators",7,11,15);
Numerical semigroup with 3 generators
gap> SmallElementsOfNumericalSemigroup(s1);
[0,7,11,14,15,18,21,22,25,26,28,29,30,32,33,35,36,37,39]
```

La función "NumericalSemigroup ("generators ", 7, 11, 15)"define un objeto semigrupo numérico generado por 7, 11 y 15.

SmallElementsOfNumericalSemigroup muestra los elementos del semigrupo menores iguales al conductor (definimos conductor más adelante).

Es sencillo ver que la intersección de semigrupos es también un semigrupo:
Si $\{S_i\}_{i\in I}$ es una familia de semigrupos numéricos, $a, b \in \cap_{i\in I} S_i$ entonces $(a+b) \in \cap_{i\in I} S_i$

Para indicar que en un semigrupo numérico S que todos los naturales a partir de un cierto elemento $\alpha_h \in S$ están en el semigrupo, usaremos la notación $\{\alpha_1, \ldots, \alpha_h, \rightarrow\}$ por ejemplo: $\{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\} = \{0, 3, 6, 7, 9, 10, 12, \rightarrow\}$.
En general podemos definir el semigrupo generado por un subconjunto como:

Definición 1.2: Dado un semigrupo S y $A \subset S$ podemos definimos el semigrupo generado por dicho subconjunto como $\langle A\rangle = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \quad | \quad n \in \mathbb{N}, \lambda_1, \ldots, \lambda_n \in \mathbb{N} \quad y \quad a_1, \ldots, a_n \in A\}$. Dado $S' = \langle A\rangle$, decimos que A es un sistema de generadores de S', y que es un sistema minimal si ningún subconjunto propio del mismo genera el semigrupo completo. Si se trata de semigrupos numéricos, consideramos que el 0 está incluido.

Ejemplo 1.2: Dado el conjunto $A = \{3, 7\}$ obtenemos el semigrupo

$$S = \langle A\rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, \ldots\}.$$

Dado que $\mathbb{N}_0 \setminus S = \{1, 2, 4, 5, 8, 11\}$, es finito, S es un semigrupo numérico.

Notemos que, cuando hablemos de semigrupos numéricos, no todo conjunto de números naturales genera un semigrupo. La tercera condición en la definición, excluye, por ejemplo, el semigrupo generado por un solo elemento $a > 1$, ya que se su complemento en $\mathbb{N}_0$ no es finito. La siguiente proposición describe en que casos un conjunto de de enteros no negativos engendra un semigrupo numérico:

Proposición 1.1: Sea A un conjunto no vacío de $\mathbb{N}_0$. Entonces, $\langle A\rangle$ es un semigrupo numérico, si, y solo si, $m.c.d(A) = 1$.

Demostración: Sea $S = \langle A \rangle$ un semigrupo numérico. Entonces, si $d = m.c.d(A)$ y $s \in S$, se tiene que $d|s$ (Pues d divide a todos los elementos de A). Por ser S un semigrupo numérico, $\mathbb{N}_0 \setminus S$ es un conjunto finito; y existe cierto $s \in S$ tal que $s+1 \in S$, entonces $(d|s) \wedge (d|(s+1)) \Rightarrow d = 1$.

Para demostrar el recíproco, basta probar que $\mathbb{N}_0 \setminus \langle A \rangle$, es finito. Como $1 = m.c.d(A)$, y si $A = \{a_1, \ldots, a_n\}$, existirán $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$, tales que $1 = \sum_{i=1}^{n} \lambda_i a_i$ (Identidad de Bézout). Si pasamos los términos con índice i en el conjunto $I = \{i \in \{1, 2, \ldots, n\} \mid \lambda_i < 0\}$ a la izquierda de la igualdad, obtenemos que $-\sum_{i \in I} \lambda_i a_i + 1 = \sum_{i \in (\{1,2,\ldots,n\} \setminus I)} \lambda_i a_i \in S$. Por tanto $s = -\sum_{i \in I} \lambda_i a_i \in \langle A \rangle$ verifica que $s + 1 \in \langle A \rangle$. Vamos a demostrar ahora que si $n \geq (s-1)s + (s-1)$, entonces $n \in \langle A \rangle$. Sean q y r enteros tales que $n = qd + r$ con $0 \leq r < s$ (división entera de n entre s). Puesto que $n = qd + r \geq (s-1)s + (s-1)$ y $r \leq s$, deducimos que $q \geq s - 1 \geq r \Rightarrow (q - r) \geq 0$. Juntándolo todo, tenemos que $n = s(q - r + r) + r = (q - r)s + (rs + r) = r(s+1) + (q-r)s \in \langle A \rangle$.

□

Definición 1.3: Dados dos semigrupos X, Y, un homomorfismo entre X y Y es una aplicación $f : X \to Y$ que verifica la siguiente propiedad:

$$f(a+b) = f(a) + f(b) \quad \forall a, b \in X$$

Decimos que dicho homomorfismo es un isomorfismo si la aplicación es biyectiva, monomorfismo si es inyectiva y epimorfismo si es sobreyectiva.

Definición 1.4: Dado un semigrupo numérico S y un elemento $n \in S \setminus \{0\}$, el conjunto de Apéry asociado a un subconjunto se define como:

$$Ap(S, n) = \{s \in S | s - n \notin S\}$$

Ejemplo 1.3: Para el semigrupo anterior: $S := \langle 3, 7 \rangle$, podemos calcular el conjunto de Apéry usando la definición:

- $Ap(S, 3) = \{0, 3, 14\}$
- $Ap(S, 7) = \{0, 3, 7, 13, 16, 18, 19\}$

Lema 1.1: Dado S un semigrupo y denotando $S^* = S \setminus \{0\}$, entonces $S^* \setminus (S^* + S^*) = \{s \in S^* \mid \nexists\, x, y \in S^* : s = x + y\}$ es un sistema de generadores de S. De echo, todo sistema de generadores contiene a este conjunto.

Demostración: Dado $s \in S^*$, si $s \notin S^* \setminus (S^* + S^*)$ entonces $\exists\, x, y \in S^*$ tales que $x + y = s$. Si $x, y \notin S^* \setminus (S^* + S^*)$, podemos iterar el razonamiento sobre x e y y sobre los elementos en los que se descomponen hasta que, en un número finito de veces obtendremos una descomposición $s = s_1 + \ldots + s_n$ donde $s_i \in S^* \setminus (S^* + S^*),\ i \in \{1, \ldots, n\}$. El proceso es finito, pues $x < s,\ y < s$. Esto demuestra que $S^* \setminus (S^* + S^*)$ es un sistema de generadores.

Dado, un sistema de generadores A de S, si tomamos $x \in S^* \setminus (S^* + S^*)$, entonces existe $n \in \mathbb{N} \setminus \{0\}, \lambda_1, \ldots, \lambda_n \in \mathbb{N}$ y $a_1, \ldots, a_n \in A$ tales que $x = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Como $x \notin S(S^* + S^*)$, entonces existe $i \in \{1, \ldots, n\} \mid x = a_i$.

□

Lema 1.2: Dado n un elemento distinto de cero del semigrupo S, podemos caracterizar el conjunto de Apéry $Ap(S, n)$ como $\{0 = w(0), w(1), \ldots, w(n-1)\}$, donde $w(i) = min_{\alpha \in S}\{\alpha = i\ (mod\, n)\} \quad \forall i \in \{0, 1, \ldots, n-1\}$.

Demostración: La demostración sigue del hecho que, $\exists k \in \mathbb{N}$ tal que $k \cdot n + i \in S$, $\forall i \in \{0, 1, \ldots, n-1\}$

□

Del lema anterior, tenemos que el cardinal de $Ap(S, n)$ es n

Lema 1.3: Dado un semigrupo numérico S y $n \in S$, tenemos que, para todo $s \in S$, existe un único par $(k, w) \in \mathbb{N} \times Ap(S, n)$ tal que:

$$s = k \cdot n + w$$

Demostración:
$s = i(mod\ n)$ para cierto $i \in \{0, 1, \ldots, n-1\}$, luego $s = w(i) + k \cdot n$ para un cierto $k \in \mathbb{N}$ y donde $w(i)$ es como en el lema anterior.

□

En particular, este lema dice que: $\langle Ap(S, n) \cup \{n\} \rangle = S$

Teorema 1.2: Todo semigrupo admite un sistema minimal de generadores. Dicho sistema minimal de generadores es finito.

Demostración: Sigue de los lemas 1.1 y 1.3. El lema 1.1 nos dice que $S^* \setminus (S^* + S^*)$ es un sistema minimal de generadores y el lema 1.3 que $\forall n \in S^*,\ S = \langle Ap(S, n) \cup \{n\} \rangle$. Dado que $\langle Ap(S, n) \cup \{n\} \rangle$ es finito, $S^* \setminus (S^* + S^*)$ también lo es.

□

Definición 1.5: Dado un semigrupo numérico S con el siguiente sistema minimal de generadores: $\{n_1 < n_2 < \ldots < n_p\}$, definimos:

- n_1 como **multiplicidad de S**, que denotaremos por $\mathbf{m}(\mathbf{S})$
- p como **dimensión embebida** del semigrupo S (en Inglés, "*embedding dimension*"). La denotaremos por $\mathbf{e}(\mathbf{S})$

Proposición 1.3 Dado S un semigrupo numérico, tenemos que:

- $m(S) = min(S \setminus \{0\})$
- $e(S) \leq m(S)$

Demostración: Por definición la multiplicidad es el menor de los generadores. Dicho elemento es el menor de los elementos distintos de 0 del semigrupo, pues no se puede poner como suma de otros dos.

La segunda afirmación viene del hecho de que $\{m(S)\} \cup Ap(S, m(S)) \setminus \{0\}$ es un sistema de generadores de S (dado por lema 1.3) y cuyo cardinal es m(S) (lema 1.2). Todo sistema minimal de generadores deberá, por tanto tener como mucho $m(s)$ elementos.

□

Definición 1.6: Dado un semigrupo numérico S, llamamos al mayor entero que no está en S *Número de Fröbenius* de S y se denota por $F(S)$. También se usa el concepto del *conductor*, que es el menor entero $C(S)$ tal que $C(S) + n \in S,\ \forall n \in \mathbb{N}$. El conducto es el número de Föbenius más uno.

Definición 1.7: Dado un semigrupo numérico S, denominamos *lagunas* o *lagunas* de S (gaps en ingles) al conjunto $G(S) = \mathbb{N} \setminus S$. La cardinalidad de dicho conjunto se llama *género* o *grado de singularidad* de S y se denota por $g(S)$.

La siguiente proposición cubre el caso particular de semigrupos generados por dos elementos $S = \langle\{a, b\}\rangle$, pero es importante, pues cuando hablemos de curvas y semigrupos de Weierstrass volverá a aparecer.

Proposición 1.4 Sea S, el semigrupo numérico generado por los enteros a, b, co-primos entre si $(m.c.d(a, b) = 1)$

- $F(\langle a, b\rangle) = ab - a - b$

- $g(\langle a,b\rangle) = \frac{(ab-a-b+1)}{2}$

Demostración: Podemos escribir el semigrupo como la unión de la siguiente familia de secuencias:

$$f_0 = \{0+0,\ 0+b,\ 0+2b, 0+3b, \ldots\} = \{n\cdot b\}_{i=1}^{\infty}$$
$$f_1 = \{a+0,\ a+b,\ a+2b, a+3b, \ldots\} = \{a+n\cdot b\}_{i=1}^{\infty}$$
$$f_2 = \{2a+0,\ 2a+b,\ 2a+2b, 2a+3b, \ldots\} = \{2a+n\cdot b\}_{i=1}^{\infty}$$
$$\ldots$$
$$f_{b-1} = \{(b-1)a+0,\ (b-1)a+b,\ (b-1)a+2b, (b-1)a+3b, \ldots\} = \{(b-1)a+n\cdot b\}_{i=1}^{\infty}$$

$S = \langle a,b\rangle = \cup_{k=1}^{b-1} f_k$. Si $s \in S$, $s = na + mb$, por lo que pertenece a la secuencia $f_{\{\overline{na}\ (mod\ b)\}}$. La otra contención es inmediata por como son los elementos de las secuencias.

Vamos a contar los elementos usando funciones generadoras, donde los exponentes de los términos distintos de cero representan los elementos de las series. En el caso de f_k, definimos la función $(0 \leq k \leq b-1)$:

$$f_k(x) = x^{ka} + x^{ka+b} + \ldots + x^{ka+nb} + \ldots = \sum_{i=1}^{\infty} \frac{x^{ka}}{1-x^b}$$

Dicha función tiene como monomios no nulos a aquellos que tienen términos de f_k por exponente. Para la unión de todas las series (y por tanto, tener en cuenta, todos los elementos del semigrupo) consideramos la función suma:

$$f(x) = \sum_{k=0}^{b-1} f_k = (\frac{1}{1-x^b})(1 + x^a + x^{2a} + \ldots + x^{(b-1)a}) = \frac{1-x^{ab}}{(1-x^a)(1-x^b)}$$

La función generadora es para los enteros no negativos es $g(x) = 1+x+x^2+\ldots = 1/(1-x)$. Por tanto, la diferencia $g - f$, es la función generadora de las lagunas $(\mathbb{N}_0 \setminus S)$:

$$h(x) = g(x) - f(x) = \frac{1}{(1-x)} - \frac{1-x^{ab}}{(1-x^a)(1-x^b)} = \frac{(1-x^a)(1-x^b) - (1-x)(1-x^{ab})}{(1-x)(1-x^a)(1-x^b)}$$

- El exponente del elemento de mayor grado de h (es decir, el grado de h), es el mayor entero no negativo que no está en S. Vemos que $deg(h) = (ab+1)-a-b-1 = ab-a-b$. Por tanto $F(\langle a,b\rangle) = ab-a-b$.

- Puesto que $h(x)$ es la función generadora de las lagunas, debe tener una cantidad finita de monomios. Bastaría pues con, sustituir $x = 1$ para conocer cuantos monomios hay, y por tanor, lagunas. Debido a que $h(x)$ no está bien definida en $x = 1$, debemos tomar el límite. Al aplicar la regla de l'Hôpital, vemos que la tercera derivada de orden 3 del

denominador no es cero. Luego,

$$g(\langle a,b\rangle) = Lim_{x\to 1}h(x) =$$

$$Lim_{x\to 1}\frac{(d^3/dx^3)[(1-x^a)(1-x^b)-(1-x)(1-x^{ab})]}{(d^3/dx^3)[(1-x)(1-x^a)(1-x^b)]} =$$

$$\frac{3ab((a-1)+(b-1)-ab-1)}{-6ab} = \frac{ab-a-b+1}{2},$$

tal y como queríamos demostrar.

□

Ejemplos 1.4: Podemos calcular las lagunas, el grado de singularidad y el número de Föbenius usando GAP:

```
gap> s1 := NumericalSemigroup("generators",3,5,7);
gap>Numerical semigroup with 3 generators>
gap> GapsOfNumericalSemigroup( s1 );
[ 1, 2, 4 ]
gap> FrobeniusNumber( s1 );
4
gap> Genus(s1);
3
```

Aunque en general no se puede dar una formula para calcular el conjunto de lagunas o el número de Fröbenius, si se conoce el conjunto de Apéry se pueden dar formulas en función de este para calcularlos:

Proposición 1.5: Dado un semigrupo numérico S y $n \in S^*$ tenemos que:

- $F(S) = (max\ Ap(S,n)) - n$
- $g(S) = \frac{1}{n}(\sum_{w\in Ap(S,n)} w) - \frac{n-1}{2}$

Demostración:
Queremos ver que si $x > (max\ Ap(S,n))-n$, $x \in S$. Por definición de $Ap(S,n)$, $(max\ Ap(S,n))-n \notin S$. Dado $x > (max\ Ap(S,n)) - n \Rightarrow x+n > (max\ Ap(S,n))$. Por el lema 1.2, existe $w \in Ap(S,n)$ tal que es congruente con x modulo n. Como $w < x+n$, existe un entero positivo k tal que $w + n\cdot k = x+n$ y por tanto $x - n = w + (k-1)\cdot n$ pertenece a S

Para la segunda afirmación, nos basamos en el lema 1.2 y la notación allí usada. Sabemos que para cada $w \in Ap(S,n)$ congruente con i modulo n, con $i \in \{0,1,\ldots,n-1\}$, $\exists k_i \in \mathbb{N}$ tal que $w = k_i \cdot n + i$. Es decir, que:

$$Ap(S,n) = \{w(0) = 0, w(1) = k_1 \cdot n + 1, \ldots, w(i) = k_i \cdot n + i, \ldots, w(n-1) = k_{n-1} \cdot n + n - 1\}$$

Cualquier entero x congruente con $w(i)$ modulo n pertenece a S si y solo si $w(i) \leq x$. En otras palabras hay k_i enteros no negativos congruentes con i modulo n que no están en el semigrupo. Por tanto:

$$g(S) = k_1 + \ldots + k_{n-1} = \frac{1}{n}\sum_{i=1}^{n-1}(n \cdot k_i + i) - \frac{n-1}{2} = \frac{1}{n}\sum_{w \in Ap(S,n)}(w - \frac{n-1}{2})$$

□

lema 1.4: Sea S un semigrupo numérico con conductor $C(S)$ y grado de singularidad $g(S)$, entonces:

$$2g(S) \geq C(S)$$

Demostración: Supongamos que $2g(S) < C(S)$ es decir: $\alpha = (\#\{ng \in S | ng < c\}) > \frac{C(S)}{2}$. Podemos escribir $F(S) = C(S) - 1$ como suma de dos enteros positivos de $\left\lfloor \frac{F(s)+1}{2} \right\rfloor \leq \frac{C(S)}{2} < \alpha$ formas distintas:

$$\begin{aligned} F(S) = F(S) + 0 = \\ (F(S) - 1) + 1 = \\ \ldots \\ F(S) - \left\lfloor \frac{F(S)}{2} \right\rfloor + \left\lfloor \frac{F(S)}{2} \right\rfloor = \\ F(S) - \left\lfloor \frac{F(S)}{2} \right\rfloor + (F(S) - \left\lceil \frac{F(S)}{2} \right\rceil) = \\ \left\lfloor \frac{F(S)}{2} \right\rfloor + \left\lceil \frac{F(S)}{2} \right\rceil = F(S) - \left\lceil \frac{F(S)}{2} \right\rceil + \left\lceil \frac{F(S)}{2} \right\rceil \end{aligned}$$

Por tanto, existen dos elementos del semigrupo a, b tales que $F(S) = a + b \in S$, pero por definición $F(S) \notin S$

□

La proposición anterior establece, en cierto modo, el número mínimo de lagunas que un semigrupo puede tener en función de su conductor. El mínimo se da cuando hay igualdad: $C(S) = 2g$. No en todos los semigrupos es cierto esto, pero en caso de que lo sea se les da un nombre especial:

Definición 1.8: Decimos que un semigrupo numérico S con grado de singularidad $g(S)$ y conductor c es simétrico si: $C(S) = 2g(S)$

Ejemplo 1.5: El grupo generado por $\{3, 5\}$ es simétrico: $S = \langle\{0, 3, 5\}\rangle = \{0, 3, 5, 6, 8, 9, 10, \ldots\} = \{3, 5, 6, 8, \rightarrow\}$. Por lo que tenemos que el conductor es $c = 8$, y las lagunas son $G(S) = \{1, 2, 4, 7\} \Rightarrow g(s) = |G(s)| = 4$. Se verifica que $2g(S) = C(S)$, por lo que el semigrupo es simétrico.

A continuación tratamos sobre el concepto de irreducibilidad de semigrupos. El estudio de irreducibilidad de ideales de semigrupos es uno de los objetivos de estudio centrales de este trabajo y empezamos definiendo ese concepto para semigrupos:

Definición 1.9: Decimos que un semigrupo numérico es irreducible si no puede ser expresado como intersección de dos semigrupos que lo contienen de forma propia.

Capítulo 2

Ideales de semigrupos numéricos

El concepto de ideal se puede extender a semigrupos, como veremos en este capítulo. Estudiaremos los ideales de semigrupos, concepto que será más adelante necesario para tratar códigos, pero también serán los ideales parte del objeto de este trabajo. He trabajado para implementar funcionalidad relacionado con Ideales de semigrupos para librería "NumericalSgps"para el sistema GAP, en particular en lo que respecta a irreducibilidad de ideales.

Definición 2.1: Sea S un semigrupo numérico, decimos que $E \subset \mathbb{Z}$ es un *ideal relativo* de S si:

- $S + E = \{s + e \mid s \in S,\ e \in E\} \subset E$
- Existe $s \in S$ tal que $s + E = \{s + e \mid e \in E\} \subset S$

La primera condición es similar a la condición tradicional de ideal en teoría de anillos, si bien en este caso no hay multiplicación. La segunda condición asegura que E tiene mínimo que denotaremos por $m(E)$ y llamaremos *multiplicidad* de E.

Para convencernos que esta condición implica que E tiene mínimo, supongamos que no es así. Entonces existe $e < 0$ con $|e| > s$ (s como en la definición) entonces $s + e < 0 \Rightarrow s + e \notin S$, pues todos los elementos de S son positivos. Pero esto contradice la definición de s.
Si $E \subseteq S$ diremos que E es un *ideal propio* o simplemente *ideal* de S

Ejemplos 2.1:

- Un ejemplo de ideal propio es S, que claramente es ideal de si mismo.

- Dado un semigrupo numérico S, podemos definir ideales relativos de S tomando un conjunto finito $A \subset \mathbb{Z}$ y definiendo $E := A+S$. Por ejemplo, dado $S = \{0, 3, 6, 7, 9, 10, 12, \rightarrow\}$

y $A = \{-1\}$; $E := \{-1\} + \{0, 3, 6, 7, 9, 10, 12\} = \{-1, 2, 5, 6, 8, 9, 11, \rightarrow\}$. La segunda condición se verifica, pues si $s = 12$, $s + E \subseteq S$. La primera condición se verifica, pues $\forall e \in E,\ \exists s_1 \in S,\ tal\ que\ e = -1 + s_1$. Entonces para cualquier $s_2 \in S$ tenemos $e + s_2 = -1 + s_1 + s_2 = -1 + s \in E,\ s \in S$.

- Veamos un ejemplo de ideal propio. Dado $\{0, 3, 6, 7, 9, 10, 12, \rightarrow\} S$ semigrupo numérico, podemos definir $D(12) := \{y \in S \mid 12 - y \in S\} = \{0, 3, 6, 9, 12\}$ (veremos más sobre este tipo de conjuntos más adelante). Entonces $S \setminus D(12) = \{7, 10, 13, \rightarrow\} \subseteq S$. Vemos que verifica ambas condiciones.

Definición 2.2: Algunos ideales relativos importantes son:

1. $M = S^* = S \setminus \{0\}$, ideal propio de S al que denotamos *ideal maximal*.
2. El *ideal conductor* es: $S - \mathbb{N} = \{z \in \mathbb{Z} \mid z + \mathbb{N} \subset S\} = \{C(S), \rightarrow\} = C(S) + \mathbb{N}$. Este es el mayor ideal común a $\mathbb{N}$ y S.
3. El *ideal canónico estándar* se define como. $K(S) = \{x \in \mathbb{Z} \mid F(S) - x \notin S\}$.

Vemos que los ideales anteriores verifican la definición de ideal relativo:

1. Que el ideal maximal es un ideal, es trivial.
2. El ideal conductor coincide con el semigrupo $\{C(S), \rightarrow\}$, luego $m(\{C(S), \rightarrow\}) = C(S)$ y $a + b \in C(S) + \mathbb{N},\ a \in \{C(S), \rightarrow\},\ b \in S$
3. El ideal canónico está acotado inferiormente, pues si $x \in \mathbb{Z}\ y\ x < 0$ entonces $F(S) < F(S) - x \in S \Rightarrow x \notin K(S)$. Por otro lado, dado $k \in K(S)$ y $s \in S$, vemos que $k + s \in K(S)$: Si no fuera así, $\alpha := F(S) - (k + s) \in S$, pero entonces $\alpha + s \in S$, $\alpha + s = F(S) - k$, que no pertenece a S por definición

Ejemplo 2.2: Vemos un ejemplo con GAP:

```
gap> s:=NumericalSemigroup(3,5,7);;
gap> k:=CanonicalIdeal(s);
<Ideal of numerical semigroup>
gap> SmallElements(k);
[ 0, 2, 3, 5 ]
gap> SmallElements(s);
[ 0, 3, 5 ]
gap> SmallElements(MaximalIdeal(s));
[ 3, 5 ]
```

Se pueden definir operaciones básicas entre ideales:

Definición 2.3: Dados dos ideales relativos E y H de un semigrupo numérico S, definimos:

- $E + H = \{e + h \mid h \in H,\ e \in E\}$
- $H - E = \{z \in \mathbb{Z} \mid z + E \subset H\}$

Ejemplo 2.3: Tomemos el semigrupo numérico $S = \langle 10, 13, 21, 22\rangle$:

Consideremos los ideales $E = \{10, 11\} + S$ y $H = \{-1, 2, 3\} + S$. Operando (con ayuda de GAP):

$$E + H = \{9, 10, 12, 13, 14, 19, 20, 22, 23, 24, 25, 26, 27, 29, \rightarrow\}$$

$$E - H = \{21, 31, 34, 38, 41, 42, 43, 44, 47, 48, 50, \rightarrow\}$$

Veamos que las operaciones entre dos ideales de S resultan en un ideal de S.

Proposición 1: Sean E y H ideales relativos cualquiera de un semigrupo numérico S. Entonces $E + H$ y $H - E$ son también ideales relativos de S.

Demostración 2.1:

1. Veamos que verifica la definición de ideal. Sea $x \in E+H$, entonces existen $e \in E,\ h \in H$ tales que $x = e + h$. Para un $s \in S$, $x + s = e + h + s \in E + H$ pues $h + s \in H$.
   Para verificar la segunda condición de la definición de ideal, sean s_H, s_E tales que $s_H + H \subset S$ y $s_E + E \subset S$ si tomamos $s = s_H + s_E$ entonces

   $$s + (E + H) = \{s + e + h \mid e \in E,\ h \in H\} = \{s_H + h + s_E + e \mid e \in E,\ h \in H\} \subset S$$

   pues $s_H + h \in S$ y $s_E + E \in S$.

2. Verifiquemos que $H - E$ también cumple la definición. Dado $z \in H - E$, $\forall e \in E,\ \exists h \in H$ tales que $z + e = h$. Para cualquier $s \in S$, para cualquier e y para el h anterior tenemos $z + s + e = h + s \in H \Rightarrow (z + s) + H \subseteq E \Rightarrow (z + s) \in H - E$.
   La segunda condición, tomemos $s = e + s_E + s_H \in S$, donde s_H y s_E son como en apartado anterior. $z \in H - E \Rightarrow\ \forall e \in E,\ \exists h \in H\ $ tal que $z + e = h \Rightarrow z = (h - e)$. Por tanto $z + s = (h - e) + s = (h - e) + s_h + e + s_e = h + s_h + s_e \in S$, verificándose así la segunda condición.

□

Podemos probar algunas propiedades de estas operaciones:

Proposición 2.2: Sean E, G, H ideales relativos de un semigrupo numérico S y z cualquier elemento de $\mathbb{Z}$. Entonces tenemos que:

1. $(x + E) - H = x + (E - H)$ y $E - (x + H) = -x + (E - H)$
2. $E - (G \cup H) = (E - G) \cap (E - H)$ y $(E - G) \cup (E - H) \subseteq E - (G \cap H)$
3. Si $G \subseteq H$ entonces $E - H \subseteq E - G$ y $H - E \subseteq G - E$

Demostración: Las demostraciones son consecuencia de operar sobre las definiciones:

1. Para la primera proposición, partimos de $(x + E) - H$.
   Sea $\overline{E} = x + E = \{x + e \mid e \in E\}$, primero computamos:

   $$\overline{E} - H = \{z \in \mathbb{Z} \mid z + H \subset \overline{E}\} = \{z \in \mathbb{Z} \mid \forall h \in H,\ \exists e \in E \textit{ tal que } z + h = e + x\}.$$

   Usando la expresión completa:

   $$x + (E - H) = x + \{z' \in \mathbb{Z} \mid z' + H \subset E\} =$$

   $$x + \{z' \in \mathbb{Z} \mid \forall h \in H,\ e \in E,\ z' + h = e\} = \{x + z' \mid z' \in \mathbb{Z},\ h \in H,\ e \in E,\ z' + h = e\}.$$

   Llamando $z = x + z' \Rightarrow z' = z - x$ obtenemos que el conjunto anterior es $\{z \in \mathbb{Z} \mid h \in H,\ e \in E,\ z - x + h = e\}$, por lo que la primera igualdad es cierta. La segunda igualdad se demuestra de forma análoga.

2. Para la primera:

   $$(E - G) \cap (E - H) = \{z \in \mathbb{Z} \mid z + G \subset E\} \cap \{z \in \mathbb{Z} \mid z + H \subset E\} =$$

   $$\{z \in \mathbb{Z} \mid z + G \subset E \wedge z + H \subset E\} = \{z \in \mathbb{Z} \mid z + (G \cup H) \subset E\}$$

   Para la segunda afirmación, dado $z \in E - G$ (respectivamente en $E - H$) entonces:

   $$z \in \{z' \in \mathbb{Z} \mid z' + G \subseteq E\} \ \Rightarrow\ \{z' \in \mathbb{Z} \mid z' + (H \cap G) \subseteq E\} = E - (E \cap H)$$

3. Si $z \in H - E = \{z \in \mathbb{Z} \mid z + E \subseteq G\}$ entonces, como $G \subseteq H$ tenemos que: $z \in \{z \in \mathbb{Z} \mid z + E \subseteq G \subseteq H\} = G - H$.
   Para la contención, dado $z \in E - H \Rightarrow\ z + g \in E \Rightarrow z \in E - G$

□

A continuación, vemos que algunos conceptos de semigrupos pueden ser extendidos a ideales, como el de número Fröbenius:

Definición 2.4: Dado un ideal relativo E de un semigrupo numérico S, llamaremos número de Fröbenius de E a $Max(\mathbb{Z} \setminus E)$ y lo denotaremos por $F(E)$.

El hecho que E este acotado inferiormente asegura que el máximo existe.

También podemos definir para ideales un sistema de generadores:

Ejemplo 2.4:

- Si consideramos a S como ideal de sí mismo, vemos que la definición de número de Fröbenius coincide con la definición para semigrupos:
  Si $S = \{3, 6, 7, 9, 10, 12, \rightarrow\}$ entonces $F(S) = max(\mathbb{Z} \setminus S) = 11$
- Para ideal $E = S \setminus D(12)$ n (ver el primer ejemplo de este capitulo), $F(E) = 12$.

Definición 2.5: Dado un ideal relativo E del semigrupo numérico S decimos que un conjunto $\{e_1, \ldots, e_n\} \subset E$ es un sistema de generadores de E si podemos expresar un elemento cualquiera $e \in E$ como $e = e_i + s,\ s \in S,\ i \in \{1, 2, \ldots, n\}$.

Vemos que todo ideal canónico tiene un sistema minimal de generadores:
Proposición 2.3: Dado un ideal relativo E de un semigrupo numérico, $E \setminus (M + E)$ es un sistema minimal de generadores de E.

Demostración: La demostración sigue un argumento similar a demostrar que $S^* \setminus (S^* + S^*)$ es un sistema de generadores de S:

Primero demostramos que es un sistema de generadores. Dado $e \in E$, si tenemos que $e \notin E \setminus (M + E)$ entonces existen $x \in E$ e $y \in M$ tales que $e = x + y$. Si $x \notin E \setminus (M + E)$. Podemos repetir el argumento y volver a descomponerlo: $\exists x' \in E,\ y' \in M \mid x = x' + y'$. De esta forma, podemos continuar la descomposición, llegando eventualmente a una descomposición finita de e:

$$e = e_1 + s_1 + e_2 + s_2 + \ldots + e_m + s_m = e_1 + e_2 + \ldots + e_m + s$$

Donde $s \in S$ y $e_1 \in E \setminus (M + E),\ \forall i \in \{1, 2, \ldots, m\}$. Esto es así pues $e > x,\ e > y$ y en cada descomposición obtenemos elementos de cardinal menor. Al al ser E un ideal relativo, tiene un mínimo: $m(E)$, por lo que el proceso de descomposición es finito.

Para ver que todo sistema de generadores está contenido en este, sea $H = \{h_1, \ldots, h_n\}$ un sistema de generadores de E. Dado $e \in E \setminus (E + M)$, tenemos que existen $h \in H,\ s \in S$ tales que $e = h + s$, pero $e \notin (E + M)$ y $h \in H \subset E$, luego $s = 0$ y $e = h$.

□

Ejemplo 2.5: Veamos un ejemplo, dado $S = \{3, 6, 7, 9, 10, 12, \rightarrow\}$, computemos un sistema de generadores de $E = S \setminus D(12) = \{7, 10, 13, \rightarrow\}$. Como acabamos de ver, $E \setminus (E + M)$ es un sistema de generadores de S. $E + M = \{10, 13, 14, 16, \rightarrow$
$E \setminus (E + M) = \{7, 15\}$. Podemos comprobar que todos los elementos de E se pueden escribir como suma de 7 ó 15 más un elemento de S:
$7 = 7 + 0,\ 10 = 7 + 3,\ 13 = 7 + 6,\ 14 = 7 + 7\ 15 = 15 + 0,$
$16 = 7 + 9,\ 17 = 7 + 10,\ 18 = 15 + 3,\ 19 = 7 + 12,\ \ldots$

Proposición 2.4: Sea S un semigrupo numérico, E un ideal relativo cualquiera y K ideal canónico, tenemos que: $K - E = \{x \in \mathbb{Z} \mid F(S) - x \notin E\}$

Demostración: Empezamos demostrando la primera contención. Sea $x \in K - E$, por la definición de resta de ideales, $x + E \subset K \Rightarrow \forall e \in E,\ x + e \in K \Rightarrow F(S) - (x + e) \notin S \Rightarrow F(S) - x \notin S + e \subset E$.

Por otro lado, si tenemos que $F(E) - x \notin E$ entonces, $\forall e \in E$ tenemos que $F(S) - (x + e) \notin S$, pues de lo contrario: $F(S) - (x + e) + e \in E \Rightarrow F(S) - x \in E$ que contradice la hipótesis. Como $F(S) - (x + e) \notin S, \forall e \in E$ entonces $\forall e \in E,\ x + e \in K \Rightarrow x + E \subset K \Rightarrow x \in K - E$

□

Una consecuencia inmediata de esta proposición es que $K - K = S$

Corolario 2.5: Sean S un semigrupo numérico, K un ideal canónico y H, E ideales relativos. Entonces se verifica la siguiente igualdad: $K - (H \cap E) = (K - E) \cup (K - H)$

Demostración: En la proposición 1 ya demostramos que $(K - E) \cup (k - H) \subseteq K - (E \cap H)$ Para la segunda contención, dado $z \in K - (H \cap E) = \{z \in \mathbb{Z} \mid F(S) - z \notin (E \cap H)\} = \{z \in \mathbb{Z} \mid (F(S) - z \notin E) \vee (F(S) - z \notin H)\} = \{z \in \mathbb{Z} \mid F(S) - z \notin E\} \cup \{z \in \mathbb{Z} \mid F(S) - z \notin H)\} = (K - E) \cup (K - H)$

□

Definición 2.6: Decimos que dos ideales relativos H y E de S son equivalentes si existe $x \in \mathbb{Z}$ tal que $E = x + H = \{x + h \mid h \in H\}$

Esto significa que todo ideal relativo de S es equivalente a un ideal propio, pues basta con trasladar E por $m(E)$ para obtener un ideal principal: $m(E) + E \subset S$. Esto define una relación de equivalencia entre ideales relativos de un determinado semigrupo.

En particular, dado un ideal E de S, podemos tomar $\tilde{E} = E - F(E) + F(S)$. Dicho ideal relativo es un ideal propio de S equivalente a E y con el mismo número de Fröbenius que S. Usando esta notación, podemos introducir el siguiente resultado:

Proposición 2.7: Sea S un semigrupo numérico y K su ideal canónico estándar. Todo ideal relativo de S es equivalente a un ideal relativo $\tilde{E}$ de modo que $S - \mathbb{N} = \{C(S), \rightarrow\} \subseteq \tilde{E} \subseteq K$

Demostración: La primera inclusión viene dada por el hecho que el número de Fröbenius de $\tilde{E}$ es $F(S)$, luego contiene al ideal conductor.

Para la segunda, supongamos que $x \in \tilde{E},\ x \notin K$, esto significa que $F(S) - x \in S$. Por definición de ideal, $F(S) = (F(S) - x) + x \in \tilde{E}$, lo cual contradice que el número de Fröbenius de $\tilde{E}$ es $F(S)$.

□

Vemos que el ideal canónico juega un papel importante en el estudio de los ideales de S. Aparecerá más adelante cuando estudiemos la irreducibilidad de ideales.

Corolario 2.8: No existe ningún ideal relativo de S que contenga propiamente al ideal canónico estándar.

Demostración: Dado E ideal relativo de S y $\tilde{E} = E + \alpha$ ($\alpha = F(S) - F(E)$). Si $K \subsetneq E$, entonces, dado B un sistema minimal de generadores de E y L, un sistema minimal de generadores de K, $|B| > |L|$. Claramente $\tilde{B} = B + \alpha$ es un sistema minimal de generadores de $\tilde{E}$, pero por la proposición anterior, tenemos que $\tilde{E} \subset K$, lo cual contradice que $|\tilde{B}| = |B| > |L|$.

□

Mostramos a continuación un lema que necesitaremos más adelante para tratar irreducibilidad de ideales:
Lema 2.1: Sea K ideal canónico y H un ideal relativo de S. Entonces se verifica la siguiente igualdad: $K - (K - H) = H$.

Demostración: Por un lado, si $z \in K - (K - H) = k - \Delta$ por la proposición 2, $F(S) - z \notin \Delta$ por tanto (usando el lema de nuevo): $F(S) - (F(S) - z) \in H \Rightarrow z \in H$.
Por otro lado, dado $z \in H \Rightarrow F(S) - (F(S) - z) \in H \Rightarrow (F(S) - z) \notin \Delta \Rightarrow z \in K - \Delta = K - (K - H)$

□

El lema anterior se puede extender a una doble implicación, y en ese caso se conoce como Teorema de Jäger. Además, como una consecuencia simple del lema anterior, tenemos que: $K - S = \{x \in \mathbb{Z} \mid F(S) - x \notin S\} = K$

Definición 2.7: Dado un semigrupo numérico S, y E un semigrupo numérico del mismo, decimos que E es irreducible ($\mathbb{Z} - irreducible$) en S, si no puede ser expresado como intersección finita de otros ideales relativos (distintos de E) de S que lo contienen.

Un ejemplo de un ideal irreducible es K, el ideal canónico. Como hemos visto, no hay ningún ideal relativo de S que lo contenga de forma de propia. A continuación veremos que se trata del único ideal $\mathbb{Z}$-irreducible

Teorema 2.9: Sea S un semigrupo numérico y E un ideal relativo del mismo. Sea $\{x_1, \ldots, x_h\}$ un conjunto minimal de generadores del ideal $K - E$. Entonces:

$$E = (-x_1 + K) \cap \ldots \cap (-x_h + K)$$

Además esta descomposición es no redundante y única. En particular, el ideal E es irreducible si y solo si es canónico.

Demostración: $\{x_1, \ldots, x_h\}$ es un sistema minimal de generadores de $K - E$, luego $K - E = \cup_{i=1}^{h}(x_i + S)$ y $x_i - x_j \notin S,\ \forall i \neq j,\ i, j \in \{1, 2, \ldots, h\}$ pues si fuera así $x_j + (x_i - x_j) = x_i \in K - E$, lo cual contradice que es minimal.

Podemos escribir:

$$E \ = \ K - (K - E) \ = \ (K - (x_1 + S)) \cap (K - (x_2 + S)) \cap \ldots \cap (K - (x_h + S)) =$$

$$(-x_1 + (K - S)) \cap (-x_2 + (K - S)) \cap \ldots \cap (-x_h + (K - S)) = (-x_1 + K) \cap \ldots \cap (-x_h + K)$$

La primera igualdad viene del Lema 2.1, mientras que la segunda es una aplicación de las propiedades de las operaciones con ideales que vimos al principio del capítulo. La tercera igualdad viene de la propiedad: $K - (x_i + H) = -x_i + (E - H)$. La última igualdad viene del hecho que $K - S = K$. Con esto demostramos la primera parte del teorema.

La descomposición es no redundante, pues si hubiera un término de la intersección que pudiéramos eliminar, entonces $\bigcap_{j \neq i}(-x_j + K) \subseteq -x_i + K$, por la proposición 1 y dada la

anterior contención se verifica que: $K-(-x_i+K)\subseteq K-\bigcap_{j\neq i}(-x_j+K)$. Por otro lado, por el corolario 1, $K-\bigcap_{j\neq i}(-x_j+K)=\bigcup_{j\neq i}(K-(-x_j+K))$. Juntándolo todo:

$$x_i\in x_i+S=x_i+(K-K)=K-(-x_i+K)\subseteq\bigcup_{j\neq i}K-(-x_j+K)=\bigcup_{j\neq i}(x_j+S)$$

La última igualdad viene dada por la proposición 1 y $(K-K)=S$. $x_i\in\bigcup_{j\neq i}(x_j+S)\Rightarrow \exists s\in S, j\neq i$ tal que $x_j+s=x_i$ contradiciendo así que $\{x_1,\ldots,x_h\}$ sea un sistema minimal de generadores.

Para demostrar que es único, supongamos que existen dos descomposiciones distintas: $E=(-x_1+K)\cap\ldots\cap(-x_{h_1}+K)=(-y_1+K)\cap\ldots\cap(-y_{h_2}+K)$. Dado que $\{x_1,\ldots,x_{h_1}\}$ y $\{y_1,\ldots,y_{h_2}\}$ son ambos sistemas de generadores minimales de $K-E$ tienen el mismo número de elementos ($h_1=h_2=:h$). Al ser conjuntos de generadores distintos, existirá un cierto $j\in\{1,2,\ldots,h\}$ tal que $x_j\notin\{y_1,\ldots,y_h\}$.

Como $\bigcap_{i=1}^{h}(-y_i+K)\subseteq\bigcap_{i=1}^{h}(-x_i+K)\subseteq(-x_j+K)$, en particular, existirá un cierto $I\subseteq\{1,2,\ldots,h\}$ de mínimo cardinal tal que $\bigcap_{i\in I}(-y_i+K)\subseteq(-x_j+K)$ pues $I=\{1,2,\ldots,h\}$ es una opción válida; y con $|I|>1$ al tenerse que $x_j\notin\{y_1,\ldots,y_h\}$. Podemos usar el mismo argumento que hemos utilizado con la no redundancia de la descomposición para llegar a una contradicción:

$$x_j\in x_j+S=x_j+(K-K)=K-(-x_j+K)\subseteq\bigcup_{i\in I}K-(-y_i+K)=\bigcup_{i\in I}(y_i+S)$$

Esto significa que $\exists k\in\{1,\ldots,h\},\ x_j=y_k+s\Rightarrow y_k=x_j-s$. Por tanto, dado $y'\in(-y_k+K)\Rightarrow\ \exists t\in K$ tal que $y'=-y_k+t\Rightarrow y'=-x_j+(s+t)\in(-x_j+K)$. Esto es una contradicción con la minimalidad de I, quedando así demostrada la minimalidad.

□

Antes hemos visto que el ideal canónico es irreducible, pero de este teorema deducimos que si E es $\mathbb{Z}$-irreducible, entonces $E=-x_i+K$ para algún $x_i\in\mathbb{Z}$. Sabiendo la forma que toman los ideales $\mathbb{Z}$-irreducibles y que la descomposición del teorema anterior es única, podemos definir una noción de componente irreducible:

Definición 2.8: Dado semigrupo numérico S y un ideal relativo del mismo E, a cada uno de los ideales de la forma $(-x_i+K)$ en los que según el teorema anterior podemos descomponer E los llamaremos **componentes $\mathbb{Z}$-irreducibles** de E (la unicidad de la descomposición

asegura que existe un único conjunto de componentes irreducibles para un ideal dado)

Ejemplo 2.6: Veamos un ejemplo en GAP de la descomposición descrita en el teorema. Sea $S = \{3, 4, 5\}$, y consideremos el ideal $I = \{4, 5\} + S$

```
gap> S:=NumericalSemigroup(3,5,7);;
gap> I:=[4,5]+S;;
gap> K:=CanonicalIdeal(S);;
gap> MinimalGenerators(K-I);
[ -2, 2 ]
gap> MinimalGenerators(Intersection(-2+K,2+K));
[ 4, 5 ]
```

Por lo que $\{4, 5\} + S = (-2 + K) \cap (2 + K)$. Como vemos, este teorema nos da un algoritmo para saber si un ideal es $\mathbb{Z}$-irreducible y nos da una descomposición en componentes irreducibles del ideal. Como parte de este trabajo de fin de grado he implementado este algoritmo en GAP.

Tratamos ahora la irreducibilidad de ideales propios.

Definición 2.9: Sea S un semigrupo numérico y E un ideal propio de S. Decimos que E es **irreducible** si no puede ser expresado como intersección finita de ideales propios de S que contengan a E propiamente.

S es ideal irreducible de si mismo, por lo que asumiremos en adelante que $0 \notin E$
Queremos un teorema que nos permita obtener una descomposición en elementos irreducibles con el caso de $\mathbb{Z}$-irreducibilidad, por lo que vamos a tener que introducir nuevos conceptos y demostrar proposiciones básicas sobre los mismos:

Definición 2.10: Sea S un semigrupo numérico:

- Dados dos enteros a,$b \in S$, decimos que $a \leq_S b$ si $b - a \in S$.
- Usando la notación anterior, definimos para $x \in S$, $D(x) = \{s \in S \mid s \leq_S x\} = \{s \in S \mid x - s \in S\}$. Al conjunto $D(x)$ lo denominaremos divisores de x en S.
- Diremos que un conjunto $X \subseteq S$ es cerrado por divisores (en S) si tiene la siguiente propiedad: $\forall x \in X$ y para todo $y \in S$ que verifique que $y \leq_S x$ entonces $y \in X$.

Ejemplo 2.7: En otros ejemplos hemos visto que para el semigrupo numérico $S = \{0, 3, 6, 7, 9, 10, 12, \rightarrow\}$ tenemos el conjunto $D(12) = \{3, 6, 9, 12\}$.

Más adelante demostraremos que todos los conjuntos de este tipo son cerrados por divisores, pero en este caso es sencillo computarlo manualmente.

Lema 2.2: Un subconjunto E de un semigrupo numérico S es un ideal si y solo si su complementario en S ($X = S \setminus E$) es cerrado por divisores.

Demostración: Por un lado, si E es un ideal de S veamos que $X = S \setminus E$ es cerrado por divisores. Sea $x \in X$, $y \in S$ con $y \leq_S x$. Si $y \in E$ entonces $y = x + s$ para algún $s \in S \Rightarrow x \in E$, llegado así a una contradicción. Por tanto, se verifica que $y \in X$ y entonces es cerrado por divisores.

Por otro lado, si partimos de que X es cerrado por divisores, entonces veamos que $E = S \setminus E$ es un ideal de S. Dado $e \in E$ y $s \in S$, $s + e \in E$, pues de lo contrario $s + e \in X$. Dado que $e \in S$ y que $e \leq_S e + s$ (pues $(e + s) - e = s \in S$) entonces aplicando la definición de cerrado por divisores sobre X, deducimos que $e \in X$. Llegando así a una contradicción.

□

Proposición 2.10: Sea S un semigrupo numérico y $x, a, b, c \in S$.

- Si $a \leq_S b$ y $b \leq_S c$ entonces $a \leq_S c$. Es decir, ($\leq_S$) es una relación transitiva.
- El conjunto $D(x)$ es cerrado por divisores.
- El conjunto $S \setminus D(x)$ es un ideal propio de S.

Demostración:

- Para la primera afirmación debemos demostrar que $c - a \in S$.
  $c - a = (c - b) + (b - a) = s_1 + s_2$. De $a \leq_S b$ deducimos que $s_2 = b - a \in S$ y de $b \leq_S c$ que $s_1 = c - b \in S$. Como S es un semigrupo $s_1 + s_2 = c - a \in S$.
- Si $z \in D(x)$, y dado $y \in S$ con $y \leq_S z$ entonces por la transitividad de ($\leq_S$) tenemos que $y \leq_S x$ y por definición de $D(x)$, $y \in D(x)$.
- Como $D(x)$ es cerrado por divisores, podemos aplicar el lema 2.2 y concluir que $S \setminus D(x)$ es un ideal de S. Como $S \setminus D(x) \subseteq S$ es un ideal propio.

□

Lema 2.3: Sea S un semigrupo numérico, y $x \in S$. Entonces, para todo ideal propio E de S, son equivalentes:

1. $x \notin E$.

2. $E \subseteq (S \setminus D(x))$

Demostración:
(1) $\Rightarrow$ (2): si $x \notin E$, entonces, para todo $s \in E$, tenemos que $s \not\leq_S x$, pues de ser así tendríamos que $x - s \in S$ y por definición de ideal $x = (x - s) + s \in E$, lo cual es una contradicción. Como $s \not\leq_S x$ entonces $s \in S \setminus D(x)$, quedando esta parte demostrada.
(2) $\Rightarrow$ (1) Es inmediata porque $x \in D(x)$

□

Proposición 2.11: Las siguientes afirmaciones son equivalentes:

1. E es irreducible

2. $E = S \setminus D(x)$ para algún $x \in S$

Demostración: Empezamos demostrando (1) $\Rightarrow$ (2). Recordemos que la definición de que E es irreducible es que no puede ser expresado como intersección finita de ideales propios que lo contienen estrictamente. Denotemos por H a la intersección de todos los ideales propios que contienen a E. Entonces $E \subsetneq H \Rightarrow \exists x \in H \setminus E$. Como $x \notin E$, podemos aplicar el lema 2.3 y deducimos que $E \subseteq S \setminus D(x)$. Si esta es una inclusión propia, entonces $E \subsetneq H \subset S \setminus D(x)$, contradiciendo que $x \in H$. Por tanto se da la igualdad.

(2) $\Rightarrow$ (1) Basta con darnos cuenta que todo ideal propio que contiene a E, debe contener a x. Si hubiera un ideal propio I tal que $E \subsetneq I$ y $x \notin I$, por el lema 2.3 $I \subseteq S \setminus D(x) = E$, que contradice que I contiene a E estrictamente.

Como todo ideal propio que contiene a $E = S \setminus D(x)$ contiene a x, no podemos escribir E como intersección finita de ideales propios que lo contienen estrictamente y, por tanto, es irreducible.

□

De la proposición anterior, podemos pensar que todo ideal irreducible es de la forma $S \setminus D(x)$ para un cierto $x \in S$. La proposición anterior y los lemas que vamos a ver ahora apuntan en esa dirección, todo con el objetivo de llegar a un Teorema que nos proporcione una descomposición en componentes irreducibles.

Lema 2.4: Sea E un ideal propio de un semigrupo numérico S. Entonces:

1. Todo ideal irreducible que contiene a E es de la forma $S \setminus D(x)$ con $x \in S \setminus E$

2. Todo ideal irreducible que contiene a E y minimal con respecto a inclusión es de la forma $S \setminus D(x)$ con $x \in Maximales_{\leq_S}(S \setminus E)$

Demostración:

1. La primera proposición sigue de la proposición 7, pues si I es un ideal irreducible que contiene a E, entonces por ser irreducible es de la forma $S \setminus D(x)$, con $x \in S \setminus I \subseteq S \setminus E$

2. Analizando la inclusión $S \setminus D(y) \subseteq S \setminus D(x) \iff D(x) \subseteq D(y)$, para ciertos $x, y \in S$. $D(x) \subseteq D(y)$ supone que $x \in D(y)$ por lo que $x \leq_S y$. De lo cual concluimos la afirmación.

□

Lema 2.5: Dados E y F ideales propios de S, el conjunto:

$$E -_S F = \{s \in S \mid s + F \subseteq E\}$$

es también un ideal propio de S.

Demostración: Por como está definido, $E -_S F$ es un subconjunto de S. Para ver que es un ideal, podemos usar la misma demostración que usamos para demostrar que $E - F$ es un ideal, veamos que verifica las dos condiciones de la definición de ideal.

La primera, que $\forall z \in E -_S F$, y cualquier $s \in S$ $s + z \in E -_S F$. Por definición $\forall f \in F$, $\exists e \in E$ tal que $z + f = e \Rightarrow z + s + f = e + s \in E \Rightarrow z + s \in E -_S F$.

Para la segunda condición, tenemos que ver que existe $s \in S$ tal que $s + (E -_S F) \subseteq S$. Tomemos $s = f + s_F + s_E \in S$ (Donde s_F y s_E son elementos de S tales que $s_E + E \subseteq S$ y $s_F + F \subseteq S$). Dado $z \in E -_S F$, $\forall$, $\forall f \in F$, $\exists e \in E$ tal que $z + f = e \Rightarrow z = (e - f) \Rightarrow z + s = (e - f) + s_e + f + s_f = e + s_e \in S$.

□

Teorema 2.12: Sea S un semigrupo numérico, M $(M = S^* = S \setminus \{0\})$ su ideal maximal y sea E un ideal propio de S. Si $(E -_S M) \setminus E = \{x_1, \ldots, x_h\}$. Entonces:

$$E = (S \setminus D(x_1)) \cap \ldots \cap (S \setminus D(x_h))$$

Y esta descomposición de E en ideales de S propios e irreducibles es única y no redundante.

Demostración: Empezamos demostrando que $E = \bigcap_{x \in S \setminus E} (S \setminus D(x))$.

Por un lado, por el lema 2.3, tenemos que $E \subseteq S \setminus D(x)$, $\forall x \in S \setminus E$. Por tanto $E \subseteq \bigcap_{x \in S \setminus E}(S \setminus D(x))$.

Por otro lado, si $y \notin E \Rightarrow y \in D(y) \Rightarrow y \notin \bigcap_{x \in S \setminus E}(S \setminus D(x))$. Podemos reducir la descomposición anterior: tenemos que siempre se verifica que $\bigcap_{x \in S \setminus E}(S \setminus D(x)) \subseteq \bigcap_{x \in Maximales_{\leq_S}(S \setminus E)}(S \setminus D(x)$.

De hecho, se da igualdad, pues usando el lema 2.4, obtenemos que:
$\forall y \in S \setminus E$, $\exists x \in Maximales_{\leq_S}(S \setminus E)$ tal que $S \setminus D(y) \subseteq S \setminus D(x)$, luego obtenemos la otra contención.

$$E = \bigcap_{x \in S \setminus E} (S \setminus D(x)) = \bigcap_{x \in Maximales_{\leq_S}(S \setminus E)} (S \setminus D(x)$$

Si demostramos ahora que $(E -_S M) \setminus E = Maximales_{\leq_S}\{S \setminus E\}$ habremos demostrado el teorema. Por definición de "$-_S$" tenemos que $x \in (E -_S M) \setminus E \iff \forall y \in M,\ x+y \in S$. Vemos ahora que el lado izquierdo de la equivalencia es equivalente a que $x \in Maximales_{\leq_S}(S \setminus E)$:

Por un lado, si existe $y \in M$ tal que $x + y \notin S$ entonces $z := x + y \in S \setminus E \Rightarrow z - x = y \in S \Rightarrow z \leq_S x \Rightarrow x \notin Maximales_{\leq_S}(S \setminus E)$.

Por otro lado, si x no es máximal, entonces $\exists y \in S \setminus E$ tal que $y \geq_S x \Rightarrow z := y - x \notin S \Rightarrow x + z = y \notin E$, demostrando la equivalencia.

Poniendo todo lo que tenemos hasta ahora:

$$E = \bigcap_{x \in S \setminus E} (S \setminus D(x)) = \bigcap_{x \in Maximales_{\leq_S}(S \setminus E)} (S \setminus D(x) = \bigcap_{x \in (E -_S M) \setminus E} (S \setminus D(x) = \bigcap_{x \in \{x_1, \ldots, x_h\}} (S \setminus D(x)$$

La minimalidad y la no redundancia son garantizadas porque cada uno de los ideales de la forma $S \setminus D(x)$, $x \in Maximales_{\leq_S}(S \setminus E)$ es maximal con respecto a la contención y es, además, irreducible. A mayores, los ideales $S \setminus D(x)$ son propios e irreducibles.

□

Veamos un ejemplo aplicando este teorema:

Ejemplo 2.8: Sean $S = \langle 3, 5, 7 \rangle$ e $I = 10 + S$. Vamos a usar el teorema anterior para obtener una descomposición en irreducibles:

```
gap> S:=NumericalSemigroup(3,5,7);;
gap> I:=10+S;;
gap> Difference(Intersection(0+S,I-M),I);
[ 12, 14 ]
```

La penúltima línea calcula primero "Intersection(0+S,I-M)", que nos da $I -_S M$ (la intersección reduce la resta a elementos de S). Después con la función "Diffence()" nos da que $(I -_S M) \setminus I = \{12, 14\}$. Por tanto:

$$I = (S \setminus D(12)) \cap (S \setminus D(14))$$

Podemos obtener una expresión más explicita para la descomposición:

Vamos usar "d:=x->DivisorsOfElementInNumericalSemigroup(x,S)" para definir una función "$d(x)$" que devuelve los divisores de x en S.

"IdealByDivisorClosedSet(d(x),S)" nos devuelve el ideal $S \setminus D(x)$. Usando "MinimalGenerators()" podemos obtener un sistema de generadores de este ideal:

```
gap> d:=x->DivisorsOfElementInNumericalSemigroup(x,S);;
gap> MinimalGenerators(IdealByDivisorClosedSet(d(12),S));
[ 8, 10 ]
gap> MinimalGenerators(IdealByDivisorClosedSet(d(14),S));
[ 10, 12 ]
```

Por tanto: $I = (\{8, 10\} + S) \cap (\{10; 12\} + S)$.
Comprobamos que efectivamente, es cierto:

```
gap> Intersection(IdealByDivisorClosedSet(d(12),S),
IdealByDivisorClosedSet(d(14),S)) = I;
true
```

Capítulo 3

Introducción a códigos correctores lineales

En este capítulo dejamos los semigrupos numéricos por el momento para introducir las nociones básicas de códigos correctores de errores. En concreto, códigos lineales. Más adelante aplicaremos estos conceptos al contexto de semigrupo numéricos e ideales.

El objetivo de un código corrector de errores es detectar y corregir errores que se producen en el proceso de transmisión de información. En el contexto de este capitulo y en adelante pensaremos que los códigos que vamos a estudiar forman parte de un proceso de comunicación. En dicho proceso hay un emisor, que manda un mensaje a un receptor a través de un canal con "ruido". El mensaje será un vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ (en este capítulo y en adelante, denotaremos por $\mathbb{F}_q$ al único cuerpo finito de q elementos). Podemos pensar que el mensaje es un número binario con n-bits (aunque trabajaremos con cualquier cuerpo finito) transmitido a través de un medio digital y que el "ruido" del medio indica que hay una cierta probabilidad de que cualquier bit del mensaje pase de ser 0 a un 1 y viceversa.

Ejemplo 3.0.1:

El ejemplo más sencillo de un código corrector consiste en mandar varias copias del mensaje. Pensando el caso de mandar un mensaje binario, el emisor puede mandar 3 copias del mensaje original. El receptor solo tiene que comparar bit a bit las copias y si existe alguna discrepancia entre las copias, asumirá que las dos copias con el mismo valor en ese bit son correctas y corregirá el bit discrepante. Por ejemplo, si el bit número $k \in \{1, \ldots, n\}$ toma valor 1 para las dos primeras copias, pero 0 en la tercera, asumiremos que 1 es el valor correcto:
El emisor manda tres copias del mensaje $m \in \mathbb{F}_2^{n=3},\ m = \{1, 1, 1\}$ al receptor a través de un canal con ruido, el cual recibe lo siguiente:
Copia 1: $m_1 = \{1, 1, 1\}$

Copia 2: $m_2 = \{1, 0, 1\}$
Copia 3: $m_3 = \{1, 1, 1\}$

El emisor compara bit a bit las tres copias y observa una discrepancia en el bit número 2. Según el protocolo que hemos descrito, el receptor asume que el valor correcto es 1, pues es el que dos de las tres copias toman. Así corrige el error y recupera el mensaje original.

Este ejemplo es una primera aproximación al problema de corrección de errores. Notemos que si dos de las copias son alteradas, el receptor llegará a una conclusión errónea. Todos los códigos correctores tienen un límite de errores que pueden detectar y/o corregir, como veremos más adelante.

También observamos que este protocolo es muy poco eficiente, requiriendo triplicar el tamaño de cada mensaje. Esto es algo que podemos mejorar considerablemente.

Ejemplo 3.0.2:

Otro ejemplo sencillo de un código que permite detectar errores (si bien no corregirlos) es un *bit de paridad*. Dado un mensaje binario de longitud n, el emisor puede sumar en $\mathbb{F}_2$ todos los bits del mensaje y el resultado será 1 si hay un número impar de bits con valor "uno" y 0 si hay un número impar.

El emisor quiere mandar el mensaje $m \in \mathbb{F}_2^{n=8},\ m = \{1, 0, 1, 1, 1, 0, 0, 0\}$, luego computa la suma de los dígitos (módulo 2):

$$\overline{1+0+1+1+1+0+0+0} = \overline{0}\ \ (mod\ \ 2)$$

Para el mensaje m decimos que el bit de paridad es 0. Al receptor le llegará un mensaje codificado con nueve bits: $c = \{1, 0, 1, 1, 1, 0, 0, 0, 0\}$ donde los ocho primeros corresponden al mensaje y el último es el bit de paridad. Si la suma módulo 2 de los 8 primeros bits no coincide con el bit de paridad sabrá que se ha producido al menos un error.

Este método requiere muy poco espacio extra, pero solo permite detectar si se han producido errores (no corregirlos) y solo si el número de errores es impar.

En adelante, consideramos que el emisor manda un mensaje $m \in \mathbb{F}_q^k$. Veremos en el contexto de los códigos lineales lo que supone codificar el mensaje y cómo es el espacio de mensajes codificados.

3.1. Conceptos básicos

Vamos a introducir a continuación las definiciones y conceptos básicos sobre códigos lineales. Empezamos dando la definición de código lineal:

Definición 3.1.1: Un **código lineal** $\mathcal{C}$ sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$.
Además en referencia a un código lineal $\mathcal{C}$ consideramos los parámetros:

- **Longitud** si el código es subespacio de $\mathbb{F}_q^n$ entonces llamaremos a n longitud de $\mathcal{C}$.
- k, la **dimensión** del código como espacio vectorial.

Dado un código lineal, diremos que es de tipo $[n,k]$ ó $[n,k,d]$ (donde d es la distancia mínima, que definiremos a continuación) y diremos que la redundancia es $r = n - k$
Vamos a definir la *distancia mínima* y la *distancia de Hamming.*

Definición 3.1.2: Dados $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_q^n$, $\mathbf{x} = (x_1, \ldots, x_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$, la **distancia de Hamming** entre $\mathbf{x}, \mathbf{y}$ es:

$$d(\mathbf{x},\ \mathbf{y}) = \left|\left\{i \mid x_i \neq y_i,\ i \in \{1, 2, \ldots, n\}\right\}\right|$$

Proposición 3.1.1: La distancia de Hamming es una distancia en $\mathbb{F}_q^n$.

Demostración:

1. Vemos que d es no negativa y que $d(\mathbf{x},\ \mathbf{y}) = 0 \Longleftrightarrow \mathbf{x} = \mathbf{y}$:
   La no negatividad sigue que $d(\mathbf{x}, \mathbf{y})$ se define como el cardinal de un conjunto, por lo que no puede ser negativo.
   Si $\mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{y} = (y_1, \ldots, y_n)$ y $\mathbf{x} = \mathbf{y}$ entonces $\forall i \in \{1, 2, \ldots, n\},\ x_i = y_i \Rightarrow d(\mathbf{x},\ \mathbf{y}) = 0$.
   Por otro lado, si $0 = d(\mathbf{x},\ \mathbf{y})$, entonces, por definición de "d", $x_i = y_i,\ \forall i \in \{1, 2, \ldots, n\} \Rightarrow \mathbf{y} = \mathbf{x}$.

2. Claramente, $d(\mathbf{x},\ \mathbf{y}) = d(\mathbf{y},\ \mathbf{x})$ pues la definición es simétrica.

3. Finalmente, veamos que verifica la desigualdad triangular: $d(\mathbf{x},\ \mathbf{y}) + d(\mathbf{y},\ \mathbf{z}) \geq d(\mathbf{x},\ \mathbf{z})$:
   Denotemos $I = \left\{i \mid x_i \neq y_i,\ i \in \{1, 2, \ldots, n\}\right\}$, $J = \left\{i \mid y_i \neq z_i,\ i \in \{1, 2, \ldots, n\}\right\}$ y $K = \left\{i \mid x_i \neq z_i,\ i \in \{1, 2, \ldots, n\}\right\}$ Si $i \in K$, por definición $x_i \neq z_i$. Entonces no puede ser que $(i \notin I) \wedge (i \notin J)$, pues si fuera así entonces $(x_i = y_i) \wedge (y_i = z_i) \Rightarrow x_i = z_i \Rightarrow i \neq K$, lo cual es una contradicción.
   Entonces concluimos que

$$i \in K \Rightarrow (i \in I) \vee (i \in K) \Rightarrow d(\mathbf{y},\ \mathbf{x}) = |K| \leq |I| + |J| = d(\mathbf{y},\ \mathbf{x}) + d(\mathbf{y},\ \mathbf{z})$$

Definición 3.1.3: Usando la distancia de Hamming, podemos definir una norma en $\mathbb{F}_q^n$. Sea $\mathbf{0} = (0, \ldots, 0)$, llamamos **peso de Hamming** de $\mathbf{x}$ a:

$$w(\mathbf{x}) := d(\mathbf{x}, \mathbf{0})$$

De forma análoga a la demostración anterior, es fácil ver que el peso de Hamming define una norma en $\mathbb{F}_q^n$.

Definición 3.1.4: Dado un código lineal $\mathcal{C}$.

- Llamaremos a d la **distancia mínima** de $\mathcal{C}$ a:

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

- Llamaremos **peso mínimo** de $w(\mathcal{C})$ a:

$$w(\mathcal{C}) = min\{w(c) \mid c \in \mathcal{C},\ c \neq \mathbf{0}\}$$

- Dado $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, denominaremos **soporte** de $\mathbf{x}$ a:

$$sop(\mathbf{x}) = \left\{ i \;\middle|\; x_i \neq 0,\ i \in \{1, 2, \ldots, n\} \right\}$$

La distancia mínima, es una de las ideas centrales de los códigos correctores lineales. Si es d es la distancia mínima de un código $\mathcal{C}$, y conocemos el conjunto de todos los mensajes codificados, entonces tenemos, automáticamente, un **algoritmo** para decodificar cualquier código lineal (si bien uno no muy eficiente):

1. Al recibir un mensaje codificado por un código lineal, el receptor puede comparar el mensaje recibido con el conjunto de mensajes posibles (todo $\mathcal{C}$). Si el mensaje recibido coincide con un elemento de $\mathcal{C}$, asumirá que no se ha producido ningún error.

2. Si no coincide, entonces el receptor computará la distancia entre el mensaje-código recibido y cada uno de los códigos de $\mathcal{C}$. Asumirá que el que tenga la menor distancia al código recibido será el mensaje original.

Este algoritmo no se puede usar en la práctica salvo para códigos con pocos elementos. Sin embargo, nos da una idea de cuál es la capacidad correctora de un código, pues está basado en la idea la idea de se producen, en general, pocos errores. Entonces, si recibimos una palabra que no está en el código, asumimos que la palabra del código que más se le asemeje es la palabra original. Si el número de errores es pequeño, esto es cierto. Podemos formalizar esto por medio de la idea de **capacidad correctora**:

Usando el algoritmo anterior, podemos corregir $t = \lfloor \frac{d-1}{2} \rfloor$ errores:

Proposición 3.1.2: Un código lineal $\mathcal{C}$ cuya distancia mínima es d puede corregir $t = \lfloor \frac{d-1}{2} \rfloor$ errores. A este número lo llamaremos **capacidad correctora** del código y lo denotamos por t.

Demostración: Si el mensaje original $\mathbf{m} \in \mathcal{C}$ sufre t o menos errores, llegará al receptor como $\mathbf{y} \in \mathbb{F}_q^n$. El receptor detectará que hay errores, pues $d(\mathbf{y}, \mathbf{m}) = s \leq t < d \Rightarrow \mathbf{y} \notin \mathcal{C}$. La palabra de $\mathcal{C}$ que tiene la mínima distancia de Hamming a $\mathbf{y}$, es el mensaje original m (y no hay otra palabra de $\mathcal{C}$ a la misma distancia, $d(\mathbf{m}, \mathbf{y}) = s$). De lo contrario, existiría $\mathbf{z} \in \mathcal{C}$ tal que $d(\mathbf{z}, \mathbf{y}) = s' \leq s \leq t$. Aplicando la desigualdad triangular, $d(\mathbf{z}, \mathbf{m}) \leq d(\mathbf{z}, \mathbf{y}) + d(\mathbf{y}, \mathbf{m}) = s' + s \leq 2t < d$, lo cual contradice la hipótesis que la distancia mínima del código es d.

Por tanto, si se han cometido t o menos errores, el algoritmo que hemos descrito nos permite decodificar el mensaje, pues el mensaje original, m, será aquel que esté a menor distancia de Hamming del mensaje con errores y.

□

Es deseable que la distancia mínima del código sea lo mayor posible con el fin de que la capacidad correctora sea lo mayor posible. También es deseable que $n-k$ sea lo menor posible, ya que así el mensaje codificado ocupará lo menos posible.

Lema 3.1 Sea $\mathcal{C}$ un código lineal, entonces su distancia mínima es igual a su peso mínimo.

Demostración: Como $\mathcal{C}$ es un espacio vectorial, esta propiedad es consecuencia de la igualdad $w(\mathbf{x}-\mathbf{y}) = d(\mathbf{x}-\mathbf{y}, \mathbf{0}) = |\{i \mid x_i - y_i \neq 0,\ i \in \{1, 2, \ldots, n\}\}| = |\{i | x_i \neq y_i,\ i \in \{1, 2, \ldots, n\}\}| = d(\mathbf{x}, \mathbf{y})$.

□

En el contexto de la definición anterior, podemos interpretar $\mathbb{F}_q^n$ como la imagen por una aplicación lineal f, del espacio vectorial $\mathbb{F}_q^k$ a $\mathbb{F}_q^n$. $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ puede ser entendida como una aplicación que codifica un mensaje que pertenece al espacio origen. Con esta idea damos la siguiente definición:

Definición 3.1.5: Llamaremos **matriz generatriz** del código $\mathcal{C}$ a la matriz de una aplicación lineal inyectiva $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$. Además, dada G, una matriz generatriz $k \times n$ y un mensaje $m \in \mathbb{F}_q^k$ diremos que $c = mG \in \mathbb{F}_q^n$ es el **mensaje codificado** (escribiendo los vectores en forma de fila). c es el mensaje que recibirá el receptor.

Como la matriz generatriz define una base de $\mathcal{C}$, no es única. Dada G una matriz generatriz de $\mathcal{C}$, cualquier matriz semejante a G es también matriz generatriz de $\mathcal{C}$.

De la definición anterior podemos deducir varias cosas. Por una lado, el requisito de inyectividad lleva a que, en casos no triviales, $n > k$. Es decir, que para que un código tenga capacidad correctora es necesario que el mensaje codificado ocupe más espacio del que el mensaje original ocupa de por sí.

Además, notamos que la matriz generatriz es una matriz $k \times n$ cuyas columnas forman una base de $\mathcal{C}$.

Ejemplo 3.1.3: Consideremos el código lineal dado por la siguiente matriz generatriz (con cuerpo $\mathbb{F}_2$):

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

En este caso tenemos que $G : \mathbb{F}_2^3 \to \mathbb{F}_2^4$, con longitud $n = 4$ y dimensión $k = 3$. Hay $2^k = 2^3$ posibles mensajes o palabras que se pueden transmitir. Si consideramos la imagen de G, obtenemos que:

$$\mathcal{C} = \{(0,0,1,1),\ (1,1,0,0),\ (1,0,1,0),\ (1,1,1,1),\ (1,0,0,1),\ (0,1,1,0),\ (0,1,0,1),\ (0,0,0,0)\}.$$

De lo anterior, podemos computar la distancia mínima, tomando la mínima distancia de las distancias entre todos los posibles pares de vectores de $\mathcal{C}$; en este caso es 2.

Dado el mensaje $m = (1,0,1)$, su codificación es:

$$c = m \times G \ = \ (1,\ 0,\ 1) \times \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (1,\ 0,\ 0,\ 1)$$

Con lo estudiado hasta este punto podemos entender los fundamentos básicos de un código lineal y cómo se codifican mensajes. Lo que nos falta por ver es el proceso de decodificación. Existen algoritmos de decodificación genéricos (ver algoritmo del líder), pero, en general, no son prácticos para situaciones reales. Por ello, se suele estudiar familias de códigos lineales que tienen un algoritmo de decodificación propio. En nuestro caso, usaremos códigos algebraico-geométricos.

3.2. Otros conceptos de códigos lineales

Los conceptos anteriores nos valen para abordar los códigos AG, pero en esta sección vamos a explorar códigos lineales en más profundidad. En particular, vamos a analizar cómo podemos usar un algoritmo genérico de decodificación.

El primero es el de **matriz de control**. La matriz generatriz define el código dando una base, pero un espacio vectorial puede ser definido mediante ecuaciones implícitas.

Definición 3.2.6: Diremos que la matriz H es **matriz de control** del código $\mathcal{C}$ si para todo $\mathbf{x} \in \mathbb{F}_q^n$ se verifica que: $\mathbf{x} \in \mathcal{C} \iff H\mathbf{x}^t = \mathbf{0}$

De esta definición podemos inferir que una matriz de control es la matriz de coeficientes de las ecuaciones implícitas que definen $\mathcal{C}$ como subespacio vectorial.

Ejemplo 3.2.4: Para el ejemplo que hemos visto antes, $H = (1,\ 1,\ 1,\ 1)$ es una matriz generatriz.

Proposición 3.2.3: Dado un código lineal $\mathcal{C}$ definido en $\mathbb{F}_q$ de tipo $[n, k]$, entonces su matriz de control, H, también está definida en $\mathbb{F}_q$. Además:

- H tiene rango $n - k$:
- H es una matriz $(n - k) \times n$.

Demostración:

- $\mathcal{C}$ es un subespacio de dimensión k de $\mathbb{F}_q^n$, luego está determinado por $n - k$ ecuaciones implícitas y por tanto H debe tener $n - k$ filas.
- H debe tener n columnas para que la multiplicación por elementos de $\mathbb{F}_q^n$ sea posible.

□

Proposición 3.2.4: Sea $\mathcal{C}$ un código lineal definido en F_q^n y sean G y H su matriz generatriz y su matriz de control respectivamente. Entonces: $GH^t = 0$.
El recíproco también es cierto, dado un código lineal $\mathcal{C}$ con matriz generatriz G y una matriz H con la propiedad $GH^t = 0$ entonces H es matriz de control de $\mathcal{C}$.

Demostración: Si partimos de $(GH^t)^t = HG^t$ entonces para todo $\mathbf{x} \in \mathbb{F}_q^k \Rightarrow \mathbf{y}^t = G^t\mathbf{x}^t \in \mathcal{C} \subseteq \mathbb{F}_q^n$, por tanto, $H\mathbf{y}^t = 0$.

En particular, dada una base $\mathcal{B} = \{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$ de $\mathbb{F}_q^k$ tenemos que $\forall b_i \in \mathcal{B},\ H\ G^t{\mathbf{b_i}}^t = 0$. Dado que $H\ G^t$ es una matriz $(n-k) \times k$, la única opción es que sea la matriz nula.

Para el recíproco, cualquier mensaje codificado $\mathbf{c} \in \mathbb{F}_q^n$ es de la forma $\mathbf{c} = \mathbf{m}G$ con $\mathbf{c} \in \mathbb{F}_q^k$. Entonces $H\mathbf{c}^t = H(\mathbf{m}G)^t = HG^t\mathbf{m}^t = \mathbf{0}$ ($HG^t = 0$ pues $HG^t = (GH^t)^t = (0)^t$). Por tanto H es matriz de control de $\mathcal{C}$

□

Proposición 3.2.5: Sea $\mathcal{C}$ un código lineal cuya matriz de control es H y su distancia mínima es d. Entonces, $d > r$ si y solo si r columnas cualquiera de H son linealmente independientes.

Demostración: Si existen r columnas linealmente dependientes de H:

Sean $\mathbf{c_1}, \ldots, \mathbf{c_n} \in \mathbb{F}_q^{n-k}$ las columnas de H. Consideremos $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ un vector tal que $\sum_{i=1}^{n}(x_i\mathbf{c_i}) = 0$ y $x_i \neq 0 \Longleftrightarrow i \in I \subseteq \{1, 2, \ldots, n\}, |I| = r$. Es decir, nos da los coeficientes para obtener una combinación lineal de r columnas de H que sea igual a $\mathbf{0}$. Entonces, $H\mathbf{x}^t = \mathbf{0}$ y por tanto $\mathbf{x} \in \mathcal{C}$. Por como hemos definido $\mathbf{x}$, su peso es menor o igual que r y al ser elemento del código, la distancia mínima, d, del código debe ser menor o igual que r.

Si partimos de la premisa que, r columnas cualesquiera de H son linealmente independientes, usando la argumentación anterior, no puede haber ningún vector con peso menor o igual que r que pertenezca al código $\mathcal{C}$. Por tanto la distancia mínima será mayor que r.

□

Corolario 3.2.6: Sea $\mathcal{C}$ un código lineal y H su matriz de control. Entonces, la distancia mínima, d, de $\mathcal{C}$ es cardinal del menor conjunto de columnas de H linealmente dependientes.

Demostración: Por la proposición anterior sabemos que si $r+1$ es el cardinal del mayor conjunto de columnas de H linealmente dependientes, entonces $d > r$. Además, la igualdad $d = r+1$ se alcanza, pues el vector que nos proporciona un combinación lineal igual a 0, de $r+1$ columnas, debe tener $r+1$ coordenadas no nulas, por tanto su peso es $r+1$ y se alcanza la igualdad $d = r+1$.

□

Corolario 3.2.7(Cota de Singleton): Si $\mathcal{C}$ es un código lineal de tipo $[n, k, d]$ sobre $\mathbb{F}_q$, entonces, $k + d \leq n + 1$.

Demostración: Sea H la matriz de control del código $\mathcal{C}$. Por el corolario anterior, la distancia mínima, d, coincide con el número de mínimo columnas linealmente independientes de H. Puesto que H tiene rango $n-k$, el número es a lo sumo $n-k+1$, luego $d \leq n-k+1 \Rightarrow k+d \leq n+1$

□

Definición 3.2.7: Los códigos que alcanza la cota de Singleton se dice que son de **máxima distancia de separación** o, para abreviar, **MDS**.

Que un código sea MDS es una propiedad deseable, pues para una elección de los parámetros $[k, d]$, un código MDS maximiza el valor de la distancia mínima y, en consecuencia, la capacidad correctora del código.

Sea $\mathcal{C}$ un código lineal $[n, k]$, con matriz generatriz G y matriz de control H. Existe una dualidad entre matriz generatriz y matriz de control. La matriz generatriz es una matriz de rango máximo $(n-k)$, por tanto, define una aplicación lineal $H : \mathbb{F}_q^{n-k} \to \mathbb{F}_q^n$ y, en consecuencia, su imagen es un subespacio vectorial y, es decir, un código lineal.

Definición 3.2.8: Dado $\mathcal{C}$ un código lineal y H su matriz de control. Llamaremos **código dual** de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$ al código lineal cuya matriz generatriz es H.

Además, debido a que $GH^t = 0$, entonces $HG^t = 0$ y G es una matriz de control de C^t.

Ambos códigos son subespacios vectoriales de $\mathbf{F}_q^n$. De hecho, son espacios ortogonales. Efectivamente, si $\mathbf{c} \in \mathcal{C}$ y H es la matriz de control de $\mathcal{C}$ y G su matriz generatriz, entonces un elemento del dual, $\mathbf{c'}$, es siempre la imagen de un cierto $\mathbf{m'} \in \mathbb{F}_q^{n-k}$ por la matriz generatriz de $\mathcal{C}^\perp$, H, es decir $\mathbf{c'} = H(\mathbf{m'})^t$. Así mismo, $\mathbf{c} = G\mathbf{m}^t$, para cierto $\mathbf{m} \in \mathbb{F}_q^k$. Si consideramos el producto escalar:

$$\langle \mathbf{c}, \mathbf{c'} \rangle = \langle G\mathbf{m}^t, H\mathbf{m'}^t \rangle = (\mathbf{m}G)(H(\mathbf{m'})^t) = \mathbf{m}0(\mathbf{m'})^t = 0$$

Luego ambos espacios son ortogonales.

3.3. Síndromes y líderes

Los últimos conceptos que introduciremos sobre códigos lineales son los del de síndrome y líder. Si el emisor manda un mensaje codificado $\mathbf{c} \in \mathcal{C} \subseteq \mathbb{F}_q^n$ a través de un canal con ruido entonces se puede producir un error $\mathbf{e} \in \mathbb{F}_q^n$ ($\mathbf{e}$ puede ser $\mathbf{0}$) y el receptor recibirá $\mathbf{y} = \mathbf{c} + \mathbf{e}$.

Definición 3.3.9: Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código lineal y H su matriz de control. Sea $\mathbf{y}$ el un mensaje recibido por el receptor tal y como hemos descrito anteriormente. Entonces llamaremos **síndrome** de $\mathbf{y}$ al vector:

$$s(\mathbf{y}) \ = \ H\mathbf{y}^t \ \in \ \mathbb{F}_q^{n-k}$$

Al recibir un mensaje, el receptor puede comprobar si el mensaje pertenece al código computando el síndrome, pues $H\mathbf{x}^t = \mathbf{0}$, $\forall \mathbf{x} \in \mathcal{C}$. Además, por ser $s(\mathbf{y})$ una aplicación lineal, tenemos que $s(\mathbf{y}) = s(\mathbf{m}+\mathbf{e}) = s(\mathbf{m}) + s(\mathbf{e}) = s(\mathbf{e})$, obtenido así el síndrome del error cometido (el receptor solo conoce $\mathbf{y}$, $\mathbf{e}$ y $\mathbf{m}$ son desconocidos).

Proposición 3.3.8: El síndrome de un vector $\mathbf{y}$ es una combinación lineal de las columnas de H a las combinaciones en las que han ocurrido errores.

Demostraciones: Las posiciones del vector de error, $\mathbf{e} = (e_1, \ldots, e_n)$, que nos son cero son en las cuales se ha producido un error. Sea $I \subseteq \{1, 2, \ldots, n\}$ el conjunto de índices tales que $e_i \neq 0$, $\forall i \in I$. Sabemos que $s(\mathbf{y}) = s(\mathbf{e}) = H\mathbf{e}^t$, si denotamos por $\mathbf{c}_1, \ldots, \mathbf{c}_n$ a las columnas de H, entonces:

$$s(\mathbf{y}) = \sum_{i=1}^{n} e_i \mathbf{c}_i = \sum_{i \in I} e_i \mathbf{c}_i$$

□

Podemos combinar esta proposición con la propiedad de la matriz de control (H) que vimos anteriormente; por la cual si la distancia del código lineal es d, $d-1$ columnas cualesquiera de H son linealmente independientes. Veamos un ejemplo sencillo de como el síndrome puede ayudar con el proceso de decodificación.

Ejemplo 3.3.5: Supongamos un código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$ cuya distancia mínima es al menos 3 y emisor que manda un mensaje codificado $c \in \mathcal{C}$ a través de un canal con ruido y el receptor recibe $\mathbf{y}$. Para este ejemplo, supongamos que se produce un único error $\mathbf{e} = (0, \ldots, 0, e_i \neq 0, \ldots, 0)$, $\mathbf{y} = \mathbf{c} + \mathbf{e}$. Tenemos que si $\mathbf{c}_i$ es la columna i-ésima de H, $s(\mathbf{y}) = H\mathbf{e}^t = \mathbf{c}_i e_i$, basta ahora resolver y obtener e_i (y por tanto $\mathbf{e}$). La proposición anterior nos asegura que $s(\mathbf{y})$ es combinación lineal de una, y solo una columna de H ($\mathbf{c}_i$); por lo que el sistema será resoluble. El mensaje original será $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

Este concepto de síndrome, lo podemos usar para proporcionar un algoritmo de decodificación. Se trata de una versión más refinada y más eficiente del algoritmo describimos anteriormente.

Definición 3.3.10: Consideremos la relación de equivalencia ($\sim$) para $\mathbf{u}, \mathbf{v} \in \mathbf{F}_q^n$, $\mathbf{u} \sim \mathbf{v} \Leftrightarrow (u - v) \in \mathcal{C}$. Si existe un único representante de la case cuyo peso de Hamming es mínimo, lo denotaremos **líder** de la clase.

Notemos que $(\mathbf{u} - \mathbf{v}) \in \mathcal{C} \Rightarrow s(\mathbf{u} - \mathbf{v}) = H(\mathbf{u} - \mathbf{v})^t = 0 \Rightarrow s(u) = s(v)$. Es decir, todos los representantes de la case tienen el mismo síndrome; y por tanto, si recibimos un mensaje $\mathbf{y}$,

al conocer $s(\mathbf{y}) = s(\mathbf{e})$ conocemos la clase a la que pertenece el error cometido e.
Es importante notar que, en general, no toda clase tiene líder, hay dos elementos con el peso minimal, no existe líder. Pero si lo hay tenemos que:

Proposición: 3.3.9 Cada clase de equivalencia de $\mathbb{F}_q^n/(\sim)$ posee un único elemento de peso $\leq t = \lfloor \frac{d-1}{2} \rfloor$.

Demostración: Supongamos que existen dos elementos de la misma clase con peso menor o igual a la capacidad correctora. Es decir, sean $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ tales que $\mathbf{u} - \mathbf{v} \in \mathcal{C}$ y $w(\mathbf{u}) \leq t$, $w(\mathbf{v}) \leq t$. Entonces $w(\mathbf{u} - \mathbf{v}) \leq w(\mathbf{u}) + w(\mathbf{v}) \leq 2t < d$. Por definición de distancia mínima, concluimos que $\mathbf{u} - \mathbf{v} = 0 \Rightarrow \mathbf{u} = \mathbf{v}$.

□

3.4. Algoritmo del líder

Vamos a dar un algoritmo de decodificación, algo más refinado que el primero que vimos. Se basa en los conceptos de síndrome y líder que acabamos de ver, así como en otros dos conceptos; que conocer el líder de una clase de equivalencia en $\mathbb{F}_q^n/(\sim)$ (si existe y su peso es menor que t) es lo mismo que conocer el error y que una clase de equivalencia se identifica por su síndrome (todos los elementos de la clase tienen el mismo síndrome).

Veamos lo primero. Siguiendo un razonamiento similar a cuando definimos la distancia de Hamming y dimos el primer algoritmo de decodificación, decodificar consistirá en encontrar la palabra de $\mathcal{C}$, más próxima al vector recibido, $\mathbf{y}$ (solo se podrá decodificar si hay una única palabra). Es decir, $argmin_{\mathbf{x}\in\mathcal{C}}(d(\mathbf{y}, \mathbf{x})) = argmin_{\mathbf{x}\in\mathcal{C}}(w(\mathbf{y} - \mathbf{x})) =: \mathbf{l}$, donde, $\mathbf{l}$ es, por definición, el líder de la clase $\{\mathbf{y} - \mathbf{x} \mid \mathbf{x} \in \mathcal{C}\}$. Si la clase tiene líder, y este tiene peso menor o igual a la capacidad correctora del código, t, entonces la proposición anterior nos garantiza que es el único con esta propiedad. Trabajando sobre la idea de que no se han producido más de t errores, concluimos que el líder de la clase ($\mathbf{l} = \mathbf{y} - \mathbf{x}$) es el error cometido, $\mathbf{e}$ (pues $\mathbf{c}' = \mathbf{y} + \mathbf{l} \in \mathcal{C}$ y es la palabra del código más cercana a $\mathbf{y}$; a distancia menor o igual a t).

Que una clase se identifica por su síndrome es sencillo, pues sabemos que $\forall \mathbf{x} \in \mathcal{C},\ s(\mathbf{y}-\mathbf{x}) = s(\mathbf{y}) + 0$. Luego el síndrome del mensaje recibido, $\mathbf{y}$, coincide con el síndrome del líder de la clase. Con estas dos ideas, describimos el siguiente algoritmo de decodificación:

1. Fase inicial: preparamos una tabla de síndromes y líderes como se indica a continuación. Esta nos servirá para todas las decodificaciones.

   a) Creamos una tabla de dos columnas y tantas filas como clases de equivalencia en

$\mathbb{F}_q^n/(\sim)$ (Es decir, q^{n-k} filas).

b) En la primera columna escribimos el síndrome de un elemento cualquiera de cada una de las clases, en la segunda, escribimos el líder de la clase.

2. Con la tabla anterior guardada podemos decodificar cualquier mensaje. El emisor manda un mensaje $\mathbf{m} \in \mathbb{F}_q^k$, que codifica como $\mathbf{c} \in \mathbb{F}_q^n$, y el receptor recibe $\mathbf{y} \in \mathbb{F}_q^n$.

   a) El receptor calcula $s(\mathbf{y})$ y lo busca en la columna de síndromes.

   b) Si la clase no tiene líder, el algoritmo falla y finaliza el proceso.

   c) Si la clase tiene líder, $\mathbf{e}$, se asume que $\mathbf{e}$ es el error cometido. Por tanto, la palabra decodificada asumimos que es $\mathbf{c}' = \mathbf{y} - \mathbf{e}$.

Ejemplo 3.4.6: Consideremos el código binario con matriz generatriz

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

Donde $\mathcal{C} = \{G((0,0)) = (0,0,0,0,0,0,0,0), G((1,0)) = (1,0,1,1,1,1,0,0),$
$G((0,1)) = (0,1,0,1,1,1,1,1),\ G((1,1)) = (1,1,1,0,0,0,1,1)\}$, y podemos computar la distancia mínima, que es 5 y la capacidad correctora es $t = \lfloor \frac{5-1}{2} \rfloor = 2$. Una matriz de control es:

$$H = ((\mathbf{c}_3, \mathbf{c}_4, \ldots, \mathbf{c}_8)^t | Id_6) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Donde $\mathbf{c}_i$ es la columna i-ésima de G. Al final del ejemplo está la tabla de líderes y síndromes.

Consideremos 3 mensajes:

1. Al receptor le llega $\mathbf{y} = (1,1,0,1,1,0,1,1)$.

   a) Computa $s(\mathbf{y}) = H\mathbf{y}^t = (1,1,1,0,0,0)^t$.

   b) Busca en la tabla de síndromes el líder de la clase, que es $\mathbf{e} = (1,0,0,0,0,1,0,0)$

   c) Por tanto $\mathbf{c}' = \mathbf{y} - \mathbf{e} = (1,1,0,1,1,0,1,1) + (1,0,0,0,0,1,0,0) = (0,1,0,1,1,1,1,1) \in \mathcal{C}$, que es la palabra enviada. Como el líder tiene peso dos y $t = 2$, entonces la corrección es correcta (si no ha habido más de 2 errores).

2. Al receptor le llega $\mathbf{y} = (0,1,1,1,0,0,1,0)$.

a) Computa $s(\mathbf{y}) = (1,0,1,1,0,1)^t$.

b) Busca en la tabla de síndromes el líder de la clase, que es $\mathbf{e} = (1,0,0,1,0,0,0,1)$.

c) Por tanto $\mathbf{c}' = \mathbf{y} - \mathbf{e} = (0,1,1,1,0,0,1,0) + (1,0,0,1,0,0,0,1) = (1,1,1,0,0,0,1,1) \in \mathcal{C}$, que es la palabra enviada. En este caso, el peso del líder es 3 (más que la capacidad correctora), pero aún así podemos decodificarlo ($[1,1,1,0,0,0,1,1]$ sigue siendo el vector más cercano). Sabemos que se han producido al menos 3 errores.

3. Al receptor le llega $\mathbf{y} = (0,1,0,1,1,0,0,0)$.

a) Computa $s(\mathbf{y}) = (0,0,0,1,1,1)^t$.

b) Vemos que la clase no tiene líder, luego el algoritmo falla.

c) Sabemos que, por tener el síndrome peso 3, se han producido al menos 3 errores.

síndrome	líder
000000	00000000
000001	00000001
000010	00000010
000011	00000011
000100	00000100
000101	00000101
000110	00000110
000111	

síndrome	líder
001000	00001000
001001	00001001
001010	00001010
001011	
001100	00001100
001101	
001110	
001111	01010000

síndrome	líder
010000	00010000
010001	00010001
010010	00010010
010011	
010100	00010100
010101	
010110	
010111	00011000

síndrome	líder
011000	00011000
011001	
011010	
011011	01000100
011100	10100000
011101	01000010
011110	01000001
011111	01000000

síndrome	líder
100000	00100000
100001	00100001
100010	00100010
110011	00100010
100100	00100100
100101	00100101
100110	00100110
100111	11000100

síndrome	líder
101000	00101000
101001	00101001
101010	00101010
101011	11001000
101100	10010000
101101	10010001
101110	10010010
101111	01110000

síndrome	líder
110000	00110000
110001	00110001
110010	00110010
110011	11010000
110100	10001000
110101	10001001
110110	10001010
110111	01101000

síndrome	líder
111000	10000100
111001	10000101
111010	10000110
111011	01100100
111100	10000000
111101	10000001
111110	10000010
111111	01100000

El algoritmo del líder permite decodificar, teóricamente, cualquier código lineal, pero su utilidad, al igual que en el caso de primer algoritmo se limita a códigos de tamaño reducido; pues el algoritmo requiere almacenar una tabla con los q^{n-k} síndromes distintos. Esto hace

que el problema sea exponencial en cuanto a los requisitos de memoria. Vemos que el concepto de síndrome nos permite dar otra forma de decodificar.

3.5. Decodificación con sistemas lineales de ecuaciones

Sea $\mathcal{C}$ un código lineal de parámetros $[n, k, d]$ definido en $\mathbb{F}_q$. Si el emisor codifica el mensaje $\mathbf{m} \in \mathbb{F}_q^k$, como $\mathbf{c} \in \mathbb{F}_q^n$, y este se transmite a través de un canal con ruido, de modo que el receptor recibe el mensaje $\mathbf{y} = \mathbf{c} + \mathbf{e}$ (donde $\mathbf{e}$ es el error que se ha producido). Entonces, vemos que es suficiente con encontrar un conjunto $I \subset \{1, 2, \ldots, n\}$, con cardinal $|I| < d$, tal que $sop(\mathbf{e}) \subseteq I$. Efectivamente, si planteamos el sistema de ecuaciones:

$$\begin{cases} s(\mathbf{x}) \;=\; s(\mathbf{y}) \\ x_i \;=\; 0, \quad \text{si } i \notin I \end{cases} . \tag{3.1}$$

Vemos que $\mathbf{e}$ es un solución, $s(\mathbf{y}) = s(\mathbf{c}) + s(\mathbf{e}) = 0 + s(\mathbf{e})$ y $sop(\mathbf{e}) \subseteq I$. Además, si $\mathbf{e}'$ es otra solución al sistema,$(\mathbf{y} - \mathbf{e}), (\mathbf{y} - \mathbf{e}') \in \mathcal{C}$ (pues su síndrome es cero). Pero, si consideramos la distancia mínima entre ambas palabras-código, $d\big((\mathbf{y} - \mathbf{e}), (\mathbf{y} - \mathbf{e}')\big) = d(\mathbf{e}, \mathbf{e}') \leq |I| < d$. Pero esto contradice que d sea la distancia mínima del código. Por tanto, $\mathbf{e}$ es la única solución del sistema, y resolver el sistema no permite decodificar cualquier mensaje.

Esta es también una solución genérica al problema decodificación. Sin embargo, resolver un sistema de ecuaciones nxn tiene un coste $O(n^3)$ para algoritmos de eliminación gausiana, y no hay algoritmos que puedan dar una solución con coste $O(n^2)$ o inferior. Este coste sigue siendo alto, por lo que es común estudiar familias particulares de códigos que, por sus propiedades y estructura, tienen un algoritmo de decodificación más eficiente.

3.6. Códigos de evaluación

El objetivo del capítulo siguiente, es introducir los códigos AG. Hasta ahora hemos introducido conceptos básicos de códigos lineales. Los códigos AG forman de un tipo más amplio de código llamado **códigos de evaluación**, los cuales introducimos ahora. Al final de esta sección veremos un ejemplo completo.

Definición 3.6.11:

Sea $\mathcal{X}$ una "objeto geométrico" (seremos más específicos mas adelante), $\mathcal{P} = \{P_1, \ldots, P_n\}$ un conjunto de puntos de $\mathcal{X}$ y V el espacio vectorial de funciones $f : \mathcal{X} \to \mathbb{F}_q$. Llamaremos **evaluación en** $\mathcal{P}$ a la aplicación:

$$ev_{\mathcal{P}} : V \longrightarrow \mathbb{F}_q^n,\ ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

Si $ev_{\mathcal{P}}$ es una aplicación lineal, su imagen es un subespacio vectorial de F_q^n y, por tanto, un código lineal sobre $\mathbb{F}_q^n$ con longitud n. Los mensajes codificados son de la forma $ev_{\mathcal{P}}(f),\ f \in V$. Este tipo de código es un **código de evaluación**, pues lo hemos obtenido evaluando $\mathcal{P}$ en las funciones de V. Para códigos algebraicos $\mathcal{X}$ es una curva algebraica, pero dependiendo del tipo de objeto que sea $\mathcal{X}$ obtendremos diferentes familias de códigos de evaluación.

3.7. Un ejemplo completo, códigos de Hamming

Veamos un ejemplo con un tipo de código famoso: **Códigos de Hamming** (Extendido) [16, 11].

Código de Hamming de forma intuitiva:

Los códigos de Hamming se basan en la misma idea del bit de paridad que vimos en el ejemplo al principio del capitulo. Consideramos mensajes binarios de 11 bits, que codificaremos como un mensaje-código de 16 bits. Es decir, que la matriz generatriz será 11×16. Sin embargo, los códigos de Hamming los podemos interpretar de una forma algo más intuitiva. Supongamos un mensaje $m \in \mathbb{F}_2^{11},\ m = (m_1, \ldots, m_{11}) = (1,1,1,0,1,0,0,0,1,1,1)$. El mensaje codificado tendrá 16 bits, escribamos el mensaje en una tabla de tamaño 4×4 del siguiente modo:

p	p_1	p_2	$m_1 = 1$
p_3	$m_2 = 1$	$m_3 = 1$	$m_4 = 0$
p_4	$m_5 = 1$	$m_6 = 0$	$m_7 = 0$
$m_8 = 0$	$m_9 = 1$	$m_{10} = 1$	$m_{11} = 1$

Usamos las casillas sombreadas en azul a modo de bits de paridad, pero en vez de hacerlo sobre todo el mensaje, lo haremos sobre partes de la tabla de forma que podamos encontrar la posición del bit en el cual se ha producido el error.

- El primer bit de paridad p_1 es el bit de paridad de la **segunda y cuarta columna** $I = \{1,2,4,5,7,9,11\}$. $p_1 = \overline{\sum_{i \in I} m_i}\ (mod\ 2) = 1$.
- El segundo bit de paridad p_2 es el bit de paridad de la mitad izquierda de la tabla, o de de la **tercera y cuarta columna**. $I = \{1,3,4,6,7,10,11\}$ $p_2 = \overline{\sum_{i \in I} m_i}\ (mod\ 2) = 0$.
- El tercer bit de paridad p_3 es el bit de paridad de la **segunda y cuarta fila** $I = \{2,3,4,8,9,10,11\}$. $p_1 = \overline{\sum_{i \in I} m_i}\ (mod\ 2) = 1$.

- El cuarto bit de paridad p_4 es el bit de paridad de la mitad inferior de la tabla, o de de la **tercera y cuarta fila**. $I = \{5, 6, 7, 8, 9, 10, 11\}$ $p_2 = \overline{\sum_{i \in I} m_i}\ (mod\ 2) = 0$.
- El bit p es un bit de paridad para toda la tabla, $p = \overline{\sum_{i=1}^{11} m_i} = 1$.

De esta forma, si se produce un error, podremos detectarlo; pues el receptor computará los valores de $p, p_1, \ldots, p_5$ y observará que hay alguna discrepancia respecto a los valores del mensaje, **c**, recibido.

El mensaje codificado de la forma que acabamos de indicar se puede escribir como la secuencia:

$$c = (p, p_1, p_2, m_1, p_3, m_2, m_3, m_4, p_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}).$$

Supongamos que esta secuencia es mandada a través de un canal con ruido y el receptor recibe la secuencia $c = (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$. Dado que $p = 1 \neq \overline{\sum_{i=2} c_i}\ (mod\ 2) = 0$.

Supongamos para este ejemplo que no hay más de un error (aunque este tipo de código puede detectar hasta dos errores y corregir un error). El receptor colocar el mensaje en una tabla y realizara las comprobaciones:

1	1	0	1
1	1	1	0
0	1	1	0
0	1	1	1

1	1	0	1
1	1	1	0
0	1	1	0
0	1	1	1

Cuadro 3.1: Computemos los primeros bits de paridad: $p_1 = 1 = 1$, por lo que no hay error en la segunda ni cuarta columna. Para el segundo, $p_2 = 1 \neq 0$, es decir, hay un error en la segunda mitad de la tabla. Deducimos que hay un error en la tercera columna.

1	1	0	1
1	1	1	0
0	1	1	0
0	1	1	1

1	1	0	1
1	1	1	0
0	1	1	0
0	1	1	1

Cuadro 3.2: Computando $p_3 = 0 \neq 1$ deducimos que hay un error en la segunda o la tercera fila. Computando $p_4 = 0 = 0$ deducimos que las dos últimas filas son correctas. Por tanto, el error se ha producido en la segunda fila.

Por todo esto, el receptor concluye que el error está en la segunda fila y en la tercera columna, es decir, hay un error en m_3. El emisor realiza la corrección y recupera el código original. Resaltemos además que el código también detecta errores que se produzcan en los

bits de paridad (aunque los que nos interesa proteger son los bits del mensaje).

Código de Hamming como código lineal:

Los códigos de Hamming son de hecho, un tipo de código lineal. Podemos escribir lo que hemos explicado de forma intuitiva anteriormente usando la notación y conceptos que hemos descrito previamente.

Partiendo del mismo mensaje original $m \in \mathbb{F}_2^{11},\ m = (m_1, \ldots, m_{11}) = (1,1,1,0,1,0,0,0,1,1,1)$, consideremos la codificación $c = (m_1, \ldots, m_1, p_1, p_2, p_3, p_4, p) \in \mathbb{F}_2^{16}$, donde p y p_1, p_2, p_3, p_4 son los bits de paridad definidos en el apartado anterior del ejemplo. Hemos reordenado los bits por comodidad.

Vemos que para un código de Hamming (aunque es cierto para cualquier código lineal), cualquier permutación o reordenación de los bits del mensaje codificado no altera significativamente la tarea del receptor. Solo necesita saber que bits corresponden al mensaje y cuales son bits de paridad. De hecho, la coordenada j-ésima depende únicamente de la columna j-ésima de la matriz generatriz: $c_j = \sum_{i=1}^{k} H_{i,j} m_i$. Consideramos por tanto la siguiente definición:

Definición 3.7.12: Diremos que dos códigos lineales $\mathcal{C}$ y $\mathcal{C}'$ son equivalente si la matriz generatriz de uno de ellos se puede obtener como resultado de una permutación σ de las columnas de la matriz generatriz del otro.

Volviendo al ejemplo anterior, consideremos la matriz C:

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

Al multiplicar un mensaje por esta matriz obtendremos los bits de paridad:

$$m \times C = (p_1, p_2, p_3, p_4, p)\ (mod\ 2)$$

La matriz generatriz de código es $G = (Id_{11}, C)$, y es de tipo $[16, 11]$. La matriz C no es más que la expresión en forma matricial de las definiciones que hemos dado en el apartado anterior.

Código de Hamming como código de evaluación:

Finalmente, podemos verlo como un código de evaluación. El código de Hamming anterior es el código extendido (con el bit de paridad, p, de los otros 15 bits). Consideremos el código de Hamming normal, es decir, aquel cuya matriz generatriz es la matriz 11×15 que resulta de eliminar la última columna de la matriz $G = (Id_{11}, C)$ del código extendido (indicada en el apartado anterior del ejemplo). Formalmente, los códigos de Hamming se definen de la siguiente manera:

Definición 3.7.13: Los códigos de Hamming binarios de redundancia $r = n - k$, $\mathcal{H}(r)$, desde el punto de vista de los códigos lineales, se definen el único código cuya matriz de control tiene por columnas los vectores no nulos de $\mathcal{F}_2^r$ (único salvo equivalencia, es decir, permutación de columnas de la matriz generatriz).

La matriz de control H, del código,es una matriz 4×15. Las columnas de H son todos los elementos de $\mathbb{F}_2^4 \setminus \{0\}$; pues tiene 15 columnas y $|\mathbb{F}_2^4 \setminus \{0\}| = 2^4 - 1 = 15$, no pueden repetirse ninguna, de lo contrario podríamos coger un conjunto de dos columnas linealmente dependientes (las dos columnas repetidas).

Consideremos $\mathcal{X} = \mathbb{F}_2^4$ y $\mathcal{P} = \mathbb{F}_2^4 \setminus \{0\} \subseteq \mathcal{X}$.

$$\mathcal{P} = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,0,0), (1,0,1,0), (1,0,0,1),$$
$$(0,1,1,0), (0,1,0,1), (0,0,1,1), (1,1,1,0), (1,1,0,1), (1,0,1,1), (0,1,1,1), (1,1,1,1)\}.$$

Sea $V = \{\text{polinomios de } \mathbb{F}_2[X_1, X_2, X_3, X_4] \text{ con grado } 1\}$. Si consideramos:

$$ev_{\mathcal{P}} : V \longrightarrow \mathbb{F}_2^{15}.$$

Por ejemplo, $f = X_1 + X_4 \in V$ y $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_{15})) = (1,0,0,1,1,1,0,0,1,1,1,0,0,1,0)$ Sea $\overline{\mathcal{C}} = \{ev_{\mathcal{P}}(f) \mid f \in V\} = \{ev_{\mathcal{P}}(a_1X_1 + a_2X_2 + a_3X_3 + a_4X_4) \mid (a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4\}$. Evaluando sobre una base de V, ($\mathcal{B} = \{X_1, X_2, X_3, X_4\}$) obtenemos la matriz generatriz:

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

Por tanto obtenemos así un código de evaluación $\tilde{\mathcal{C}}$, que tiene matriz generatriz H'. Este es un código de longitud 15 y dimensión 4; es un código $[15, 4]$ y de hecho, veremos que es el

código dual u ortogonal a $\mathcal{C}$, el código de Hamming de los apartados anteriores (o equivalente a uno que lo es)

Las columnas de H' son todos los elementos de $\mathbb{F}_2^4 \setminus \{\mathbf{0}\}$ y por tanto H' es la única matriz 4×15 (salvo permutaciones de columnas) que es matriz de control del código de Hamming $\mathcal{H}(4)$.

Para convencernos que el código que hemos obtenido así es el mismo (o equivalente) al código de los apartados anteriores, consideremos el siguiente razonamiento:

Si C' es la matriz C del apartado anterior pero eliminando la última columna, vemos que C contiene todos los elementos de $\mathbb{F}_2^4 \setminus \{(0,0,0,0),(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$ y ya sabemos que las columnas de H' contiene todos los elementos de $\mathbf{F}_2^4 \setminus \{\mathbf{0}\}$. Por tanto podemos reordenar las columnas de H' para que: $H = ((C')^t \mid Id_4) \in \mathcal{M}_{4\times15}(\mathbb{F}_2)$. Obtenemos así un código equivalente a $\tilde{\mathcal{C}}$, con matriz generatriz H. Ahora hagamos el producto por bloque de las matrices:

$$GH^t = (Id_{11} \mid C') \times \left(\frac{C'}{Id_4}\right) = Id_{11}C' \ + C'Id_4 = C' + C' \ = \ 0 \ (mod\ 2)$$

Por tanto, H es, tras reordenar columnas, la matriz de control del código $\mathcal{C}$ que hemos visto antes.

3.8. Pesos de Hamming Generalizados y "Wire-Tap Channel II"

La noción de peso de Hamming se puede generalizar [12]. Así como los pesos de Hamming son importantes en el contexto de códigos correctores, los pesos generalizados lo son para el problema de "wiretap channel II" en criptografía.

Definición 3.8.14: El **peso de Hamming generalizado** r-ésimo, del código lineal $\mathcal{C}$, se define como:

$$d_r(\mathcal{C}) = min\{|sop(D)| \ \big| \ \mathcal{D} \text{ es un subcódigo lineal de } \mathcal{C}, dim(\mathcal{D}) = r\}$$

Donde $sop(D)$ es el soporte del código, es decir, $sop(\mathcal{D}) = \{i \mid c_i = 0, \text{ para cierto } (c_1, \cdots, c_k) = \mathbf{c} \in \mathcal{D}\}$.

Notamos que, para $r = 1$, el peso de Hamming generalizado coincide con la distancia mínima del código (definición 3.14). Efectivamente, para $r = 1$, $d_1 = min\{sop(\mathcal{D}) \mid dim(\mathcal{D}) = 1, \ \mathcal{D} \text{ subcódigo de } \mathcal{C}\}$. Cómo $dim(\mathcal{D}) = 1$, existe un cierto $\mathbf{c} \in \mathcal{C}$ tal que $\mathcal{D} = \langle \mathbf{c} \rangle$. Por tanto,

$$sop(D) = \{i \mid c'_i \neq 0, \ (c'_1, \ldots, c'_k) = \mathbf{c}' \in \langle \mathbf{c} \rangle\} = \{i \mid c_i \neq 0, \ (c_1, \ldots, c_k) = \mathbf{c}\} = sop(\mathbf{c}).$$

Puesto que $w(\mathbf{c}) = |sop(\mathbf{c})|$, tenemos que, $d_1 = min\{w(\mathbf{c})|\mathbf{c} \in \mathcal{C}\}$, es decir, el peso mínimo del código (que coincide con la distancia mínima).

Proposición 3.8.10 (monotonía): Sea $\mathcal{C}$ un código lineal de tipo $[n, k]$, con $k > 0$. Entonces, tenemos que:

$$1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n$$

Demostración: Por definición, $d_r(\mathcal{C}) = min\{|sop(D)| \mid \mathcal{D}$ es un subcódigo lineal de $\mathcal{C}, dim(\mathcal{D}) = r\}$, luego siempre tenemos que $d_{r-1}(\mathcal{C}) \leq d_r(\mathcal{C})$. Veamos que la desigualdad es estricta.
Sea $\mathcal{D}$ un código lineal tal que $d_r(\mathcal{C}) = |sop(\mathcal{D})|$, y en consecuencia, $dim(\mathcal{D}) = r$. Sea $i \in sop(\mathcal{D})$. Si definimos $\mathcal{D}_i := \{\mathbf{x} \in \mathcal{D} \mid x_i = 0\}$, entonces, $dim(\mathcal{D}_i) = r - 1$. Luego $d_r(\mathcal{C}) \leq |sop(\mathcal{D}_i)| \leq |sop(\mathcal{D}_i)| - 1 \leq d_r(\mathcal{C}) - 1$.

□

Podemos, dar un resultado que generaliza el que vimos en el corolario 3.2.6. Sea H, una matriz de control de un código lineal $\mathcal{C}$, de tipo $[n, k]$, y denotemos las columnas de dicha matriz por los vectores $\mathbf{h}_i \in \mathbb{F}_q^{n-k}$.

Proposición 3.8.11: Sea $\mathcal{C}$ un código lineal, con matriz de control H. Entonces, tenemos que:

$$d_r(\mathcal{C}) = min\big\{|I| \;\big|\; I \subseteq \{1, 2, \ldots, n\},\ r \leq |I| - dim(\langle \mathbf{h}_i \;\big|\; i \in I\rangle)\big\}$$

Demostración: Primero, consideremos, para $I \subseteq \{1, 2, \ldots, n\}$:

$$S(I) := \langle \mathbf{h}_i \mid i \in I\rangle$$
$$S^{\perp}(I) := \{\mathbf{x} \in \mathcal{C} \mid x_i = 0 \text{ para } i \notin I,\ \sum_{i \in I} x_i \mathbf{h}_i = \mathbf{0}\}$$

Por como está definido $S^{\perp}(I)$, tenemos que,

$$dim(S^{\perp}(I)) + dim(S(I)) = |I|.$$

Efectivamente, si $\ell = |I| - dim(S(I))$, entonces hay ℓ vectores del conjunto $\{\mathbf{h}_i\}_{i \in I}$ linealmente dependientes; y por tanto, existen ℓ vectores de coeficientes, $\mathbf{x}_j = (x_{1j}, \ldots, x_{|I|j})$, $j \in \{1, 2, \ldots, \ell\}$, tales que $\sum_{ij \in I} x_i \mathbf{h}_i = \mathbf{0}$. Estas sumas, o combinaciones lineales, son linealmente independientes y, por tanto, también lo son los vectores $\mathbf{x}_j$. En consecuencia, $S^{\perp}(I)$ tiene dimensión ℓ.

Denominemos $d := min\big\{|I| \;\big|\; I \subseteq \{1, 2, \ldots, n\},\ r \leq |I| - dim(\langle \mathbf{h}_i \;\big|\; i \in I\rangle)\big\}$ (la parte derecha de la igualdad), demostremos que $d_r(\mathcal{C}) \leq d$. Sea $I \subseteq \{1, 2, \ldots, n\}$ tal que $|I| - dim(S(I)) = r$ e $|I| = d$. Entonces, por la afirmación inicial, $dim(S^{\perp}(I)) = r$. Como subespacio

vecotrial de $\mathbb{F}_q^n$, $S^{\perp}(I)$ es un subcódigo de $\mathcal{C}$, y podemos aplicar la definición de $d_r(\mathcal{C})$ (definición 3.8.14), y obtenemos que:

$$d_r(\mathcal{C}) \leq |sop(S^{\perp}(I))| = |I| = d.$$

Vemos que se da la igualdad $|sop(S^{\perp}(I))| = |I|$. Para el caso, $|I| = dim(S(I))$, por definición $S^{\perp}(I) = \{\mathbf{0}\} \Rightarrow |sop(S^{\perp}(I))| = 0$. Recíprocamente, si $0 = |sop(S^{\perp}(I))|$, $S^{\perp}(I) = \{\mathbf{0}\} \Rightarrow |I| = dim(S(I))$. En el resto de los caso, tenemos que, por un lado $\forall \mathbf{x} \in S^{\perp}(I),\ x_i = 0\ \forall i \notin I$, entonces $|sop(S^{\perp}(I))| \leq |I|$. Por otro lado, como $|dim(S(I))| < |I|$, para cada $j \in I$, $\mathbf{h}_j$ existe una combinación lineal no trivial, $\mathbf{h}_j = \sum_{i \in I \setminus \{j\}} x_i \mathbf{h}_i$, donde $\forall i \notin I, x_i = 0$. Luego $(-x_1, -x_2, \ldots, 1_{(j)}, \ldots, -x_n) \in S^{\perp}(I)$ y no puede ser que $\forall \mathbf{x} \in S^{\perp}(I),\ x_j = 0$. Por tanto, $|I| \leq |sop(S^{\perp}(I))|$

Para la otra desigualdad, consideremos $\mathcal{D}$, un subcódigo de $\mathcal{C}$ en el cual se alcanza el mínimo de la definición de $d_r(\mathcal{C})$, es decir, $dim(\mathcal{D}) = r$ y $|sop(\mathcal{D})| = d_r(\mathcal{C})$. Denotemos $I = sop(\mathcal{D})$, entonces por definición de soporte, tenemos que, $\forall \mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{D}$, $c_i = 0\ \forall i \notin I$. Así mismo, aplicando la definición de matriz de control, $\forall \mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{D} \subseteq \mathcal{C}$ se verifica que $H\mathbf{c}^T = \mathbf{0}$ y entonces, $\sum_{i \in I} c_i \mathbf{h}_i = \mathbf{0}$. Por tanto, $\mathcal{D} \subseteq S^{\perp}(I) \Rightarrow |dim(\mathcal{D})| \leq dim(S^{\perp}(I))$.
Pero por hipótesis, $r = dim(\mathcal{D})$ y, aplicando la afirmación inicial, $dim(S(I)) = |I| - dim(S^{\perp}(I)) \leq |I| - r$, luego $|I| - dim(S(I)) \geq r$.

Si suponemos que la desigualdad es estricta, $dim(S^{\perp}(I)) = |I| - dim(S(I)) = r' > r$, entonces, $\mathcal{D} \neq S^{\perp}(I)$, y aplicando la definición de peso de Hamming generalizado, $d_{r'}(\mathcal{C}) \leq |sop(S^{\perp}(I))| = |I|$. Usando hipótesis inicial, $sop(\mathcal{D}) = I \Rightarrow |I| = |sop(\mathcal{D})| = d_r(\mathcal{C})$, y tenemos que $d_{r'}(\mathcal{C}) \leq d_r(\mathcal{C})$, con $r < r'$, lo que contradice la proposición anterior (3.8.10), llegando así a una contradicción. Por tanto, $|I| - dim(S(I)) = r$. Con esto, y la definición de d, $d \leq |I| - dim(S(I)) = r \leq d_r(\mathcal{C})$ (la última desigualdad, dada por la proposición anterior, 3.8.10).

□

Calcular la distancia mínima de un código corrector es un problema computacionalmente intenso, y más aún es calcular los pesos de Hamming generalizados. Continuaremos con este tema en el capítulo 5, donde usaremos la distancia de Feng-Rao para dar una cota inferior para $d_r(\mathcal{C})$.

El problema de "Wire-Tap Channel II ":

Como hemos dicho, una de las principales aplicaciones de los pesos de Hamming generalizados es en el problema de "Wire-Tap Channel II". Este es un problema de criptografía, que planteamos de forma similar a como hemos planteado la comunicación en el contexto de

los códigos correctores. Un mensaje, representado por el vector $\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$ es codificado como $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, $n \geq k$. El mensaje es mandado por el emisor, a través de un canal (con o sin ruido), al que un tercer actor tiene acceso. El espía, puede leer $\mu < n$ coordenadas del vector codificado, las que elija. Asumiendo que el receptor (y presumiblemente, el espía) pueden reconstruir el mensaje original a partir de $\mathbf{c}$, se quiere que con μ posiciones del mensaje (bits), esto no sea posible.

Es decir, codificar el mensaje de tal forma que se cause al espía el mayor grado posible de incertidumbre, sin usar un cripto-sistema (y, por tanto, sin usar una clave). Es posible usar códigos correctores para resolver este problema.

Además, tenemos, en lema 6 de [1], se demuestra que:

Proposición 3.8.12: Si denotamos por Δ_μ a la información que puede obtener el espía (las posiciones del mensaje original que deduce), tenemos que:

$$\Delta_\mu = min_{|I|=n-\mu} \left(dim\{ \langle \mathbf{h}_i \mid i \in I \subseteq \{1, 2, \ldots, n\} \rangle \} \right)$$

Con esto podemos dar el siguiente resultado:

Teorema 3.8.13: Sea $\mathcal{C}$ el código con matriz de control H. Denotemos, para cierto μ, $\Delta = \Delta_\mu$. Entonces, tenemos la siguientes cotas:

$$d_{n-\mu-\Delta}(\mathcal{C}) \leq n - \mu < d_{n-\mu-\Delta+1}(\mathcal{C})$$

Demostración: Existe I tal que $|I| = n - \mu$ y $\Delta = dim(\langle H_i \mid i \in I \rangle)$. Por la proposición 3.8.11, tenemos que $d_{n-\mu-\Delta}(\mathcal{C}) \geq |I| = n - \mu$.

Para la otra desigualdad, supongamos que $n - \mu \geq d_{n-\mu+\Delta+1}(\mathcal{C})$. Por la proposición 3.8.11, existe I, con $|I| = d_{n-\mu-\Delta+1}(\mathcal{C}) = n - \mu - \epsilon$, para $\epsilon \geq 0$, y con $dim(\langle \mathbf{h}_i \mid i \in I \rangle) = |I| - (n - \mu - \Delta + 1) = \Delta - \epsilon - 1 \leq \Delta - 1$. Por tanto, $\Delta_\mu \leq \Delta_{\mu+\epsilon} \leq \Delta_\mu - 1$, que es una contradicción.

□

Es decir, que para un cierto n, podemos elegir un Δ (nivel de información a la cual es espía tendrá acceso), y obtener una cota inferior y superior para μ (máximo número de "bits" que el espía puede conocer del mensaje codificado).

Por supuesto, esta cota requiere poder calcular los pesos de Hamming generalizados. Esto puede hacerse (aunque sea costoso), pero en el capítulo 5, veremos dos cotas para los pesos de Hamming generalizados, usando distancias de Feng-Rao.

Capítulo 4

Introducción a códigos AG

Los códigos algebraico-geométricos pertenecen a una familia más amplia de códigos, los códigos de evaluación, vistos al final del capitulo anterior. Además necesitaremos algunas nociones de geometría proyectiva y algebraica.

4.1. Curvas algebraicas

El objetivo de esta sección es introducir los conceptos necesarios sobre curvas algebraicas para poder trabajar con los códigos AG. Si bien daremos las nociones esenciales, no pretende ser un estudio auto-contenido de la materia. La materia que se cubre en esta sección es contenido de las asignaturas del grado; *Álgebra 2, Álgebra Conmutativa y Geometría Algebraica.*

En esta sección trabajaremos sobre K, que será la clausura algebraica de un cuerpo finito. Denotamos $\mathbb{P}^n(K)$ al espacio proyectivo n-dimensional (esencialmente trabajaremos sobre el plano proyectivo, $n = 2$). Recordemos que un punto del espacio proyectivo P es la clase de equivalencia formada por todos los puntos afines, $\mathbf{x},\ \mathbf{y} \in K^{n+1} \setminus \{\mathbf{0}\}$, que satisfacen $\mathbf{x} = \lambda\mathbf{y},\ \lambda \in K \setminus \{0\}$; decimos que $\mathbf{x}$ e $\mathbf{y}$ son equivalentes ($\mathbf{x} \sim \mathbf{y}$, y esta relación es de equivalencia). Dado $\mathbf{x} = (x_0, x_1, \ldots, x_n) \neq \mathbf{0}$, pertenece a la clase de equivalencia P, formada por todos los puntos afines equivalentes a $\mathbf{x}$. Una expresión de P en **coordenadas homogéneas** es $P = (x_0 : x_1 : \ldots : x_n)$ (las coordenadas homogéneas de un punto del espacio proyectivo no son únicas, ya que pueden diferir en un factor escalar $\lambda \in K$).

4.1.1 Definición:

- Un polinomio $F \in K[X_0, X_1, \ldots, X_n]$ es **homogéneo** de grado l si cada uno de sus

monomios es de grado l. Es decir:

$$F = \sum_{i=0}^{m} a_i X_0^{e_{i0}} X_1^{e_{i1}} \dots X_n^{e_{in}}, \quad \forall i \in \{1, 2, \dots, m\},\ l = \sum_{j=0}^{n} e_{ij}$$

En consecuencia, $F(\lambda X_0, \lambda X_1, \dots, \lambda X_n) = \lambda^l F(X_0, X_1, \dots, X_n)$. Por tanto si $F(\mathbf{X}) = 0$, entonces $F(\lambda \mathbf{X}) = 0$. Notemos además que el producto de polinomios homogéneos es homogéneo (desarrollo binomial del producto).

- Diremos que un **ideal es homogéneo**, si está generado por polinomios homogéneos.
- Sea $F \in K[X, Y]$, un polinomio de grado l, la **homogeneización** de F se define como:

$$F^*(X, Y, Z) = Z^l F(\frac{X}{Z}, \frac{Y}{Z}) \in K[X, Y, Z]$$

Claramente, F^*, es un polinomio homogéneo de grado l.

Ejemplo 4.1.1: Consideremos la hipérbola $f = x^2 - y^2 - 1$, en $K[x, y]$. La homogeneización de f es: $F = X^2 - Y^2 - Z^2$, polinomio homogéneo de grado 2.

Para la siguiente definición, analizaremos lo que sucede cuando un polinomio se anula en un punto del espacio proyectivo. Notemos que, para que esto tenga sentido, debemos restringirnos a polinomios homogéneos, ya que un polinomio no homogéneo puede anularse en $\mathbf{x} \in K^{n+1}$, pero no en $\lambda \mathbf{x},\ \lambda \in K$ (por ejemplo, $f(x, y, z) = x^2 - y^2 - 1$, $f(1, 0, 0) = 0$, pero $f(3, 0, 0) = 8$). Al restringirnos a polinomios homogéneos, los polinomios se anulan en todos los miembros de la clase de equivalencia y, por tanto, tiene sentido decir que un polinomio se anula en un punto del plano proyectivo de coordenadas $(X_0 : X_1 : \dots : X_n) = P$.

A continuación definiremos variedades algebraicas y proyectivas. Para el uso de este texto, una variedad será el conjunto de ceros de un ideal primo. Recordemos que un ideal, $I \subsetneq R$, es un ideal primo del anillo R, si $fg \in I \Rightarrow (f \in I) \vee (g \in I)$. Los ideales primos tienen la propiedad de que su conjunto de ceros no puede ser escrito como la unión propia de dos o más conjuntos de ceros de otros ideales. En este sentido, diremos que la curva o la variedad es irreducible.

Definición 4.1.2: Dado un ideal homogéneo I del anillo de polinomios $R := K[X_0,\ X_1, \dots,\ X_n]$ entonces:

- El **conjunto de ceros** del ideal I se define como:

$$V(I) = \{P = (x_0 : x_1 : \dots : x_n) \in \mathbb{P}^n \mid F(P) = 0,\ \forall F \in I\} \subseteq \mathbb{P}^n$$

- Dado I un ideal primo homogéneo de $K[X_0,\ X_1,\ \dots,\ X_n]$, el conjunto de ceros $V(I) \subseteq \mathbb{P}^n$ lo llamaremos **variedad proyectiva** y lo denotaremos por $\mathcal{X}_I$ o simplemente $\mathcal{X}$.

- Dado $F \in K[X_0,\ X_1, \ldots,\ X_n]$, un polinomio irreducible, denotaremos por $\mathcal{X}_F$ a la variedad proyectiva dada por $V(\langle F\rangle)$, donde $\langle F\rangle$ es el ideal generado por F. Como el polinomio es irreducible, el ideal que genera es primo.

Ejemplo 4.1.2: Para el caso de la hipérbola que hemos mencionado antes. Partimos un polinomio en dos variables que define la hipérbola $f(x,y) = x^2 - y^2 - 1$ si lo homogeneizamos en $\mathbb{P}^2(\mathbb{F}_2)$ obtenemos $F(X,Y,Z) = X^2 - Y^2 - Z^2 = X^2 + Y^2 + Z^2 \ \ (mod\ 2)$. Entonces $\mathcal{X}_F = V(\langle F\rangle) = \{(1,1,0),\ (1,0,1),\ (0,1,1)\}$

Definición 4.1.3:

- Sea el polinomio $F = \sum a_{i_0 i_1 \ldots i_n} X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n} \ \in K[X_0, X_1, \ldots, X_n]$. Entonces F_{X_j}, la **derivada parcial** de F respecto de X_j $(0 \leq j \leq n)$ es definida como:

$$F_{X_j} = \sum i_j a_{i_0 i_1 \ldots i_n} X_0^{i_0} \cdots X_{j-1}^{i_{j-1}} X_j^{i_j - 1} X_{j+}^{i_{j+1}} \cdots X_n^{i_n}$$

- Sea $\mathcal{X}$ una variedad en $\mathbb{P}^n$. Dado $P = (a_0 : a_1 : \ldots : a_n)$ un punto en la variedad, diremos que es **no singular** o **regular**, si al menos una de las derivadas, F_{X_0}, F_{X_1}, ..., F_{X_n}, es distinta de cero en P. De lo contrario, diremos que P es un punto singular.

- Diremos que una variedad $\mathcal{X}$ es **no singular**, **regular**, **lisa** o **suave** (del inglés, *smooth*); si todos sus puntos son no singulares.

- Si $P = (x_0 : x_1 : \ldots : x_n)$ es un punto no singular de la variedad, definimos el operador d_P actuando sobre el polinomio F como:

$$d_P(F) = \sum_{i=0}^{n} (F_{X_i}(P)(X_i - x_i))$$

  El **espacio tangente** a la variedad $\mathcal{X}$, definida por $F = 0$, es la variedad definida por la ecuación $d_P(F) = 0$

Ejemplo 4.1.3: Si consideramos la hipérbola de ecuación $F = X^2 - Y^2 - Z^2$, en $\mathbb{P}^2(\mathbb{F}_q)$ $(q > 10,\ char(\mathbb{F}_q) > 10)$, vemos que $P = (5,3,4)$ es no singular, pues:

$$F_X(P) = 2X(P) = 10,\ F_Y(P) = -2Y(P) = 6,\ F_Z(P) = -2Z(P) = 8.$$

Su recta tangente en P viene dada por la ecuación $10(X-5) - 6(Y-3) - 8(Z-4) = 0$

Vamos a definir a continuación el concepto de función racional sobre una variedad proyectiva. Las funciones racionales son funciones definidas en puntos de la variedad, que son puntos del plano, por tanto la definición debe tener en cuenta las peculiaridades del espacio proyectivo para que tenga sentido.

Si $\mathcal{X}_F$ es la variedad proyectiva generada por el polinomio irreducible F. Consideremos el dominio de integridad $R = K[X_0,\ X_1, \ldots,\ X_n]/(\langle F\rangle)$ y su cuerpo de fracciones Q_F. Al evaluar fracción $\frac{G}{H} \in Q_F$ en un punto proyectivo, es deseable que el resultado no dependa del representante del punto. Para ello requerimos que G y H sean polinomios homogéneos y sean ambos del mismo grado. De este modo, si $deg(G) = deg(H) = d$, y ambos son homogéneos: $\frac{G}{H}(\lambda P) = \frac{G}{H}((\lambda \mathbf{X_0} : \lambda \mathbf{X_1} : \ldots : \lambda \mathbf{X_n})) = \frac{\lambda^d G}{\lambda^d H}(X_0 : X_1 : \ldots : X_n) = \frac{G}{H}(P)$. El **cuerpo de funciones** de $\mathcal{X}_F$ será el conjunto de elementos de Q_F que cumpla las propiedades anteriores. Formalmente:

Definición 4.1.4: Sea $\mathcal{X}_F$ una variedad proyectiva en $\mathbb{P}^n$ definida por el ideal primo y homogéneo $I = \langle F\rangle$, donde F es un polinomio irreducible en $K[X_0,\ X_1, \ldots,\ X_n]$ definimos el **cuerpo de funciones** de $\mathcal{X}_F$ como:

$$K(\mathcal{X}_F) := \left\{ \frac{G}{H} \;\middle|\; (\frac{G}{H} \in Q_F) \ \wedge\ (G \text{ y } H \text{ son homogéneos}) \ \wedge\ (deg(G) = deg(H)) \wedge\ (G \neq 0) \right\}$$

Es sencillo ver que se trata de un cuerpo, heredando las operaciones y la estructura de Q_F además de comprobando que sus propiedades se preservan por producto y suma y que si una fracción pertenece también lo hace su inverso.

Si $f \in K(\mathcal{X}_F)$, diremos que es una **función racional** en la variedad.
Además, si una función racional con representación $f = \frac{G}{H}$ verifica que $H(P) \neq 0$, diremos que es **regular en** P y $f(P) = G(P)/H(P)$. El **anillo de** todas las **funciones regulares en** P se denota por $\mathcal{O}_P$.

Notemos que si tenemos una variedad afín definida por el ideal primo I, $\mathcal{X} = V(I) = \{\mathbf{x} \in \mathbb{A}^n \mid F(\mathbf{x}) = 0,\ \forall F \in I\}$. Entonces, si denotamos por I^* al ideal generado por $\{F^* | F \in I\}$ (donde F^* es la homogeneización de F), entonces I^* es un ideal primo homogéneo que define una variedad proyectiva $\mathcal{X}^*$ en $\mathbb{P}^n$. Si denotamos por $\mathcal{X}_0^* = \{(x_0 : x_1 : \ldots : x_n) \in \mathcal{X}^* \mid x_0 \neq 0\}$, entonces, vemos que la aplicación $(x_1, \ldots, x_n) \to (1 : x_1 : \ldots : x_n)$ define un isomorfismo entre $\mathcal{X}$ y $\mathcal{X}_0^*$. A los puntos de $\mathcal{X}^*$ con $x_0 = 0$ los llamamos **puntos del infinito** de la variedad. Además los cuerpos de funciones $K(\mathcal{X}^*)$ y $K(\mathcal{X})$ son isomorfos, pues podemos considerar la aplicación

$$\frac{f}{g} \longrightarrow \frac{x_0^{(deg(g)-deg(f))} f^*}{g^*}$$

Teorema 4.1.1: Sea P un punto de la curva proyectiva $\mathcal{X}_F$:

- El anillo $\mathcal{O}_P$, es un anillo de local, cuyo ideal maximal es $\mathcal{M}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}$, que es además un ideal principal. Es decir, existe $t \in \mathcal{M}_P$ tal que $\mathcal{M}_P = \langle t\rangle$.

- Existe $t \in \mathcal{O}_P$ tal que $\forall f \in K(\mathcal{X}_F) \setminus \{0\}$ existe un único entero, $v_P(f)$ de modo que:

$$f = t^{v_P(f)}u$$

Donde $u \in \mathcal{O}_P$, $u(P) \neq 0$. El valor de $v_P(f)$ depende únicamente de $\mathcal{X}_F$ y P. Decimos que t es un **parámetro local**.

Demostración:

- Ver que el ideal $\mathcal{M}_P$ es un ideal maximal, es sencillo, pues $K' = \mathcal{O}_P/\mathcal{M}_P$ es un cuerpo. Dado $G/H \in K' \setminus \{0\}$, $\frac{G}{H} \neq 0$ y $G(P) \neq 0, H(P) \neq 0$, por lo que $\frac{H}{G} \in K'$ está bien definido, y $\frac{G}{H}\frac{H}{G} = 1$, y todo elemento es invertible. Dados $\frac{G}{H}$, $\frac{G'}{H'}$, $\frac{G}{H}\frac{G'}{H'} = \frac{GG'}{HH'} \in K'$. Luego el ideal es maximal. Como $\mathcal{M}_P$ es el conjunto de elementos no invertibles del anillo, $\mathcal{O}_P$ se trata de un anillo local.

  Ahora vemos que $\mathcal{M}_P$ es un ideal principal, es decir, generado por un único elemento. Supongamos, sin pérdida de generalidad, que $P = (A : B : C) \mid C \neq 0$. Transformamos el problema en uno afín, y que la definición de $\mathcal{O}_P$, formado por polinomios nos permite reducir la demostración al caso afín pues, como hemos visto antes, $K(V(\langle F* \rangle))$ y $K(V(\langle F \rangle))$ son cuerpos isomorfos (en este caso partimos del polinomio homogéneo). Consideremos $\mathbf{X}_f$ la curva afín generada por la ecuación $f(x, y) = 0$, donde $f(x, y) = F(x = X/Z, y = Y/Z, 1 = Z/Z)$ (la des-homogeneización de F, por la carta afín φ_z^{-1}). Sea $P' = \varphi_z^{-1}(P) = (a = A/C, b = B/C)$ un punto en la curva. El ideal maximal, $\mathcal{M}_P$, está generado por $(x - a)$ e $(y - b)$. Consideremos la tangente en P:

$$F_X(P)(x - a) + F_Y(P)(y - b) \equiv 0 \pmod{\mathcal{M}_P^2}$$

  Es decir, que $(x - a)$, $(x - b)$ no son linealmente independientes en el espacio vectorial $\mathcal{M}_P/\mathcal{M}_P^2$, por tanto este espacio tiene dimensión 1, y tiene un generador. Como consecuencia del lema de Nakayama [6], [8], esto significa que $\mathcal{M}_p$ también está generado por un único generador. Además, el lema de Nakayama nos dice que si $\overline{g}$ genera $\mathcal{M}_P/\mathcal{M}_P^2$, entonces g genera $\mathcal{M}_P$. A efectos prácticos, esto significa que, podemos obtener un parámetro local simplemente encontrando g tal que, $K \ni c \neq g \pmod{\mathcal{M}_P^2}$.

- Usando la primera parte, existe t, tal que, $\mathcal{M}_P = \langle t \rangle$, luego podemos escribir cualquier elemento $f \in \mathcal{O}_P$ como una potencia de t multiplicado por un elemento invertible, u; $f = ut^s$. En este caso, denotaremos $v_P(f) := s$. El valor depende de la curva y del punto.

□

Definición 4.1.5:

- Si $v_P(f) = m > 0$, diremos que f tiene un cero de orden m en P.

- Extendemos la función v_P a todo $K(\mathcal{X})$, definiendo $v_P(f/g) = v_P(f) - v_P(g)$
- Diremos que f presente un polo de orden m en P, si $v_P(f) = -m < 0$

Ejemplo 4.1.4: Consideremos $\mathbb{P}^1$, la línea proyectiva sobre $\mathbb{F}_q$. Sea $P = (1 : 0)$, entonces, y/x es un parámetro local. Dado $f = \frac{y^2}{x^2+1} \in \mathcal{O}_P$, tenemos que $f = (\frac{y}{x})^2 \frac{x^2}{x^2+1}$, donde $\frac{x^2}{x^2+1}$ es invertible. Por tanto, $v_P(f) = 2$.

Si tomamos $g = \frac{x^2-y^2}{y^2} = \frac{s}{t}$, $s = (\frac{y}{x})^0(x^2 - y^2) \Rightarrow v_P(s) = 0$ y $t = (\frac{y}{x})^2(x^2) \Rightarrow v_P(t) = 2$. Por tanto, $v_P(g) = -2$ y g tiene un polo de orden 2 en P.

Ejemplo 4.1.5 Sea K un cuerpo con característica distinta de 2. Sea $\mathcal{C}$ el circulo en $\mathbb{A}^2$ dado por la ecuación $X^2 + Y^2 = 1$, y sea $P = (1, 0)$. Consideramos la función $z = 1 - x$. Esta función es cero en P, luego está en el ideal $\mathcal{M}_P$. Veamos que tiene orden 2.

En este caso, vemos que y es un parámetro local, pues $d_{(1,0)}(F) = 2(X - 1)$, e y no es un múltiplo suyo, $\mathcal{M}_P = \langle y \rangle$, y en $\mathcal{X}$, $1 - x = y^2/(1 + x)$ (pues $1 - x = y^2/(1 + x) \Leftrightarrow (1 - x)(1 + x) = y^2 \Leftrightarrow x^2 - 1 = y^2$) y la función $1/(1 + x)$ es una unidad en $\mathcal{O}_P$

Definición 4.1.6: Sea una curva $\mathcal{X}$ definida por un con ecuaciones cuyos coeficientes pertenecen a $\mathbb{F}_q$. Llamaremos **puntos racionales** a aquellos puntos de la curva con coordenadas en $\mathbb{F}_q$.

El **grado** de una curva proyectiva es el número de puntos que hay en la intersección de la curva con un hiperplano que no contiene a la curva. En el caso de una curva en el plano proyectivo, son los puntos en la intersección de la curva con una recta proyectiva. Hay un resultado, conocido como el teorema de Bézout (que no demostraremos, pero que se puede encontrar en [16], que afirma que el grado de una curva proyectiva coincide con el grado de la ecuación que lo define.

Definición 4.1.7: Consideramos la intersección de una curva proyectiva $\mathcal{X}$, irreducible y no singular, con una hypersuperficie $\mathcal{Y}$ definida por la ecuación $G = 0$ y de grado m. Asumiremos que $\mathcal{X} \not\subset \mathcal{Y}$.

Sea P un punto de $\mathcal{X} \cap \mathcal{Y}$, Sea $H \in K[X, Y, Z]$ polinomio lineal homogéneo tal que $H(P) \neq 0$. Sea $h \in K[X, Y, Z]/(I)$ su clase de equivalencia modulo el ideal que define $\mathcal{X} = V(I)$ y g la de G. Entonces la **multiplicidad intersección** es $v_P(g/h^m)$ y la denotamos por $I(P; \mathcal{X}, \mathcal{Y})$.

Esta definición no depende de la elección de H, pues h/h' es una unidad en $\mathcal{O}_P$ para cualquier otro polinomio lineal homogéneo H' que no sea cero en P.

Enunciamos a continuación el teorema de Bézout:

Teorema 4.1.2 (de Bézout): Dada $\mathcal{X}$ una curva algebraica de grado ℓ e $\mathcal{Y}$, una hipersuperficie de grado m en $\mathbb{P}^n$, tal que, $\mathcal{X} \not\subset \mathcal{Y}$. Entonces, las variedades se cortan exactamente en ℓm puntos (contando multiplicidad). Es decir:

$$\ell m = \sum_{P \in \mathcal{X} \cap \mathcal{Y}} I(P; \mathcal{X}, \mathcal{Y})$$

De aquí en adelante, trabajaremos sobre el plano proyectivo $n = 2$, $\mathbb{P}^2(K)$, y diremos que una variedad sobre el plano es una curva. Además, $\mathcal{X}$, será siempre una curva proyectiva irreducible y suave. Si hablamos de la curva definida por un polinomio $\mathcal{X}_F$, asumiremos que F es irreducible.

4.2. Divisores

Los divisores son una pieza esencial para poder definir los códigos algebraico-geométricos.

Definición 4.2.8: Sea $\mathcal{X}$ una curva en $\mathbb{P}^2(K)$ suave e irreducible.

- Un **divisor** de una curva $\mathcal{X}$, es la suma formal $D = \sum_{P \in X}(n_P P)$, con $n_P \in \mathbb{Z}$ y $n_P = 0$ para todos salvo una cantidad finita de puntos P.
- El **soporte** del divisor es el conjunto de puntos P cuyo coeficiente n_P no es cero, y lo denotaremos por $sop(D)$.
- El **grado** del divisor es la suma $\sum n_P$.
- Si todos los coeficientes de un divisor son no negativos diremos que $D \succeq 0$.

Definición 4.2.9: Sean $\mathcal{X}$ e $\mathcal{Y}$ curvas proyectivas en $\mathbb{P}^2(K)$ definidas, respectivamente, por las ecuaciones $F = 0$ y $G = 0$, entonces la **división intersección** $\mathcal{X} \cdot \mathcal{Y}$ se define como:

$$\mathcal{X} \cdot \mathcal{Y} = \sum_{P \in \mathcal{X} \cap \mathcal{Y}} I(P; \mathcal{X}, \mathcal{Y}) P$$

donde $I(P; \mathcal{X}, \mathcal{Y})$ es la multiplicidad intersección (Def 4.1.7).

El teorema de Bézout, nos garantiza que $\mathcal{X} \cdot \mathcal{Y}$ sea un divisor; pues el numero puntos donde se cortan las curvas es finito. De hecho, afirma $\ell m = \sum_{P \in \mathcal{X} \cap \mathcal{Y}} I(P; \mathcal{X}, \mathcal{Y})$, que es el grado del divisor (donde ℓ es el grado de $\mathcal{X}$, y m el grado de $\mathcal{Y}$).

Definición 4.2.10: Si f es una función racional en $K(\mathcal{X})$, no idénticamente igual a 0, entonces definimos un **divisor** de f como:

$$(f) = \sum_{P \in \mathcal{X}} v_P(f)P$$

En cierto modo, un divisor de f nos dice donde están los ceros y los polos de f y cuales son sus órdenes y multiplicidad, ya que $v_P(f) \neq 0$ precisamente si $f(P) = 0$ o P es un polo de f. Las definiciones de grado, soporte y $\succeq$ son las mismas que para divisor de una curva

Teorema 4.2.3: El grado del divisor de una función racional, $f \in K(\mathcal{X})$ es cero.

Demostración: Sea $\mathcal{X}$ una curva proyectiva de grado l. Sea f una función racional en la curva $\mathcal{X}$. Entonces $f = A/B$, para ciertos polinomios homogéneos A, B del mismo grado ($deg(A) = deg(B) = m$) y con clases de equivalencia $a,\ b$. Sean $\mathcal{Y}$ y $\mathcal{Z}$ las hipersuperfices definidas por $A = 0$ y $B = 0$ respectivamente. Entonces, para un polinomio lineal homogéneo H, $H(P) \neq 0$ y con representante h, tenemos:

$$v_P(f) = v_P(\frac{a}{b}) = v_P(\frac{a/(h^m)}{b/(h^m)}) = v_P(a/(h^m)) - v_P(b/(h^m)) = I(P; \mathcal{X}, \mathcal{Y}) - I(P; \mathcal{X}, \mathcal{Z})$$

Por tanto $v_P(f) = I(P; \mathcal{X}, \mathcal{Y}) - I(P; \mathcal{X}, \mathcal{Z})$ y en consecuencia:

$$(f) = \sum_{P \in \mathcal{X}} v_P(f)P = \sum_{P \in \mathcal{X}} (I(P; \mathcal{X}, \mathcal{Y}) - I(P; \mathcal{X}, \mathcal{Z}))P = \mathcal{X} \cdot \mathcal{Y} \ - \ \mathcal{X} \cdot \mathcal{Z}.$$

Luego (f) es un divisor, y su grado es 0, pues tanto $\mathcal{X} \cdot \mathcal{Y}$ como $\mathcal{X} \cdot \mathcal{Z}$ son de grado lm,y entonces $deg((f)) = deg(\mathcal{X} \cdot \mathcal{Y}) - deg(\mathcal{X} \cdot \mathcal{Z}) = 0$

□

Ejemplo 4.2.6: Consideremos el círculo proyectivo $\mathcal{X} = V(Y^2 + Z^2 - X^2) \subset \mathbb{P}^2$ y sobre está curva, la función racional $f = Y/X - 1$. Deshomogeneizamos a $A = \varphi_X^{-1}(\mathbb{P}^2) \cong \mathbb{A}^2$, donde tenemos mandamos $X = 1$, $y = Y/X$, $z = Z/X$ y obtenemos $f|_A(y, z) = y - 1$. En este caso $P = (1, 0)$ correspondiente al punto proyectivo $(1 : 1 : 0)$ es un cero con multiplicidad 2, luego $v_{(1:1:0)}(f) = 2$. En el plano afín $y - z$, f no tiene polos, por lo que estos deben estar en en la recta $X = 0$, es decir, los puntos del círculo que son soluciones a la ecuación $Y^2 = Z^2$; es decir, los puntos de la circunferencia las bisectrices del primer y segundo cuadrante (del plano afín) $(0 : 1 : i)$ y $(0 : i : 1)$. Ambos son polos de orden 1, luego $v_{(0:1:i)}(f) = v_{(0:1:i)}(f) = -1$. Estos son todos los polos y ceros de f, luego no hay más puntos donde $v_P(f) \neq 0$. El divisor es:

$$(f) = 2(1 : 1 : 0) - (0 : 1 : i) - (0 : i : 1)$$

Observamos que por ser f una función racional, el grado de (f) es cero.

Definición 4.2.11: El divisor de una función racional se denomina **divisor principal**. Diremos que dos divisores, D, D' son **equivalentes** (o linealmente equivalentes) si y solo si $D - D'$ es un divisor principal ($D \equiv D'$).

Definición 4.2.12: El **grado de singularidad** o género de una curva $\mathcal{X}_F$ no singular se define como:

$$g = \frac{(deg(F) - 1)(deg(F) - 2)}{2}$$

4.3. Construcción de los Códigos

La idea es evaluar funciones racionales en puntos de la curva que no sean polos. Sea $\mathcal{X}$ una curva proyectiva suave e irreducible, definida sobre $\mathbf{F}_q$ (en adelante, diremos solo "una curva"). Para cada divisor D de $\mathcal{X}$, definimos el conjunto de funciones racionales:

$$\mathcal{L}(D) = \{f \in K(\mathcal{X}) \mid (f) + D \succeq 0\} \cup \{0\}$$

Este conjunto es un espacio vectorial en $\mathbb{F}_q$, cuya dimensión denotaremos por $l(D)$.
Sea $\mathcal{P} = \{P_1, \ldots, P_n\}$ un conjunto de puntos racionales distintos de $\mathcal{X}$. Podemos construir el divisor $D = P_1 + \ldots + P_n$. Sea G otro divisor racional de la curva tal que su soporte cumpla $sop(D) \cap sop(G) = \emptyset$. Podemos entonces, considerar la siguiente evaluación:

$$ev_{\mathcal{P}} : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n, \quad ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

Como $P_i \notin sop(G)$, entonces P_i no puede ser un polo de $f \in \mathcal{L}(G)$ (el que no esté en el soporte supone que $v_{P_i}(f)$ debe ser mayor o igual que 0). Por otro lado, $f(P_i) \in \mathbb{F}_q$, puesto que tanto P_i como G son puntos racionales (puntos con coordenadas en $\mathbb{F}_q$). Además, es sencillo ver que $ev_{\mathcal{P}}$ se trata de una aplicación lineal entre espacios vectoriales.

Lema 4.1: Sea D un divisor de la curva $\mathcal{X}$ tal que $deg(D) < 0$, entonces, $l(D) = 0$.

Demostración: Si $deg(D) < 0$, entonces para cualquier función racional $f \in K(\mathcal{X}) \setminus \{0\}$. Usando el teorema 4.2.3, que vimos sobre divisores de funciones racionales, sabemos que, $deg(f) = 0$. En consecuencia, $deg((f) + D) < 0 \Rightarrow f \notin \mathcal{L}(D)$

□

Definición 4.3.13: Dada una curva $\mathcal{X}$, y D y G divisores con las propiedades indicadas anteriormente. Un **código algebraico geométrico** es el subespacio vectorial dado por la imagen $ev_{\mathcal{P}}(\mathcal{L}(G))$; y lo denotaremos por $\mathcal{C}_{\mathcal{L}}(D, G)$

Teorema 4.3.4: El código $\mathcal{C}_{\mathcal{L}}(D, G)$ es un código lineal de parámetros $[n, k, d]$.

1. $k = l(G) - l(G - D)$

2. $d \geq n - deg(G)$

Demostración: Recordando que, por como hemos construido los códigos, los divisores D, G los podemos escribir como $D = \sum_{P_i \in sop(D)} n_{P_i} P_i = \sum_{P_i \in sop(D)} P_i$ y $G = \sum_{G_i \in sop(G)} m_{G_i} G_i$, con $sop(D) \cap sop(G) = \emptyset$. Consideremos el núcleo de $ev_{\mathcal{P}}$:

$$Ker(ev_{\mathcal{P}}) = \left\{ f \in \mathcal{L}(G) \;\middle|\; f(P_i) = 0,\ i \in \{0, 1, \ldots, n\} \right\} = \mathcal{L}(G - D)$$

Examinemos la segunda igualdad, empezando por la contención $Ker(ev_{\mathcal{P}}) \supseteq \mathcal{L}(G - D)$. Por hipótesis, $sop(D) \cap sop(G) = \emptyset$, luego si $(f) + (G - D) \succeq 0$, en particular, los coeficientes correspondientes al soporte de D son positivos $\forall P_i \in sop(D)$. El coeficiente del divisor $(f) + (G - D)$, en el punto P_i, es $v_{P_i}(f) - n_{P_i} \geq 0 \Rightarrow v_{P_i}(f) - 1 \geq 0$, eso implica que $v_{P_i}(f) > 0 \Rightarrow f(P_i) = 0$, $\forall P_i \in sop(D)$ y por tanto $f \in Ker(ev_P)$.
Para la otra contención, si $f \in \mathcal{L}(G)$ con $f(P_i) = 0$ entonces su valoración es positiva, $v_{P_i}(f) > 0$. Luego $\forall P_i \in sop(D)$, $v_{P_i}(f) - 1 = v_{P_i}(f) - n_{P_i} \geq 0$. Para los puntos $Q_i \notin sop(D)$, por tener que $f \in \mathcal{L}(G)$, tenemos coeficiente $v_{G_i}(f) + m_{G_i} - n_{P_i} = v_{G_i}(f) + m_{G_i} \geq 0$. Por tanto, $(f) + (G - D) \succeq 0 \Rightarrow f \in \mathcal{L}(G - D)$. Demostrando así la igualdad.
Con lo anterior, aplicando la fórmula de las dimensiones al código:

$$k := dim(\mathcal{C}_{\mathcal{L}}(D, G)) = dim(Img(ev_{\mathcal{P}})) = dim(\mathcal{L}(G)) - dim(Ker(ev_{\mathcal{P}})) =$$
$$dim(\mathcal{L}(G)) - dim(\mathcal{L}(G - D)) = l(G) - l(G - D).$$

Para la segunda afirmación, si tenemos $\mathbf{0} \neq \mathbf{c} \in \mathcal{C}_{\mathcal{L}}(D, G)$, es un elemento de peso mínimo, d. Entonces, por definición de peso, f se anula en $n - d$ puntos del soporte de D , que denotaremos por $P_{i-1}, P_{i_2}, \ldots, P_{i_{n-d}}$. Por tanto, razonando de forma similar a como lo hemos en el caso del núcleo, tenemos que $f \in \mathcal{L}(G - (\sum_{j=1}^{n-d} P_{i_j}))$. Como $f \neq 0$, $dim(\mathcal{L}(G - (\sum_{j=1}^{n-d} P_{i_j}))) \geq 1$. Esto dignifica que $deg(G - (\sum_{j=1}^{n-d} P_{i_j})) \geq 0$, por el lema 4.1. Por tanto $0 \leq deg(G - (\sum_{j=1}^{n-d} P_{i_j})) = \sum_{G \in sop(G)} m_{G_i} - (n - d) \Rightarrow 0 \leq deg(G) - (n - d)$.

□

Vamos a enunciar un resultado importante, pero cuya demostración está fuera del alcance de este trabajo:

Teorema 4.3.5 (de Riemann-Roch): Sea D un divisor de una curva proyectiva suave con grado de singularidad g. Entonces, para cada divisor canónico W (ver [16], capítulo 2, definición 2.47), tenemos que:

$$l(D) - l(W - D) = deg(D) - g + 1$$

Como consecuencia de esto, si W es divisor canónico, $deg(W) = 2g - 2$.

Corolario 4.3.6: Si $deg(G) < n$, entonces $k = l(G)$ y si $2g - 2 < deg(G) < n$, entonces $k = deg(G) + 1 - g$

Demostración: Si $deg(G) < n$, tenemos que dado que $deg(D = \sum_{i=1}^{n} P_i) = n$ y $\emptyset = sop(G) \cap sop(D)$, entonces $deg(G - D) = deg(G) - deg(D) = deg(G) - n < 0$. Usando el lema 4.1, tenemos que $l(G - D) = 0$ y por tanto $k = l(G) - l(G - D) = l(G)$.
La segunda parte de la demostración es consecuencia del teorema de Riemman-Roch, pero trata con divisores canónicos, que no hemos definido.

□

En genera, trataremos con códigos $\mathcal{C}_{\mathcal{L}}(D, G)$ que verifican la segunda condición del corolario ($2g - 2 < deg(G) < n$) y se los denomina **fuertemente algebraico-geométricos**. En adelante, trataremos solo con este tipo de códigos.

No existen en general condiciones sobre D y G que permitan dar una expresión exacta sobre la distancia mínima del código, pero podemos tratar con una aproximación:

Definición 4.3.14: Llamaremos **distancia diseñada** a $d^* := n - deg(G)$ a la aproximación de la distancia mínima dada por la anterior expresión.

El siguiente resultado nos dice cuando d^* coincide con la distancia mínima:

Proposición 4.3.7: Supongamos que $deg(G) < n$. Entonces, $(d^* = d) \Longleftrightarrow$ (existe un divisor $D', D \succeq D' \succeq 0$ tal que $D \equiv D'$).

Demostración: En la demostración teorema 4.3.4 vimos que la distancia mínima es d si y solo si existen $n-d$ puntos, $\{P_{i_j}\}_{j=1}^{n-d}$ tales que $l(G - P_{i_1} - \cdots - P_{i_{n-d}}) > 0$. Si $d^* = d$, entonces $n - d = deg(G) \Leftrightarrow deg(\sum_{j=1}^{n-d} P_{i_j}) = n - d = deg(G)$. Es decir que $deg(G - \sum_{j=1}^{n-d} P_{i_j}) = 0$. Si consideramos el divisor $B = G - \sum_{j=1}^{n-d} P_{i_j}$ sean $Q_i = (Q_{iX} : Q_{iY} : Q_{iZ})$ los puntos donde sus coeficientes no son cero; y $\varphi_z^{-1}(Q_i) = (q_{ix}, q_{iy})$ su versión afín (sin pérdida de generalidad, asumimos $Q_{iZ} \neq 0$, podemos igualmente considerar φ_x^{-1} o φ_y^{-1}) $B = \sum n_j Q_j$. Vemos que es el divisor de una función racional, g, con $v_{Q_j}(g) = n_j$, puesto que su grado es cero, y:

$$g = \frac{R}{H} = \frac{\prod_{v_{Q_j}(g)>0}(x - q_{jx})^{v_{Q_j}} + \prod_{v_{Q_j}(g)>0}(y - q_{jy})^{v_{Q_j}}}{\prod_{v_{Q_j}(g)<0}(x - q_{jx})^{v_{Q_j}} + \prod_{v_{Q_j}(g)<0}(y - q_{jy})^{v_{Q_j}}}$$

Los polinomios R, H son de grado $\sum_{v_{Q_j}(g)>0} v_{Q_j}(g) = \sum_{v_{Q_j}(g)<0} v_{Q_j}(g)\ g(Q_j)$ (igualdad dada porque $deg(B) = 0$), y $R(\varphi_z^{-1}(Q_i)) = 0,\ \forall Q_j$ con $v_{Q_j}(g) > 0$ y $H(\varphi_z^{-1}(Q_j)) =$

0, $\forall Q_j$ con $v_{Q_j}(g) < 0$. Si consideramos la homogeneización $g^* = R^*/H^*$ obtenemos un cociente de polinomios homogéneos del mismo grado, luego $g^* \in K(\mathcal{X})$ es una función racional. Además, los ceros y polos se preservan por la transformación. Luego, los divisores son equivalentes.

□

Como hemos dicho, nos limitamos a los códigos con $deg(G) > 2g - 2$. Juntando la cota de sigleton (Corolario 3.2.7) con el corolario 4.3.5 del teorema de Riemann-Roch, obtenemos que:

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

Por tanto, los códigos AG, obtenidos de curvas de género cero son MDS (definición 3.2.7), y la cota empeora para curvas de género mayor.

Notemos que, con esto podemos caracterizar el código, ya que podemos dar una matriz generatriz. Supongamos que $\{f_1, f_2, \ldots, f_k\}$ es una base del espacio $\mathcal{L}(G)$, entonces, la matriz generatriz del código $\mathcal{C}_{\mathcal{L}}(D, G)$ es:

$$G = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{pmatrix}$$

En general, esta matriz generatriz será difícil de obtener, pues obtener una base de $\mathcal{L}(G)$ no es sencillo.

4.4. Códigos $\mathcal{C}_{\Omega}(\mathcal{X})$ y decodificación

Vamos a introducir ahora el código dual de $\mathcal{C}_{\mathcal{L}}(D, G)$. Este código se puede definir usando formas diferenciales (ver [16], sección 2.5 para una introducción a formas diferenciales y [10] capítulo 13, para ver la definición de estos códigos con formas diferenciales), y demostrar que ambos códigos son equivalentes pero, para propósitos de este trabajo, lo introduciremos como el código dual. Se trata también de un código algebraico geométrico, de evaluación.

Definición 4.4.15: Consideremos el código algebraico-geométrico $\mathcal{C}_{\mathcal{L}}(D, G)$. Entonces denotaremos $\mathcal{C}_{\Omega}(D, G)$ a su código dual (definición 3.2.8).

Por tratarse del código dual, si $\mathcal{C}_{\mathcal{L}}(G, D)$ es un código de parámetros $[n, k]$, entonces $\mathcal{C}_{\Omega}(D, G)$ es un código $[n, n - k]$. No podemos obtener información sobre la distancia mínima sobre el dual a partir del código dual, pero usando propiedades sobre la construcción

del código podemos saber más. Del mismo modo a como hicimos para, $\mathcal{C}_\mathcal{L}(D,G)$, podemos obtener una cota inferior sobre d. Como hemos dicho, no demostraremos estos resultados, pero los enunciamos a continuación.

Proposición 4.4.8: Si el código $\mathcal{C}_\Omega(D,G)$ es un código lineal de parámetros $[n,k,d]$, entonces presenta las siguientes propiedades.

- $d > deg(G) - 2g + 2$
- Si $2g-2 < deg(G) < n$, entonces $k = n + g - 1 - deg(G)$.

Al igual que ocurre con $\mathcal{C}_\mathcal{L}(G,D)$, no se puede dar una distancia mínima de forma exacta, y trataremos con aproximaciones. Llamaremos **distancia diseñada** del código $\mathcal{C}_\Omega(D,G)$ a $d^* = deg(G) - 2g + 2$.

Veamos ahora cómo podemos dar un algoritmo de decodificación para este tipo de códigos. Consideraremos D y G como en las secciones anteriores, y $2g-2 < deg(G) < n$. También recordemos que, ya que la distancia mínima del código no es en general conocida, hablaremos de distancia diseñada d^*.

Nos ponemos en la situación del proceso de comunicación que hemos descrito cuando introdujimos los códigos correctores lineales. El emisor quiere mandar un mensaje $\mathbf{m}$, que codifica usando el código $\mathcal{C}_\Omega(D,G)$ como $\mathbf{c} \in \mathcal{C}_\Omega(D,G)$. El mensaje se manda a través de un canal con ruido, y el receptor recibe la palabra $\mathbf{y} = \mathbf{c} + \mathbf{e}$ (donde $\mathbf{e}$ es el error que se ha producido). Denotaremos por $I := sop(\mathbf{e})$ al conjunto de índices correspondientes a posiciones donde se producido un error (recordemos la notación introducida en el capitulo anterior, cuando hablamos de decodificación basada en códigos lineales, en la sección 3.5).

Definición 4.4.16: Una **función localizadora de errores**, ϕ, es una función tal que el conjunto $J(\phi) = \{i \mid \phi(P_i) = 0\}$, verifica que $sop(\mathbf{e}) = I \subseteq J(\phi)$ y $|J(\phi)| < d^*$.

Como vimos en el capítulo anterior, conocer $J(\phi)$, nos permitirá plantear un sistema de ecuaciones y así calcular el vector de error. Para ello necesitamos introducir el concepto de síndrome, pues si bien la definición genérica sigue siendo válida, vamos a dar una específica a este tipo de códigos, ya que las matrices generatriz y de control son difíciles de obtener para estos códigos.

Definición 4.4.17: Dado $\mathbf{x} \in \mathbb{F}_q^n$ y $f \in \mathcal{L}(G)$, llamaremos **síndrome** de $\mathbf{x}$ respecto a f a:

$$s(\mathbf{x}, f) = \langle \mathbf{x},\ ev_\mathcal{P}(f) \rangle = \sum_{i=1}^{n} x_i f(P_i).$$

Puesto que ambos códigos son duales (y en consecuencia, ortogonales), si $\mathbf{x} \in \mathcal{C}_\Omega(D,G)$, entonces $s(\mathbf{x},f) = 0,\ \forall f \in \mathcal{L}(G)$. Además, si $\mathbf{y} = \mathbf{c} + \mathbf{e}$, $\mathbf{c} \in \mathcal{C}_\Omega(D,G)$, entonces $s(\mathbf{y}f) = s(\mathbf{c},f) + s(\mathbf{e},f) = 0 + s(\mathbf{e},f)$.

Sea t un entero positivo. Supongamos que existe F, un divisor racional sobre la curva $\mathcal{X}$ con la cual hemos construido el código, y cuerpo $\mathbb{F}_q$, que satisface las siguientes condiciones:

$$\begin{aligned} sop(F) \cap sop(D) &= \emptyset. \\ deg(F) < deg(G) - 2g + 2 - t &= d^* - t. \\ l(F) &> t. \end{aligned} \tag{4.1}$$

Así mismo, fijamos las bases:

$$\{f_1, \ldots, f_l\} \quad \text{de } \mathcal{L}(F).$$

$$\{g_q, \ldots, g_m\} \quad \text{de } \mathcal{L}(G-F).$$

Lema 4.2: Si se verifican las condiciones impuestas sobre el divisor F y el vector que le llega al receptor $\mathbf{y}$ tiene como mucho t errores, entonces, el sistema de ecuaciones homogéneas:

$$\sum_{i=1}^{l} s(\mathbf{y}, f_i g_i) = 0,\ j = 1, \ldots, m$$

Posee una solución no nula.

Demostración: Primero vemos que, efectivamente $f_i g_i \in \mathcal{L}(G)$. Esto es cierto, pues $f_i g_i$ es una función racional y $(f_i g_i) + G \succeq 0$, pues:

$$(f_i g_i) = \sum_{P \in \mathcal{X}} v_P(f_i g_i) P = \sum_{P \in \mathcal{X}} v_P(f_i) P + \sum_{P \in \mathcal{X}} v_P(g_i) P = (f_i) + (g_i)$$

Usando que $v_P(fg) = v_P(f) + v_P(g))$ ver ([9], teorema 2.16). Además, como $G = (G - F) + F$, tenemos que: $(f_i g_i) + G = ((g_i) + G - F) + ((f_i) + F)$. Por definición $(f_i) + F$ tiene todos sus coeficientes positivos, y $(g_i) + G - F$ también. Su suma también los tendrá, y por tanto, $(f_i g_i) + G \succeq 0$.
Si $|I| = |sop(\mathbf{e})| \leq t$, tenemos que, por la condición 3 sobre F, $l(F) > t$:

$$0 \neq \mathcal{L}(F - \sum_{i \in I} P_i) \leq \mathcal{L}(F)$$

Para ver esto, tenemos que $\{f \in \mathcal{L}(F) \mid f(P_i) = 0,\ \forall i \in I\} = \mathcal{L}(F - \sum_{i \in I} P_i)$. Esto es cierto, porque podemos aplicar el mismo razonamiento que usamos para ver que $ker(ev_P) = \mathcal{L}(G - D)$, tal y como vimos en la demostración del teorema 4.3.4. Podemos ver $\{f \in \mathcal{L}(F) \mid f(P_i) = 0,\ \forall i \in I\}$ como el núcleo de $e\tilde{v}_{\mathcal{P}} : \mathcal{L}(F) \to \mathbb{F}_q^{|I|}$, $e\tilde{v}_{\mathcal{P}}(f) =$

$(f(P_{i_1}),\ldots,f(P_{i_{|I|}}))$, $i_j \in I$. Puesto que $l(F) > t \geq |I|$, existe $f \in \mathcal{L}(F)$, tal que $f \in \{f \in \mathcal{L}(F) \mid f(P_i) = 0,\ \forall i \in I\}$, por tanto, $f \in \mathcal{L}(F - \sum_{i\in I} P_i) \Rightarrow l((F - \sum_{i\in I} P_i)) \geq 1$.

Podemos, considerar, $h \in \mathcal{L}(F - \sum_{i\in I} P_i) \setminus \{0\}$, con $h(P_i) = 0\ \forall i \in I$. Es decir, para todo punto en que $\mathbf{e}_i \neq 0$. Como $h \in \mathcal{L}(F)$, se puede expresar como:

$$h = \sum_{i=1}^{l} \alpha_i f_i.$$

Por el mismo motivo que $f_i g_i \in \mathcal{L}(G)$, $hg_j \in \mathcal{L}(G))$, $\forall j = 1, 2, \ldots, m$. Además, los síndromes son funciones lineales, por lo que:

$$\sum_{i=1}^{l} \alpha_i s(\mathbf{y}, f_i g_i) = s(\mathbf{y}, hg_i) = s(\mathbf{e}, hg_i) = \sum_{i=1}^{n} e_i h(P_i) g_j(P_i) = 0$$

Luego $(\alpha_1, \ldots, \alpha_l)$ es una solución no trivial del sistema (pues $h \neq 0$).

□

Con la notación de la demostración anterior, definimos:

$$\phi = \sum_{i=1}^{l} \alpha_i f_i \in \mathcal{L}(F)$$

Proposición 4.4.9: Si un F verifica las tres condiciones que hemos descrito, y el número de errores es menor o igual que t, entonces ϕ es una función localizadora de errores de $\mathbf{y}$

Demostración: Debemos probar que $I \subseteq J(\phi)$ y que $|J(\phi)| < d^*$. La segunda condición es consecuencia de que $\phi \in \mathcal{L}(F - \sum_{i\in J(\phi)} P_i) \setminus \{0\}$ (que es cierto por el mismo argumento que dimos para ver $\mathcal{L}(F - \sum_{i\in I} P_i) \neq 0$ en el lema anterior). Por tanto $l(F - \sum_{i\in I} P_i) \geq 1 \Rightarrow deg(F - \sum_{i\in I} P_i) \geq 0$ (ver lema 4.1).

Usando $F - \sum_{i\in J(\phi)}$ y que el soporte de F y D es disjunto, tenemos que $0 \leq deg(F - \sum_{i\in I} P_i) = deg(F) - deg(\sum_{i\in I} P_i) \Rightarrow deg(F) \geq deg(\sum_{i\in I} P_i) = \sum_{i\in I} 1 = |J(\phi)|$. Usando la segunda condición sobre el divisor F, tenemos $deg(F) < d^* - t < d^*$. Juntándolo todo, $|J(\phi)| \geq deg(F) < d^*$.

Para la segunda condición, probaremos que todos los puntos $P_i \in sop(D)$, con $\mathbf{e}_i \neq 0$, son ceros de ϕ. Razonamos por reducción al absurdo. Si uno de los puntos P_{i_0} no verifica esta condición, entonces, por la segunda condición del divisor F, tenemos que.

$$deg\big(G - F - \sum_{i\in I} P_i\big) \geq deg(G) - deg(F) > 2g - 2$$

Y por el teorema de Riemann-Roch, (ver corolario 2.58 del teorema de Riemann-Roch en [16]), tenemos la primera y última igualdad de la siguiente expresión:

$$l(G-F-\sum_{i\in I} P_i) = deg(G-F-\sum_{i\in I} P_i)-g+1 < deg(G-F-\sum_{i\in I\setminus\{i_0\}} P_i)-g+1 = l(G-F-\sum_{i\in(I\setminus\{i_0\})} P_i)$$

La desigualdad central es aritmética, al calcular el grado del divisor. Existe, por tanto, una función $z \in \mathcal{L}(G-F)$ con ceros en todos los puntos excepto en P_{i_0} (pues podemos tomar $0 \neq z \in \mathcal{L}(G-F-\sum_{i\in(I-\{i_0\})} P_i) \setminus \mathcal{L}(G-F-\sum_{i\in I} P_i)$). Por tanto:

$$s(\mathbf{y},\phi z) = s(\mathbf{e},\phi z) = \sum_{i=1}^{n} e_i\phi(P_i)z(P_i) = e_{i_0}z(P_{i_0})z(P_i) \neq 0$$

Si bien, para cada $g_j \in \mathcal{L}(G-F)$, el lema anterior nos dice que $(\alpha_1,\ldots,\alpha_l)$ es solución del sistema de ecuaciones homogéneo:

$$\sum_{i=1}^{l} s(\mathbf{y}, f_i g_i) = 0,\ j = 1,\ldots,m$$

Y por definición de ϕ, $s(\mathbf{y},\phi z) = \sum_{i=1}^{l} s(\mathbf{y}, f_i g_i)$. Como z pertenece a $\mathcal{L}(G-F)$, $z = \sum_{i=1}^{m} \lambda_i g_i$. Si consideramos el síndrome:

$$s(\mathbf{y},\phi z) = \sum_{i=1}^{m} \lambda_i s(\mathbf{y},\phi g_i) = 0$$

Pero hemos visto antes que $s(\mathbf{y},\phi z) \neq 0$, llegando así a una contradicción.

□

Con esta proposición hemos completado la descripción del proceso de decodificación. Recapitulando, hemos de:

1. Encontrar un divisor F que cumpla las condiciones descritas (4.1).

2. Calcular una solución $(\alpha_1,\ldots,\alpha_l)$ al sistema homogéneo planteado en el lema 4.2, para lo cual debemos conocer las bases de $\mathcal{L}(F)$ o $\mathcal{L}(G-F)$ o, al menos, los coeficientes del sistema dados por los síndromes $s(\mathbf{y}, f_i g_i)$.

3. Con dicha solución, podemos definir la función localizadora de errores (definición 4.4.16), y calcular el conjunto $J(\phi)$, evaluando ϕ en cada uno de los puntos, P_i, del divisor D. Anotamos los índices de los puntos donde es cero dicha función.

4. Con esto, podemos plantear y resolver el sistema de ecuaciones:

$$\begin{cases} s(\mathbf{x}) &= s(\mathbf{y}) \\ x_i &= 0, \quad \text{si } i \notin J(\phi) \end{cases} . \tag{4.2}$$

   Como vimos en el la sección 3.5 del capítulo anterior, este sistema tiene a $\mathbf{e}$, el vector de errores, como única solución.

5. Finalmente, podemos recuperar $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

Para evaluar la capacidad correctora de este método, es necesario saber para qué valores es posible. En [10] se muestra que este método no permite corregir los $\lfloor (d^* - 1)/2 \rfloor$) que a priori parecían posibles, pero si $0 \leq t \leq (d^* - 1 - g)/2$, se puede encontrar un divisor racional (con todas las coordenadas en $\mathbb{F}_q$), F, de modo que el algoritmo corrige $\lfloor (d^* - 1 - g)/2 \rfloor$ errores. De hecho, si existe un punto racional P sobre $\mathcal{X}$ que no pertenezca al soporte de D, $F = (g + t)P$ es un divisor que cumple las condiciones.

Capítulo 5

Códigos algebraico-geométricos en un punto

En este capítulo vamos a tratar un caso especial de códigos algebraico-geométricos, los llamados "one-point-algebraic codes", o códigos en un punto.

5.1. Conexión entre semigrupos y curvas algebraicas

Consideremos el espacio $\mathcal{L}(mP) = \{f \in K(\mathcal{X}) \mid (f) + mP \succeq 0\}$, donde m es un entero positivo y P es un punto en la curva proyectiva $\mathcal{X}$. Observamos que dicho $\mathbb{F}_q$-espacio vectorial se trata del espacio de funciones racionales que poseen únicamente un polo, en el punto P, y dicho polo es de grado menor o igual que m. Para la dimensión de dicho espacio, denotada por, $l(mP) := dim_{\mathbb{F}_q}(\mathcal{L}(mP))$, tenemos el siguiente resultado:

Proposición 5.1.1:

- $l(mP) = l((m-1)P) + 1$, si y solo si existe una función racional $f \in K(\mathcal{X})$ con un único polo en el punto P y tal que $v_P(f) = -m$.
- Uno de los dos siguientes casos es cierto, o se cumple que $l(mP) = l((m-1)P)$, o se cumple que $l(mP) = l((m-1)P) + 1$. Además, el primer caso se da g veces (siendo g el género de la curva).

Demostración:

- Supongamos que $l(mP) = l((m-1)P) + 1$, entonces, la dimensión del espacio cociente $V := \big((\mathcal{L}(mP))/(\mathcal{L}((m-1)P)\big)$, es 1. Por lo que $\exists f \in V,\ f \in \mathcal{L}(mP)$, tal que f solo tiene polos en P (como todas las funciones de $\mathcal{L}((m-1)P)$ y $\mathcal{L}(mP)$). Además, como $f \notin \mathcal{L}((m-1)P)$, dicho polo es de grado $m \Rightarrow v_P(f) = -m$.

Por otro lado, si $\exists f \in K(\mathcal{X})$ tal que f tiene un único polo de grado m en P, entonces, por el grado del polo $f \in \mathcal{L}(mP)$, además $0 \neq \overline{f} \in V = (\mathcal{L}(mP)/\mathcal{L}((m-1)P)) \Rightarrow dim(V) \geq 1 \Rightarrow l(mP) > l((m-1)P)$. Entonces, basta con que veamos que $dim_K(V) = 1$. Si $\mathcal{Z}$ es una base de $\mathcal{L}(mP)$, entonces, para un cierto $I \subset \mathbb{N}_0$, $|I| \leq \infty$ y $a_i \in K$, tenemos que

$$f = \sum_{i\in I,\ z_i\in\mathcal{Z}} a_i z_i \Rightarrow \overline{f} = \sum_{\substack{i\in I,\ z_i\in\mathcal{Z},\\ v_P(z_i)>-m}} a_i\overline{z}_i + \sum_{\substack{i\in I,\ z_i\in\mathcal{Z},\\ v_P(z_i)=-m}} a_i\overline{z}_i = 0 + \sum_{\substack{i\in I,\ z_i\in\mathcal{Z},\\ v_P(z_i)=-m}} a_i\overline{z}_i$$

Donde $a \in K$. Usando el teorema 4.1.1, tenemos que $z_i \mid v_P(z_i) = -m$, $a_i z_i = ut^{-m}$, donde t es un parámetro local de $\mathcal{P}_P$ en P, y u es una unidad de $K(\mathcal{X})$. Entonces,

$$\overline{f} = \overline{t^{-m}}\overline{(u + u' + u'' + \ldots + u^{(n)})} = b\overline{t^{-m}}$$

Con $b \in K$. Luego $V = \langle\overline{t^{-m}}\rangle$ es un K-espacio vectorial de dimensión 1.

- Consideremos el corolario al teorema de Riemann-Roch que vimos en la sección anterior. Si $deg(mP) = m > 2g-1 > 2g-2$, podemos aplicar el corolario 4.3.6 a $\mathcal{L}(mP)$, además, $deg((m-1)P) = m-1 > 2g-2$, por lo que también podemos aplicar el corolario 4.3.6 a $\mathcal{L}((m-1)P)$. Tenemos pues:

$$l(mP) = m - g + 1 = ((m-1) - g + 1) + 1 = l((m-1)P) + 1.$$

Consideramos $m = 2g-1$, el primer valor para el que no se verifica la hipótesis $m > 2g-1$. Entonces, por el corolario 4.3.6, tenemos que $l(mP) = 2g-1-g+1 = g$. Además, puesto que para dos enteros positivos n, m con $n \leq m$, tenemos que, $\mathcal{L}(nP) \subseteq \mathcal{L}(mP) \Rightarrow l(nP) \leq l(mP)$, podemos escribir la siguiente cadena de desigualdades de longitud $2g$:

$$g = l((2g-1)P) \geq l((2g-2)P) \geq \ldots \geq l(P) \geq l(0) = 1$$

Luego al menos, hay g valores de $0 \geq m \geq 2g-1$, en los cuales se da $l(mP) = l((m-1)P)$. Vemos que este número no es mayor que g. Si fuera así, como la cadena de desigualdades tiene $2g$ elementos, habría como mucho $g-1$ desigualdades estrictas; de tipo $l(mP) > l((m-1)P)$. Esto implicaría que, para cierto $0 \geq m \geq 2g-1$, $l(mP) \geq l((m-1)P) - 2$, lo cual es absurdo.
Si así fuera, entonces, $\exists f \in \mathcal{L}(mP) \setminus \mathcal{L}((m-1)P)$ que presenta un único polo de grado m en P. Usando el primer apartado, tenemos que $l(mP) = l((m-1)P) + 1$, llegando a una contradicción.

□

Definición 5.1.1: Sea P un punto de la curva con las propiedades descritas anteriormente. Definimos $\mathcal{A}(P) := \cup_{m\geq 0}\mathcal{L}(mP)$. Si no hay confusión sobre P, lo denotaremos simplemente

por $\mathcal{A}$.

Veamos que $\mathcal{A}$ se trata del conjunto de funciones racionales teniendo un único polo, en el punto P. De esta propiedad deducimos que se trata de un anillo, pues suma y producto preservan la propiedad, y si $0 \neq f \in \mathcal{A}$, entonces $-f$ también. El cero y el uno pertenecen, por ser funciones constantes (con un polo de grado cero en P y sin polos de grado mayor que cero en otros puntos).

Definición 5.1.2: Sea P un punto de la curva $\mathcal{X}$, definimos el conjunto

$$\Lambda = \{ -v_P(f) \mid f \in \mathcal{A}(P) \setminus \{0\} \}$$

Claramente, Λ es un conjunto de enteros no negativos. Tenemos además:

Proposición 5.1.2: El conjunto Λ, es un semigrupo numérico. Es decir, satisface:

1. $0 \in \Lambda$
2. $m + m' \in \Lambda$, si $m, m' \in \Lambda$
3. $\mathbb{N}_0 \setminus \Lambda$ tiene una cantidad finita de elementos. Además, $|\mathbb{N}_0 \setminus \Lambda| = g$

Demostración:

1. Las funciones constantes $f = a$ no tienen polos, luego $v_P(a) = 0$ para cualquier $P \in \mathcal{X}$. Por tanto, $0 \in \Lambda$.
2. Si $m, m' \in \Lambda$, entonces, existen $f, g \in \mathcal{A}(P)$, tales que $v_P(f) = -m$ y $v_P(g) = -m'$. Sabemos que $fg \in \mathcal{A}$ (pues fg solo puede tener polos en P, porque f y g solo tienen polos en P) entonces, $v_P(fg) = v_P(f) + v_P(g) = -(m + m')$, luego $(m + m') \in \Lambda$.
3. Para todos los enteros positivos, $m \in \mathbb{N}_0$ tenemos dos opciones, según la proposición anterior (5.1.1). Si $l(mP) = l((m-1)P) + 1$, entonces, existe $f \in K(\mathcal{X})$ con $v_P(f) = -m \Rightarrow m \in \Lambda$.
   Si $l(mP) = l((m-1)P)$, entonces no existe $f \in K(\mathcal{X})$ tal que $v_P(f) = -m$ y entonces $m \notin \Lambda$. Puesto que hemos visto que este último caso se da solo para g enteros positivos, $m_1, \ldots, m_g$, entonces, $\{m_1, \ldots, m_g\} = \mathbb{N}_0 \setminus \Lambda$ es un conjunto finito; y su cardinal (el género del semigrupo) es g, que coincide con el género de la curva.

□

El semigrupo numérico Λ, lo llamamos, **semigrupo de Weierstrass** de la curva $\mathcal{X}$ en el punto P. Este resultado, no solo nos permite definir un semigrupo asociado a una curva

algebraica, si no que establece la conexión entre género de la curva y del semigrupo.

Ejemplo 5.1.1 (Curva Hermítica):

Consideramos que trabajamos en $\mathbb{F}_q$, q potencia de un número primo. La curva Hermítica, está definida por las ecuaciones:

$x^{q+1} = y^q + y$ (Ecuación afín), $\quad F(X,Y,Z) = X^{q+1} - Y^q Z - Y Z^q = 0$ (Ecuación proyectiva)

Es decir, $\mathcal{H}_q := V(\langle F \rangle)$. Las derivadas parciales son:

$$F_X = (q+1)X^q = X^q, \quad F_Y = -qY^{q-1}Z - Z^q = 0 - Z^q, \quad F_Z = -Y^q - qYZ^{q-1} = -Y^q$$

Con lo cual vemos que no hay ningún punto singular ($P = (a : b : c) \in \mathbb{P}^2$ tal que $F_X(P) = F_Y(P) = F_Z(P) = 0$), luego es una curva suave. El punto $P_\infty = (0 : 1 : 0)$ es el único punto de la recta del infinito, $Z = 0$, que pertenece a $\mathcal{H}_q$. Queremos conocer un parámetro local de la curva en P_∞, por lo que examinamos la tangente:

$$d_{P_\infty} F = F_X(P_\infty)X + F_Y(P_\infty)Y + F_Z(P_\infty)Z = 0 \cdot X + 0 \cdot Y + -1 \cdot Z = -Z$$

Como X/Y no es múltiplo constante de la tangente, es un parámetro local en P_∞. Consideremos las funciones racionales X/Z e Y/Z sobre $\mathcal{H}_q$, como P_∞ es el único punto en $Z = 0$ de la curva, tenemos que ambas funciones son regulares en todos los puntos de la curva, excepto en P_∞. En consecuencia, ambas funciones pertenecen a $\mathcal{A}(P_\infty) = \cup_{m \geq 0} \mathcal{L}(mP_\infty)$; vamos a calcular $v_{P_\infty}(X/Z)$ y $v_{P_\infty}(Y/Z)$.

Si consideramos $F(\varphi_y^{-1}(X : Y : Z)) = F(X/Y, 1 = Y/Y, Z/Y) = (X/Y)^{q+1} - (Z/Y) - (Z/Y)^q$, es decir, $(Z/Y) + (Z/Y)^q = t^{q+1}$ y entonces $v_{P_\infty}((Z/Y) + (Z/Y)^q) = q + 1$. Usando las propiedades de v_{P_∞}, tenemos que:

$$q + 1 = v_{P_\infty}((Z/Y)^q + (Z/Y)) = min\{v_{P_\infty}(Z/Y), v_{P_\infty}(Z/Y)^q\} =$$
$$min\{v_{P_\infty}(Z/Y), q \cdot v_{P_\infty}(Z/Y)\} = v_{P_\infty}(Z/Y)$$

Pues $v_{P_\infty}(Z/Y) \neq v_{P_\infty}((Z/Y)^q) = q v_{P_\infty}(Z/Y)$. Por tanto $v_{P_\infty}(Z/Y) = q+1 \Rightarrow v_{P_\infty}(Y/Z) = -(q+1)$.

Usando un razonamiento similar, podemos obtener $v_{P_\infty}(X/Z)$, tomando la carta φ_z^{-1}, obtenemos $(X/Z)^{q+1} = (Y/Z)^q + (Y/Z)$, y por tanto:

$$(q+1)v_{P_\infty}(X/Z) = min\{v_{P_\infty}(Y/Z), v_{P_\infty}((Y/Z)^q)\} = v_{P_\infty}((Y/Z)^q) = q \cdot -(q+1) \Rightarrow v_{P_\infty}(X/Z) = -q$$

Por tanto, $q - 1, q \in \Lambda$, tenemos que, $\langle q, q+1 \rangle \subseteq \Lambda$. El género de la curva $\mathcal{H}_q$ es $g = \frac{(deg(F)-1)(deg(F)-2)}{2} = \frac{q(q-1)}{2}$, que coincide con el género calculado según la proposición 1.4.

En consecuencia, puesto que un semigrupo está contenido en otro, y tienen el mismo número de lagunas, deben coincidir; $\langle q, q+1\rangle = \Lambda$.

5.2. La operación $\oplus$ y la sucesión ν

Podemos dar una aplicación biyectiva que nos permita indexar o enumerar los elementos del semigrupo. Dicha aplicación se denomina enumeración:

Definición 5.2.3: Sea S un semigrupo numérico, $S = \{0 = s_0, s_1, \ldots, s_j, \ldots\}$, tal que $\forall i \in \mathbb{N}_0,\ s_i < s_{i+1}$. La aplicación $\lambda : \mathbb{N}_0 \to S$, $\lambda(i) = s_i$ es la **enumeración** del semigrupo S. Usaremos la notación $\lambda_i = \lambda(i)$

La aplicación anterior es claramente una biyección, y es creciente ($s_{i+1} = \lambda(i+1) > \lambda(i) = s_i = s$). Es por tanto la única aplicación con estas propiedades.

Definición 5.2.4: Definimos la operación $\oplus_S : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, asociada al semigrupo S, como:

$$i \oplus_S j = \lambda^{-1}(\lambda_i + \lambda_j)$$

Para cualquier $i, j \in \mathbb{N}_0$. λ^{-1} es la inversa de la enumeración de S. Si $\lambda_k - \lambda_i = \lambda_j \in \Lambda$, entonces decimos que $k \ominus_S i = \lambda^{-1}(\lambda_k - \lambda_j) = j$

Ejemplo 5.2.2: Consideremos el semigrupo $\langle 3, 5\rangle = \{0, 3, 5, 6, 8, \to\}$ y su correspondiente enumeración, λ. Entonces $1 \oplus 2 = \lambda^{-1}(3+5) = \lambda^{-1}(8) = 5$ y $3 \oplus 2 = \lambda^{-1}(6+5) = \lambda^{-1}(11) = 8$. Veamos un ejemplo usando GAP (donde los índices comienzan en 1):

```
gap> S:=NumericalSemigroup(3,5);;
gap> Oplus(2,3,S);
5
gap> S[2]; S[3]; S[5];
3
5
8
```

La operación $\oplus$ es conmutativa y asociativa, pues $i \oplus j = \lambda^{-1}(\lambda_i + \lambda_j) = \lambda^{-1}(\lambda_j + \lambda_i) = j \oplus i$ (y similarmente para la asociatividad). El cero es su elemento unidad, $0 \oplus i = \lambda^{-1}(\lambda_0 + \lambda_i) = \lambda^{-1}(0 + \lambda_j) = j$. Sin embargo, por lo general no hay inverso (si $\lambda_k - \lambda_i \notin S$ entonces $k \ominus_S i$ no está definida).

La operación también es compatible con la relación de orden del semigrupo. Es decir, si $a < b,\ a, b \in \mathbb{N}_0$, entonces $a \oplus c < b \oplus c$. Efectivamente $b \oplus c - a \oplus c = \lambda^{-1}(\lambda_c + \lambda_b) - \lambda^{-1}(\lambda_c + \lambda_a) > 0$, pues la enumeración es monótona creciente, luego también lo es la inversa, y $\lambda_b > \lambda_a$.

Definición 5.2.5: Sea S un semigrupo numérico y $\oplus_S$ la suma de índices asociada a S. Entonces definimos:

- El orden parcial en los naturales asociado a S, $(\mathbb{N}_0, \succeq_S)$ de forma que:

  $$j \succeq_S i \Leftrightarrow \lambda_j - \lambda_i \in S$$

  O, equivalentemente, existe $k \in \mathbb{N}_0$, tal que $i \oplus_S k = j$.

- El conjunto:

  $$D(\lambda_i) = \{j \in \mathbb{N}_0 \mid i \succeq j\} = \{j \in \mathbb{N}_0 \mid \lambda_i - \lambda_j \in S\}$$

  Al cardinal de dicho conjunto, lo denotaremos por $\nu_i = |D(\lambda_i)|$.

- Denotaremos ν a la sucesión $\{\nu_i\}_{i=0}^{\infty}$

Ejemplo 5.2.3 Para el caso trivial $S = \mathbb{N}_0$, tenemos que $D(\lambda_i) = \{j \in \mathbb{N}_0 \mid i - j \in \mathbb{N}_0\} = \{j \in \mathbb{N}_0 \mid j \leq i\} \Rightarrow \nu_i = 1 + i$. Luego $\nu = 1, 2, 3, \ldots$

Usando la función que he implementado en GAP, podemos calcular la sucesión ν de un semigrupo numérico. Esta función nos da la primera parte de la sucesión, pues a partir de un número crece en incrementos de 1 [4].

```
gap> S:=NumericalSemigroup(3,5);
<Numerical semigroup with 2 generators>
gap> NuSequence(S);
[ 1, 2, 2, 3, 4, 4, 3, 6, 5, 6, 8, 8 ]
```

Proposición 5.2.3: Sea S un semigrupo numérico, y ν su correspondiente sucesión ν. Tenemos que para todo $i \in \mathbb{N}_0$:

$$\nu_i = |\{(j, k) \in \mathbb{N}_0^2 \mid j \oplus k = i\}|$$

Demostración: Denotamos al conjunto $\{(j, k) \in \mathbb{N}_0^2 \mid j \oplus k = i\}$ como B, y definimos la aplicación $f : D(\lambda_i) \to B$ como indicamos a continuación. Si $j \in D(\lambda_i) \Rightarrow \lambda_i - \lambda_j \in S \Rightarrow$ $!\exists k \in \mathbb{N}_0\ |\lambda_i - \lambda_j = \lambda_k$. Por tanto, podemos definir $f(j) = (j, k)$. Efectivamente, $j \oplus k = \lambda^{-1}(\lambda_j + \lambda_k) = \lambda^{-1}(\lambda_i) = i$. La aplicación es inyectiva, pues $f(j_1) = f(j_2) \Leftrightarrow (j_1, k_1) = (j_2, k_2) \Leftrightarrow j_1 = j_2$. Es también sobreyectiva, pues dado $(j, k) \in B$, $j \oplus k = i \Rightarrow \lambda^{-1}(\lambda_j + \lambda_k) = i \Rightarrow \lambda_j + \lambda_k = \lambda_i \Rightarrow \lambda_i - \lambda_j = \lambda_k \in \Lambda \Rightarrow j \in D(\lambda_i)$

□

5.3. Códigos en un punto

5.3.1. Construcción de los códigos

Los códigos en un punto siguen una construcción muy similar a la que vimos en el capítulo anterior. El nombre viene dado porque están definidos en un divisor formado por un solo punto; es decir, el espacio de partida para definir la función $ev_P(f)$ es un espacio de la forma $\mathcal{L}(mP)$. Necesitamos un concepto nuevo, el de orden de una función, que ha motivado en parte la introducción de los semigrupos de Weierstrass en la sección anterior.

Definición 5.3.1.6: Dada $\mathcal{X}$, una curva suave e irreducible definida sobre el cuerpo $\mathbb{F}_q$. Si $\Lambda = \{0 = \lambda_0, \lambda_1, \ldots\}$ es el semigrupo de Weierstrass de la curva en el punto racional P, donde los elementos del semigrupo están enumerados en orden creciente ($\lambda_i > \lambda_j$ si $i > j$). Entonces, podemos definir una aplicación $\rho : \mathcal{A} \to \mathbb{N}_0 \cup \{-1\}$, de forma que, si $f \in \mathcal{A} \setminus \{0\}$ y $v_P(f) = -\lambda_s$, definimos $\rho(f) = s$; y si $f = 0$, establecemos $\rho(0) = -1$. Llamaremos a $\rho(f)$ **orden** de la función f.

Lema 5.1: Con las hipótesis y notación de la definición anterior, podemos encontrar una base infinita, $\mathcal{Z} = \{z_0, z_1, \ldots, z_i, \ldots\}$, de $\mathcal{A}(P)$, tal que $\forall i \in \mathbb{N}_0,\ v_P(z_i) = -\lambda_i$, o equivalentemente, $\forall i \in \mathbb{N}_0,\ \rho(z_i) = i$.

Demostración: Si $\lambda_i \in \Lambda \subseteq \mathbb{N}_0$, entonces, por definición del semigrupo de Weierstrass, $\exists f \in \mathcal{A}$ tal que $v_P(f) = -\lambda_i$ Veamos que, dada una base $\mathcal{Z} = \{z_0, z_1, \ldots, z_i, \ldots\}$ de $\mathcal{A}$, hay un elemento z_i de la base tal que $v_P(z_i) = -\lambda_i$.

Podemos expresar $f = \sum_{i \in I} a_i z_i,\ a_i \in K$, ($|I| < \infty$). Claramente, $v_P(a_i z_i) = 0 + v_P(z_i) \neq 0 + v_P(z_j) = v_P(a_j z_j),\ \forall i \neq j$ (Para ver que si $i \neq j$, $v_P(z_i) \neq v_P(z_j)$, ver demostración de la proposición 5.1.1, donde vimos que $dim(\mathcal{L}(mP) \setminus \mathcal{L}((m-1)P))) \leq 1$, luego dos elementos, $f_1,\ f_2 \in \mathcal{A}$ tales que $v_P(f_1) = v_P(f_2) = -m$ son linealmente dependientes). Entonces $v_P(f) = v_P\big(\sum_{i \in I} a_i z_i\big) = min_{i \in I}\{v_P(z_i)\}$ (segunda igualdad, por las propiedades de $v_P(f+g)$, ver teorema 2.16 en [16]). Por tanto el mínimo se alcanza para un cierto z_i, tal que $\lambda_i = v_P(f) = v_P(z_i)$.

□

Con esto podemos definir los códigos en un punto. Recordemos la definición de $ev_P(f)$, dada en el capítulo anterior (Sección 4.3).

Definición 5.3.1.7: Sea P, un punto racional de la curva suave e irreducible $\mathcal{X}$, y $D = P_1 + P_2 + \ldots + P_n$ un divisor racional, con $P_i \neq P$, $\forall i \in \{0, 1, \ldots, n\}$ y $\mathcal{Z}$ una base de $\mathcal{A}(P)$,

con las propiedades descritas por el lema anterior. Entonces, para cada subconjunto $W \in \mathbb{N}_0$, definimos el código **en un punto** asociado a W como:

$$\mathcal{C}_W = \langle ev_P(z_i) \mid i \in W \rangle^{\perp} = \langle (z_i(P_1), z_i(P_2), \ldots, z_i(P_n)) \mid i \in W \rangle^{\perp}.$$

Donde $\perp$ denota el código dual. En este caso la función de evaluación va del espacio vectorial de partida $V = \langle \{w_i\}_{i \in W} \rangle$ a $\mathbb{F}_q^n$.

Al conjunto W lo denominaremos conjunto de **comprobaciones de pariedad** de $\mathcal{C}_W$. Para el caso particular en que $W = \{1, 2, \ldots, k\}$, hablamos de código en un punto **clásicos**, y usaremos la notación $\mathcal{C}_k$.

Notamos que, si hablamos del caso de códigos clásicos, $V = \langle \{z_i\}_{i=1}^m \rangle = \mathcal{L}(mP)$, entonces, tenemos que $\mathcal{C}_m = ev_P(\mathcal{L}(mP))^{\perp} = \mathcal{C}_\Omega(D, mP)$ (ver definición 4.4.15).

Podemos dar la matriz de control si conocemos z_i, $\forall i \in W = \{w_1, w_2, \ldots, w_k\} \subseteq \mathbb{N}_0$:

$$H = \begin{pmatrix} z_{w_1}(P_1) & z_{w_1}(P_2) & \cdots & z_{w_1}(P_n) \\ z_{w_2}(P_1) & z_{w_2}(P_2) & \cdots & z_{w_2}(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ z_{w_k}(P_1) & z_{w_k}(P_2) & \cdots & z_{w_k}(P_n) \end{pmatrix}$$

Y en base la matriz de control, podemos usar álgebra lineal para calcular la matriz generatriz, usando la relación $GH^T = \mathbf{0}$ dada por la proposición 3.2.4.

5.3.2. Decodificación

En esta sección daremos las nociones fundamentales sobre como decodificar este tipo de códigos. En particular, estudiar las condiciones para las cuales es posible obtener una decodificación. Supongamos que el emisor transmite un mensaje codificado, $\mathbf{c} \in \mathcal{C}_W$, que llega al receptor como $\mathbf{y} = \mathbf{c} + \mathbf{e}$. Denotemos t' al número de posiciones no nulas del vector $\mathbf{e}$. Definimos el síndrome como:

Definición 5.3.2.8: El **Síndrome** de **órdenes** i, j de $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ es:

$$s_{ij} = \sum_{\ell=1}^{n} z_i(P_\ell) z_j(P_\ell) e_\ell$$

Definimos también:

$$s_k = \sum_{\ell=1}^{n} z_k(P_\ell) e_\ell$$

Así definidos, los síndromes definen una matriz, $S^{rr'} = (s_{ij})$, $0 \leq i \leq r$, $0 \leq j \leq r'$, de dimensiones $(r+1) \times (r'+1)$. Vemos por la definición, que $s_{ij} = s_{ji}$, por tanto, si $r = r'$, es una matriz simétrica. Tenemos que $H\mathbf{y}^t = H\mathbf{c}^t + H\mathbf{e}^t = 0 + (s_1, s_2, \ldots, s_k)^t$, que coincide con el síndrome tal como lo definimos en la sección 3 (definición 3.3.9).

Lema 5.1: Si $z_i, z_j \in \mathcal{C}_W$, y $k = i \oplus j$, entonces el síndrome s_{ij} se puede expresar como combinación lineal de síndromes s_ℓ, $0 \leq \ell \leq k$:

$$s_{ij} = a_k s_k + a_{k-1} s_{k-1} + \ldots + a_0 s_0 \tag{5.1}$$

Para los coeficientes $a_1, a_2, \ldots, a_k \in K$ tales que $z_i z_j = a_k z_k + \ldots + a_0 z_0$.

Demostración: Si $i \oplus j = k$ (recordando la definición 5.2.3), $z_i, z_j \in \mathcal{C}_W$ (recordemos que elegimos la base do modo que $v_P(z_i) = -\lambda_i$) entonces $z_i z_j \in \mathcal{C}_W$, con $v_P(z_i z_j) = v_P(z_i) + v_P(z_j) = -\lambda_i - \lambda_j = -\lambda_k$. Por tanto, $z_i z_j$ se puede expresar como combinación lineal de elementos de orden no superior a k; $z_i z_j = \sum_{i=0}^{k} a_i z_i$. Entonces, podemos escribir los síndromes como:

$$s_{ij} = \sum_{\ell=1}^{n} z_i(P_\ell) z_j(P_\ell) e_\ell = \sum_{\ell=1}^{n} (\sum_{s=0}^{k} a_s z_s(P_\ell) e_\ell) = \sum_{s=0}^{k} a_k \sum_{\ell=1}^{n} z_i(P_\ell) e_\ell = \sum_{s=0}^{k} a_k s_k.$$

□

Los síndromes dependen del vector de error $\mathbf{e}$, que es a priori desconocido.

Vamos a trabajar, al igual que hicimos en el capítulo anterior, con funciones localizadoras de errores (ver definición 4.4.16).

Proposición 5.3.2.4: Sea $f = z_r + a_{r-1} z_{r-1} + \ldots + a_0$, para ciertos $a_i \in K$, $z_i \in \mathcal{Z}$, y sea $S^{rr'}$ la matriz de síndromes del código. Entonces, si f es una función localizadora de errores, entonces, $(a_0, a_1, \ldots, a_r) S^{rr'} = \mathbf{0}$, para todo $r' > 0$. Como recíproco, se tiene que existe M, tal que si $(a_0, a_1, \ldots, a_r) S^{rr'} = \mathbf{0}$ para todo r' con $r \oplus r' \leq M$, entones, f es una función localizadora de errores.

Demostración: Empezamos por la primera afirmación, es decir, bajo la hipótesis que, $f = z_r + a_{r-1} z_{r-1} + \ldots + a_0$ es una función localizadora de errores, es decir, $e_k \neq 0 \Rightarrow f(P_k) = 0$. Computando el producto $(a_0, a_1, \ldots, a_r) S^{rr'} =$

$$(\sum_{i=0}^{r} a_i s_{i0}, \sum_{i=0}^{r} a_i s_{i1}, \ldots, \sum_{i=0}^{r} a_i s_{ir'}) = (\sum_{i=0}^{r} a_i \sum_{k=1}^{n} z_i(P_k) z_0(P_k) e_k, \ldots, \sum_{i=0}^{r} a_i \sum_{k=1}^{n} z_i(P_k) z_{r'}(P_k) e_k) =$$

$$(\sum_{k=1}^{n} z_0(P_k) e_k \sum_{i=0}^{r} a_i z_i(P_k), \ldots, \sum_{k=1}^{n} z_{r'}(P_k) e_k \sum_{i=0}^{r} a_i z_i(P_k)) = (\sum_{k=1}^{n} z_0(P_k) e_k f(P_k), \ldots, \sum_{k=1}^{n} z'_r(P_k) e_k f(P_k)) = \mathbf{0}$$

Pues si $e_k \neq 0$, por ser f función correctora de errores, $f(P_k) = 0$. Y si $f(P_k) \neq 0$, entonces $e_k = 0$. Una demostración del recíproco puede encontrarse en [11].

□

Por tanto, buscamos pares de valores de r y r' suficientemente grandes como para que el sistema $(x_0, \ldots, x_{r-1}, 1)S^{rr'} = \mathbf{0}$ tenga una solución no trivial. Notemos que, si $(x_0, \ldots, x_{r-1}, 1)S^{rr''} = \mathbf{0}$, entonces,

$$\forall r'' < r', \quad (x_0, \ldots, x_{r-1}, 1)S^{rr'} = \mathbf{0}.$$

Aún así, la matriz de síndromes no es conocida o, al menos, no todas sus entradas. Vamos a describir un proceso iterativo para calcular los síndromes s_k a partir de síndromes de órdenes inferiores. Explicamos, a continuación, como vamos a proceder:

Cálculo de los síndromes, sistema de votación:

Vamos trabajar, de iterada, sobre los elementos de Λ, en orden creciente. Supondremos conocidos los síndromes para valores pequeños, los s_{ij} con $i \oplus j < k$. Queremos calcular los s_{ij} con $i \oplus j = k$. Usando la ecuación 5.1, vemos que esto es equivalente a calcular s_k (ya que $s_0, s_1, \ldots, s_{k-1}$ los conocemos, por hipótesis).

- El caso más sencillo es en el cual $k \in W$. Escribiendo $\mathbf{e} = \mathbf{y} - \mathbf{c}$, y usando que, por definición de $\mathcal{C}_W$, $\mathbf{c}$ es ortogonal a $(z_k(P_1), z_k(P_2), \ldots, z_k(P_n)),\ k \in W$:

$$s_k = \sum_{\ell=1}^{n} z_k(P_\ell)e_\ell = \sum_{\ell=1}^{n} z_k(P_\ell)y_\ell - \sum_{\ell=1}^{n} z_k(P_\ell)c_\ell = \sum_{\ell=1}^{n} z_k(P_\ell)y_{\ell 0}.$$

  Como es $\mathbf{y}$ es conocido, podemos determinar en este caso el valor de s_k.

- Para determinar s_k, en el caso que $k \notin W$, usamos un sistema de votación.

  Definición 5.3.2.9: Los elementos i tales que $k \succeq_\Lambda i$ (definición 1.2.12) y para los cuales, los siguientes sistemas de ecuaciones,

$$\begin{aligned}(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,(k\ominus i)-1} &= \mathbf{0} \\ (y_0, y_1, \ldots, y_{k\ominus i}, 1)S^{k\ominus i,(i-1)} &= \mathbf{0}\end{aligned} \tag{5.2}$$

  tienen soluciones no triviales, son los **votantes**.

Lema 5.2: Sea i, $i \preccurlyeq k$, un votante, consideramos el valor:

$$\tilde{s}_{i,k\ominus i} = -\langle (s_{0,k\ominus i}, s_{1,k\ominus i}, \ldots, s_{i-1,k\ominus i}), (x_0, x_1, \ldots, x_{i-1})\rangle$$

Entonces, el valor anterior coincide con

$$\tilde{s}_{i,k\ominus i} = -\langle (s_{i0}, s_{i1}, \ldots, s_{i(j-1)}), (y_0, \ldots, y_{(k\ominus i)-1})\rangle.$$

Además, si $s_{i,k\ominus i} = \tilde{s}_{i,k\ominus i}$, entonces, $(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,k\ominus i} = \mathbf{0}$ y $(y_0, y_1, \ldots, y_{k\ominus(i-1)}, 1)S^{k\ominus i,i} = \mathbf{0}$. Si no se da la igualad, no hay funciones correctoras de errores de orden i ni j.

Demostración: Vemos primero que, las dos definiciones de $\tilde{s}_{i,k\ominus i}$, son equivalentes. Denotemos $j = k\ominus i$. Si se verifican los sistemas de ecuaciones 5.2, tenemos que $(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,j-1} = \mathbf{0}$ implica que $(s_{i0}, s_{i1}, \ldots, s_{i(j-1)}) = -(x_0, \ldots, x_{i-1})S^{i-1,j-1}$ (colocando a la derecha del s.e los términos en $\mathbf{x}$ y a la izquierda los términos independientes). Similarmente, obtenemos de $(y_0, y_1, \ldots, y_j, 1)S^{j,(i-1)} = \mathbf{0}$, que $(s_{0j}, s_{1j}, \ldots, s_{(i-1)j}) = -(y_0, \ldots, y_{j-1})S^{i-1,j-1}$. Entonces,

$$\begin{aligned}
-\tilde{s}_{i,j} &= \langle (s_{0,j}, s_{1,j}, \ldots, s_{i-1,j}), (x_0, x_1, \ldots, x_{i-1}) \rangle \\
&= \langle -(y_0, \ldots, y_{j-1})S^{i-1,j-1}, (x_0, x_1, \ldots, x_{i-1}) \rangle \\
&= -(y_0, \ldots, y_{j-1})S^{i-1,j-1}(x_0, x_1, \ldots, x_{i-1})^t \\
&= -(x_0, x_1, \ldots, x_{i-1})S^{j-1,i-1}(y_0, \ldots, y_{j-1})^t \\
&= \langle -(x_0, x_1, \ldots, x_{i-1})S^{j-1,i-1}, (y_0, \ldots, y_{j-1}) \rangle \\
&= \langle (s_{i0}, s_{i1}, \ldots, s_{i(j-1)}), (y_0, \ldots, y_{j-1}) \rangle
\end{aligned}$$

La igualdad central viene dada porque $s_{ij} = s_{ji}$.
Si para cierto i se da la igualdad $s_{i,k\ominus i} = \tilde{s}_{i,k\ominus i}$, veamos que $(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,k\ominus i} = \mathbf{0}$.

Puesto que,

$$0 = (x_0, \ldots, x_{i-1}, 1)S^{i,(k\ominus i)-1} = (x_0, \ldots, x_{i-1}, 1)S^{i-1,(k\ominus i)-1} + (s_{0,j}, s_{1,j}, \ldots, s_{i-1,j})$$

entonces:

$$\begin{aligned}
&(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,k\ominus i} = \\
&((x_0, x_1, \ldots, x_{i-1})S^{i-1,(k\ominus i)-1} + (s_{0,j}, s_{1,j}, \ldots, s_{i-1,j}), \langle (x_0, x_1, \ldots, x_{i-1}), (s_{i0}, s_{i1}, \ldots, s_{i(j-1)}) \rangle + s_{ij}) \\
&\qquad = (\mathbf{0}, -\tilde{s}_{ij} + s_{ij}) = \mathbf{0}.
\end{aligned}$$

Del mismo modo, y teniendo en cuenta que $s_{ij} = s_{ji}$, obtenemos que $(y_0, \ldots, y_{i-1}, 1)S^{k\ominus i,1} = \mathbf{0}$.

En caso que $s_{ij} \neq \tilde{s}_{ij}$, entonces tenemos que

$$(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,k\ominus i} = 0 \text{ y } (y_0, y_1, \ldots, y_{k\ominus(i-1)}, 1)S^{k\ominus i,i} = \mathbf{0}$$

no tienen soluciones no triviales. Por la proposición 5.2.2.3, eso significa no hay funciones localizadoras de errores e orden i ni j.

□

Definición 5.3.2.10: Podemos usar los lemas 5.1 y lema 5.2 para describir un **candidato,** $\tilde{s}_k$, a s_k, como $\tilde{s}_{i,k\ominus i} = a_k\tilde{s}_k + a_{k-1}s_{k-1} + \ldots + a_0a_0$ (con $a_0, \ldots, a_k$ tales que $z_iz_{k\ominus i} = a_kz_k + \ldots a_0z_0$) Por tanto, $\tilde{s}_k = \frac{\tilde{s}_{i,k\ominus i} - a_{k-1}s_{k-1} - \ldots + a_0a_0}{a_k}$.

Vemos que para diferentes valores de i, obtenemos, potencialmente, diferentes valores de $\tilde{s}_k$. En este caso, decimos que i vota al candidato $\tilde{s}_k$. El siguiente resultado nos da garantías sobre el proceso de votación.

Lema 5.3

- Si $i \in D(\lambda_i)$ (definición 1.2.12), y $i \notin \Delta_{\mathbf{e}} := \mathbb{N}_0 \setminus \{\rho(f) \mid f \text{ es localizadora de errores}\}$, $j := k \ominus i \notin \Delta_{\mathbf{e}}$, entonces i es un votante, y su voto coincide con s_k.
- Si un votante i vota a un candidato incorrecto, $\tilde{s}_k$, para s_k, entonces $i, j \in \Delta_{\mathbf{e}}$ ($j := k \ominus i$).
- Si $\nu_k > 2|D(\lambda_i) \cap \Delta_{\mathbf{e}}|$, entonces, la mayoría de los votantes votan al candidato correcto s_k. (ν_k definida en 1.2.12)

Demostración: Como dijimos antes, asumiremos que $\forall i, j \mid i \oplus j < k$, conocemos s_{ij}.

- Si $i, j \notin \Delta_{\mathbf{e}}$, entonces, existen funciones localizadoras de errores $f_1 = z_i + x_{i-1}z_{i-1} + \ldots + x_0z_0$ y $f_2 = z_j + y_{j-1}z_{j-1} + \ldots + y_0z_0$. Por la proposición 5.2.2.3, tenemos que $(x_0, x_1, \ldots, x_{i-1}, 1)S^{i,r'} = \mathbf{0}$, $\forall r' > 0$, y que $(y_0, y_1, \ldots, y_{j-1}, 1)S^{j,r'} = \mathbf{0}$, $\forall r' > 0$. En concreto, se verifican los sistemas de ecuaciones 5.2, que, junto con que $k \succeq i$, nos lleva a concluir que i es un votante. Además, por el lema 5.2, al haber funciones correctoras de errores de orden $\rho(f_1) = i$ y $\rho(f_2) = j$, no puede darse que $s_{ij} \neq \tilde{s}_{ij}$. Luego $s_{ij} = \tilde{s}_{ij} \Rightarrow \tilde{s}_k = s_k$.
- Si $s_k \neq \tilde{s}_k \Rightarrow s_{ij} \neq \tilde{s}_{ij}$. Entonces, por el lema 5.2, no hay funciones correctoras de errores de ordenes i ni j, es decir, $i, j \in \Delta_{\mathbf{e}}$
- Consideremos los conjuntos:

$$A = \{i \in D(\lambda_i) \mid i, k \ominus i \in \Delta_{\mathbf{e}}\}$$
$$B = \{i \in D(\lambda_i) \mid i \in \Delta_{\mathbf{e}}, k \ominus i \notin \Delta_{\mathbf{e}}\}$$
$$C = \{i \in D(\lambda_i) \mid i \notin \Delta_{\mathbf{e}}, k \ominus i \in \Delta_{\mathbf{e}}\}$$
$$D = \{i \in D(\lambda_i) \mid i, k \ominus i \notin \Delta_{\mathbf{e}}\}$$

  Por un lado, tenemos que, debido al segundo apartado, hay como mucho $|A|$ votos erróneos (de los $|A|$ votantes que se equivocan). Por otro lado, debido al primer apartado, los votos correctos son al menos $|D|$.
  Puesto que $\nu_k = |D(\lambda_i)|$, y A, B, C, D forman una partición disjunta de $D(\lambda_i)$, tenemos

que $\nu_k = |A| + |B| + |C| + |D|$. Además, $|D(\lambda_i) \cap \Delta_{\mathbf{e}}| = |A| + |B| = |A| + |C|$ (la última igualdad por simetría de i y $j = k \ominus i$). Que la mayoría de los votos sean correctos significa que $|D| - |A| > 0$ (más votos correctos que incorrectos), deducimos que esto ocurre si, $0 < |D| - |A| = \nu_k - |B| - |C| - 2|A| = 2 - |D(\lambda_i) \cap \Delta_{\mathbf{e}}| \Leftrightarrow |D(\lambda_i) \cap \Delta_{\mathbf{e}}| < \nu_k$

□

Como conclusión, tenemos que:

Teorema 5.3.2.5: Si $\nu_i > 2|D(\lambda_i) \cap \Delta_{\mathbf{e}}|$, para todo $i \notin W$, entonces $\mathbf{e}$ es corregible, en el código $\mathcal{C}_W$.

Demostración: Por el lema anterior, si $\nu_i > 2|D(\lambda_i) \cap \Delta_{\mathbf{e}}|$, para todo $i \notin W$, entonces es posible calcular, por el método de votación que hemos descrito, los síndromes s_k, y construir la matriz de síndromes $S^{rr'}$ para cualesquiera $r, r' > 0$. Buscamos un par (r, r') tal que $r \oplus r'$ es suficientemente grande para que $(a_0, \ldots, a_r)S^{rr'} = 0$ tenga una solución no trivial, ya que, la solución de este sistema nos proporciona una función localizadora de errores, f, para $\mathbf{e}$ (y ahora lo podemos resolver, pues conocemos el valor de $S^{rr'}$). Con la función f, conocemos el conjunto $J(f) = \{i \in \mathbf{N} \mid f(P_i)\} = 0$, finito, pues f no puede tener una cantidad infinita de ceros (salvo $f = 0$). Podemos plantear el sistema en $\mathbf{x}$, que discutimos en el apartado 3.5:

$$\begin{cases} s(\mathbf{x}) = H\mathbf{x}^t = s(\mathbf{e}) \\ x_i = 0, \quad \forall i \in J(f) \end{cases} \tag{5.3}$$

Luego se puede obtener, $\mathbf{e}$ y recuperar $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

□

5.4. Cotas inferiores para la distancia mínima y pesos de Hamming

En esta sección trataremos de dar una cota inferir para la para distancia mínima de los códigos en un punto. En particular, tratamos con códigos clásicos, de la forma $\mathcal{C}_m$ (definición 5.2.1.4). Una de las cotas más conocidas es la llamada cota de *Goppa*. Para el código $\mathcal{C}_m$, tenemos que:

$$d(\mathcal{C}_m) \geq m + 2 - 2g$$

Esta cota resulta de aplicar la proposición 4.4.8 al código $\mathcal{C}_m$. Como indicamos en el capítulo 4, no se conoce una expresión para distancia mínima, pero podemos dar una inferior que se ajuste más. Vamos a usar el concepto de distancia de Feng-Rao con este fin. Así mismo, veremos como también se puede usar como una cota inferior para las pesos de Hamming

generalizados. Por tantp, la distancia de Feng-Rao será útil tanto en el estudio de códigos, como al problema de "wire-tap channel II".

Distancia de Feng-Rao generalizada y números de Feng-Rao

Empezamos definiendo la distancia de Feng-Rao que, como veremos, es una mejora sobre la cota anterior para la distancia mínima.

Definición 5.4.11: Sea Λ un semigrupo numérico (no necesariamente el semigrupo de Wierstrass asociado a una curva en un punto) y sea $m \in \mathbb{N}_0$. Entonces,

$$\delta_{FR}(m) = min_{\nu_i \in \nu}\{\nu_i \mid \lambda_i > \lambda_m, \lambda_i \in \Lambda\}$$

se denomina **distancia de Feng-Rao** del semigrupo.

En algunos textos se usa la definición $\delta_{FR}(m) = min_{\nu_i \in \nu}\{\nu_i \mid \lambda_i \geq \lambda_m, \lambda_i \in \Lambda\}$, en cuyo caso los resultados que vamos a discutir a continuación son ligeramente diferentes.

Proposición 5.4.6: Sea Λ un semigrupo numérico y $m \in \mathbb{N}_0$. Consideremos el conjunto, F_m, asociado al semigrupo Λ (no confundir con $D(\lambda_i)$, descrito en definición 1.2.12),

$$F_m = \{(x, y) \in \mathbb{N}_0^2 \mid x, y \text{ son lagunas de } \Lambda \text{ y } x + y = \lambda_m\}.$$

Sea $\delta_{FR}(m)$ la distancia de Feng-Rao del semigrupo. Denotamos además, por $g(\lambda_i)$, $i \in \mathbb{N}_0$ al número de lagunas menores que λ_i (Donde si $\lambda_i > c - 1$, entonces $g(\lambda_i) = g$). Tenemos el siguiente resultado:

- Para todo $m \in \mathbb{N}_0$, $\nu_m = \lambda_m + 1 - 2g(\lambda_m) + F_m$. En caso que $\lambda_m \geq c$, (siendo c el conductor del semigrupo), tenemos que $\nu_m = \lambda_m + 1 - 2g + F_m$.
- También tenemos que $\nu_m = m + 1 - g(\lambda_m) + |F_m|$.
- $\delta_{FR}(m) \geq \lambda_m + 1 - 2g$ (equivalentemente, $\delta_{FR}(m) \geq m + 1 - g$), para todo $\lambda_m \geq c$. Además, la igualdad se da cuando $\lambda_m > 2c - 2$.

Demostración:

- Consideremos los siguientes conjuntos,

$$A_m = \{(x, y) \in \mathbb{N}_0 \mid x + y = \lambda_m\}$$
$$B_m = \{(x, y) \in A_m \mid x \text{ es una laguna de } \Lambda\}$$
$$C_m = \{(x, y) \in A_m \mid y \text{ es una laguna de } \Lambda\}$$
$$D_m = \{(x, y) \in \Lambda^2 \mid x + y \in \Lambda\}$$

Claramente, $F_m = B_m \cap C_m$, y $A_m = D_m \cup B_m \cup C_m$ (Notemos, con la definición 2.10, $|D(\lambda_m)| = |\{s \in \Lambda \mid \lambda_m - s \in \Lambda\}| = |\{(s_1, s_2) \in \Lambda^2 \mid s_1 + s_2 = \lambda_m\}| = |D_m|$). Además, $D_m \cap (B_m \cup C_m) = \emptyset$. Por tanto,

$$\nu_m = |D(\lambda_m)| = |D_m| = |A_m| - |B_m \cup C_m| =$$
$$|A_m| - |B_m| - |C_m| + |B_m \cap C_m| = |A_m| - |B_m| - |C_m| + |F_m|.$$

Hay $\lambda_m + 1$ pares $(x, y) \in \mathbb{N}_0$ tales que, $x + y = \lambda_m$, luego $|A_m| = \lambda_m + 1$. La simetría en la definición de B_m y C_m conlleva que $|B_m| = |C_m|$. Además, si $x \leq \lambda_m$ es una laguna de Λ, entonces $y = \lambda - x \in \mathbb{N}_0 \Rightarrow (x, y) \in B_m$. Recíprocamente, si $(x, y) \in B_m$, entonces x es una laguna, con $x \leq \lambda_m$. Puesto que hay $g(\lambda_m)$ lagunas menores o iguales que λ_m, (por hipótesis, $\lambda_m \geq c$), tenemos que, $|B_r| = g(\lambda_m)$. Luego $\nu_m = \lambda_m + 1 - 2g(\lambda_m) + |F_m|$. Y como hemos dicho, si $\lambda_m \geq c$, $g(\lambda_m) = g$.

- Vemos que $\lambda_m = m + g(\lambda_m)$. Efectivamente, λ_m es el elemento $m + 1$ del semigrupo y, en los naturales, contando las $g(\lambda_m)$ lagunas, es el elemento $m + 1 + g(i)$ elemento de $\mathbb{N}_0$, es decir, $\lambda_m = m + g(\lambda_m)$. Por tanto, usando el apartado anterior, $\nu_m = \lambda_m + 1 - 2g(\lambda_m) + F_m = m + g(\lambda_m) + 1 - 2g(\lambda_m) + F_m = m + 1 - g(\lambda_m) + F_m$.

- Si $\lambda_m \geq c$, $\nu_m = \lambda_m + 1 - 2g + |F_m| \geq \lambda_m + 1 - 2g$, por el apartado anterior. Por tanto, $\delta_{FR}(m) = min_{\lambda_i > \lambda_m}\{\nu_i\} \geq min_{\lambda_i > \lambda_m}\{\lambda_i + 1 - 2g\} = min_{\lambda_i > \lambda_m}\{\lambda_i\} - 2g + 1 \geq \lambda_m + 1 - 2g$. Además, para $\lambda_m \geq 2c - 2$, supongamos que existen, x, y, lagunas tales que, $x + y = \lambda_m$. Entonces, $x + y = \lambda_m > 2c - 2$, pero $c - 1$ es la mayor de las lagunas de S, luego no existen tales x, y. Usando el segundo apartado, tenemos le resultado $\delta_{FR}(m) \geq m + 1 - g$.

□

Como dijimos en al capítulo 4, es habitual trabajar con códigos AG que verifican que $m = deg(G) > 2g - 2$, o equivalentemente, $m \geq c \Rightarrow \lambda_m > 2c - 2$, luego podremos aplicar este resultado.

Como consecuencia de la proposición, tenemos que:

$$\delta_{FR}(m + 1) \geq (m + 1) - g + 1 \geq m - 2g + 2.$$

Además, en el teorema 2.5 de [14], demuestra que, para todo $m \in \mathbb{N}_0$, $d(C_m) \geq \delta_F R(m)$, luego tenemos:

$$d(C_m) \geq \delta_{FR}(m + 1) \geq m - 2g + 2.$$

Con la cota que acabamos de ver para $\delta_{FR}(m)$ ya tenemos una para la distancia mínima, más ajustada que la dada por la proposición 4.4.8. Además, si conocemos una forma de computar la distancia de Feng-Rao, podemos dar una aproximación más refinada. Aquí, vamos

a generalizar $\delta_{FR}(m)$, que nos da una mejor cota inferior, no solo para la distancia mínima del código, pero también para el peso de Hamming generalizado:

Definición 5.4.12: Sea Λ un semigrupo, y $\lambda_m, s_1, s_2, \ldots, s_r \in \Lambda$, entonces:

- Definimos $D(s_1, s_2, \ldots, s_r) = D(s_1) \cup D(s_2) \cup \ldots \cup D(s_r) = \{s \in \Lambda \mid s_i - s \in \Lambda \text{ para algún } i = 1, 2, \ldots, r\}$.
- Y, en base a lo anterior, definimos $\nu_{s_1,\ldots,s_r} = |D(s_1, \ldots, s_r)|$.
- La **distancia r-ésima de Feng-Rao** se define como:

$$\delta^r_{FR}(m) = min\{\nu_{s_1,\ldots,s_r} \mid \lambda_m \leq s_1 < \ldots < s_r, s_i \in \Lambda\}.$$

Vemos que, para $r = 1$, $\delta^1_{FR}(m) = \delta_{FR}(m)$.

A continuación, veremos como podemos obtener resultados similares a los de la proposición 5.3.5, para acotar la distancia mínima.

Teorema 5.4.7: Sea Λ un semigrupo numérico, con género g y conductor c. Sea también $r \geq 2$, entonces existe una constante $E_r = E(\Lambda, r)$ tal que para todo $\lambda_m \geq 2c - 2$ tenemos que:

$$\delta^r_{FR}(m) = m + 1 - g + E_r$$

Demostración Sea $\Lambda \ni s_1 \geq \lambda_m$ y sea $k_i > 0$ para $i = 1, 2, \ldots, r-1$ tal qué $\Lambda \ni s_{i+1} = s_i + k_i, \quad \forall i \in \{1, 2, \ldots, r-1\}$. Denotamos $\mathbf{k} = (k_1, k_2, \ldots, k_{r-1})$. Para $h \in \{1, 2, \ldots, r-1\}$, definimos (para $\mathbf{k}$ fijo):

$$\gamma_{\mathbf{k}} = \left|\left\{\rho \in \mathbb{N}_0 \setminus \Lambda \;\middle|\; \rho + \sum_{i=1}^{j} k_i \in \Lambda \text{ para cierto } j = 1, 2 \ldots, r-1\right\}\right|$$

$$\mu^h_{\mathbf{k}} = \left|\left\{l \in [1, k_h] \;\middle|\; -l + \sum_{i=h}^{j} k_i \in \Lambda \text{ para cierto } j = h, h+1, \ldots, r-1\right\}\right|$$

Vemos que $\gamma_{\mathbf{k}}$ no depende de s_1, además, tenemos las siguientes **afirmaciones**:

- Para $s_1 \geq 2c - 1$, es el número de enteros en el intervalo $[0, s_1]$ que no pertenecen a $D(s_1)$, pero pertenecen a $D(s_j)$ para $j \geq 2$.
- Por otro lado, si $s_1 \geq c$, entonces $\mu^h_{\mathbf{k}}$ es el número de elementos de $D(s_1, s_2 \ldots, s_r)$ en el intervalo $[s_h + 1, s_{h+1}]$.

Demostremos lo anterior:

- Demostremos la primera afirmación. Denotamos $\overline{\gamma_{\mathbf{k}}}$ al conjunto para el cual hemos definido $\gamma_{\mathbf{k}}$ como su cardinal.
  Sea $s \in [0, s_1]$ tal que existe $j \geq 2$ tal que $s \in D(s_j)$ y $s \notin D(s_1)$. Entonces, para dicho j, $s_j - s \in \Lambda \Rightarrow s_1 + \sum_{i=1}^{j} k_i - s \in \Lambda$. Como $s \notin D(s_1)$ y $s_1 - s \geq 0$ tenemos que $\rho := s_1 - s \notin \Lambda$. Por tanto, $\rho \in \overline{\gamma_{\mathbf{k}}}$.
  Recíprocamente, si $\rho \in \overline{\gamma_{\mathbf{k}}}$, definimos $s := s_1 - \rho \in [0, s_1]$, ya que, por hipótesis, $s_1 \geq 2c-1$, y ρ es una laguna (es decir, $\rho \leq g \leq c$). En particular, si $g \geq 1$, tenemos que $s_1 - \rho \geq 2c - 1 - g \geq c$, luego $s_1 - \rho \in \Lambda$ (si $g = 0$ $\gamma_{\mathbf{k}} = 0$). Existe $j \in \{1, 2, \ldots, r-1\}$ tal que $\rho + \sum_{i=1}^{j} k_i \in \Lambda$. Para dicho j:

$$s_{j+1} - s = s_1 + \sum_{i=1}^{j} k_i - s_1 + \rho = \rho + \sum_{i=1}^{j} k_i \in \Lambda$$

  Luego $s \in D(s_{j+1})$. Pero $s_1 - s = s_1 - s_1 + \rho = \rho \notin \Lambda \Rightarrow s \notin D(s_1)$. Por tanto, tenemos una biyección entre $\overline{\gamma_{\mathbf{k}}}$ y los enteros en el intervalo $[0, s_1]$ que no pertenecen a $D(s_1)$, pero pertenecen a $D(s_j)$ para $j \geq 2$, y por tanto el cardinal de ambos conjuntos es el mismo.

- Veamos la segunda afirmación. Denotemos $\overline{\mu_{\mathbf{k}}^h}$ al conjunto del cual $\mu_{\mathbf{k}}^h$ es el cardinal:
  Por un lado, consideremos $s \in [s_h + 1, s_{h+1}]$ tal que $s \in D(s_1, s_2, \ldots, s_r)$. Entonces, consideremos $l := s - s_h$. Tenemos que $l \in [s_h + 1 - s_h, s_{h+1} - s_h] = [1, k_h]$. Además, como $s \in D(s_1, s_2, \ldots, s_r)$, existe s_j tal que $s_j - s \in \Lambda$, donde $s_j > s$. Por lo tanto, para dicho j,

$$-l + \sum_{i=h}^{j} k_i = s_h - s + \sum_{i=h}^{j} k_i = s_j - s \in \Lambda$$

  Luego $l \in \overline{\mu_{\mathbf{k}}^h}$. Recíprocamente, tenemos que si $l \in \overline{\mu_{\mathbf{k}}^h}$, $s := l + s_h \in [s_h + 1, s_{h+1}]$, y para cierto $h \leq j \leq r-1$ tenemos que $-l + \sum_{i=h}^{j} k_i \in \Lambda$. Para dicho j, $s_j - s = s_j - l - s_h = s_h + \sum_{i=h}^{j} k_i - l - s_h = -l + \sum_{i=h}^{j} k_i \in \Lambda$. Por tanto, $s \in D(s_j) \Rightarrow s \in D(s_1, s_2, \ldots, s_r)$. Por tanto, hay una biyección entre $\overline{\mu_{\mathbf{k}}^h}$ y los elementos de $D(s_1, s_2 \ldots, s_r)$ en el intervalo $[s_h + 1, s_{h+1}]$, dada por $f_h(l) = s_h + l$. Luego ambos conjuntos tienen el mismo número de elementos.

Por tanto, si $s_1 \geq \lambda_m \geq 2c - 1$:

1. $\sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h$ es el número de elementos de $D(s_1, \ldots, s_r)$ en $[s_1 + 1, s_r]$
2. $\gamma_{\mathbf{k}}$ es el número de elementos de $D(s_1, \ldots, s_r) \setminus D(s_1)$ en $[0, s_1 + 1)$
3. ν_{s-1} es el número de elementos de $D(s_1)$ en $[0, s_1 + 1)$

Juntando lo anterior:

$$\nu_{s_1,s_2,\ldots,s_r} = \nu_{s_1} + \gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h$$

Y, por tanto, dado que ni ν_{s_1} depende de $\mathbf{k}$, ni $\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h$ depende de m_1, para calcular la distancia de Feng-Rao generalizada es suficiente con calcular, de forma independiente, el mínimo de ambas cantidades. Por tanto (aplicando la proposición 5.3.5), obtenemos que:

$$\delta_{FR}^r(m) = min\{\nu_{s_1,\ldots,s_r}\} = min\{\nu_{s_1}\} + min\{\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h\} = m + 1 - g + E(\Lambda, r),$$

Donde $E(\Lambda, r) = min\{\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h \mid k_i > 0,\ \forall i\}$

□

Definición 5.4.13: Para $r \geq 2$, denominaremos **número de Feng-Rao r-ésimo** del semigrupo Λ a la constante $E_r(\Lambda, r)$, que hemos tratado en el teorema anterior.

Proposición 5.4.8: Sea Λ un semigrupo de género $g > 0$, y sea $r \geq 2$. Entonces:

$$r \leq E(\Lambda, r) \leq \lambda_{r-1}$$

Además, si $r \geq c$, entonces $E(\Lambda, r) = \lambda_{r-1} = r + g - 1$.

Demostración: La primera desigualdad es consecuencia de que hay al menos r elementos $(0, s_2, s_3, \ldots, s_r)$ en $D(s_1, \ldots, s_r) \setminus D(s_1)$ en el intervalo $[0, s_r]$. Por tanto (recordado la demostración del teorema anterior) $min\{\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h \mid k_i > 0,\ \forall i\} \geq r$.
Demostremos la otra desigualdad. Primero, veamos que, para $i = 0, 1, \ldots, r-1$ tenemos que $D(\lambda_m + \lambda_{r-1} - \lambda_i) \subseteq D(\lambda_m + \lambda_{r-1})$. Por definición $x \in D(\lambda_m + \lambda_{r-1} - \lambda_i) \Rightarrow a := \lambda_m + \lambda_{r-1} - \lambda_i - x \in \Lambda$ por tanto, $a + \lambda_i \in \Lambda \Rightarrow \lambda_m + \lambda_{r-1} - x \in \Lambda \Rightarrow x \in D(\lambda_m + \lambda_{r-1})$. Aplicando lo anterior, tenemos que $D(\lambda_m + \lambda_r - \lambda_0, \ldots, \lambda_m + \lambda_r - \lambda_{r-1}) \subseteq D(\lambda_m + \lambda_{r-1})$. Aplicando la definición, tenemos que si $\lambda_m \geq c$, entonces $\delta_{FR}^r(m) \leq \nu_{\lambda_m + \lambda_{r-1}}$; donde, por la proposición 5.3.5, $\nu_{\lambda_m + \lambda_{r-1}} = \lambda_m + \lambda_{r-1} + 1 - 2g$ cuando $\lambda_m + \lambda_{r-1} \geq 2c - 1$. Aplicando el teorema 5.3.6,

$$\delta_{FR}^r(m) = m + 1 - 2g + E(\Lambda, r) \leq \lambda_m + \lambda_{r-1} + 1 - 2g \Rightarrow E(\Lambda, r) \leq \lambda_{r-1}).$$

Finalmente, si $r \geq c$, entonces $\forall \rho \in \mathbb{N}_0 \setminus \Lambda$ y $\forall \mathbf{k} \in \mathbb{N}_{>0}^r$ tenemos que, $\rho + \sum_{i=1}^{r-1} k_i \geq \rho + (r-1) \geq r \in \Lambda$ luego todas las lagunas pertenecen a $\overline{\gamma_{\mathbf{k}}} \Rightarrow \gamma_{\mathbf{k}} = g$. Concluimos que:

$$E(\Lambda, r) = g + min\Big\{ \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h \;\Big|\; k_i > 0,\ \ \forall i \Big\} = g + r - 1,$$

Pues en este caso, se alcanza el mínimo cuando $1 = k_1 = k_2 = \cdots = k_{r-1}$.

□

Notas:

1. Dado que $E(\Lambda, r) = \lambda_{r-1} = r + g - 1$, para $r \geq c$, implica que, para valore altos de r, el valor del número de Feng-Rao r-ésimo solo depende de las lagunas del semigrupo, y no de su distribución.

2. En general, para la cota $E(\Lambda, r) \leq \lambda_{r-1}$, no se da la igualdad.

3. Es posible calcular, en tiempo finito el valor de la constante $E(\Lambda, r)$. Al trabajar con códigos códigos correctores, se trabaja con $r \leq k$ (donde k es la dimensión del código).

4. De hecho, puesto que $D(\lambda_m) \subseteq D(\lambda_m + s), \quad \forall s \in \Lambda$, tenemos que, para $\{s'_i\}_{i=1}^{r}$ con $1 \leq k_i \leq \lambda_1,\ s'_{i+1} = s'_i + k_i$, entonces $D(s'_1, \ldots, s'_r) \subseteq D(s_1, \ldots, s_r)$. En cuyo caso, hay λ_1^{r-1} en el conjunto $\{\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu_{\mathbf{k}}^h \mid k_i > 0,\ \forall i\}$, del cual hay que calcular el mínimo (ver "remark 6" de [5]).

5. Par el caso particular $r = 2$, la formula queda simplificada:

$$E(\Lambda, 2) = min\{\gamma_k + \mu_k \mid 1 \leq k \leq \lambda_1\}$$

Donde $\gamma_k = |\{\rho \notin \Lambda \mid \rho + k \in \Lambda\}|$ y $\mu_k = |\Lambda \cap [0, k-1]| = 1$ (con $k \leq \lambda_1$). Por tanto:

$$E(\Lambda, 2) = 1 + min\{\gamma_k \mid 1 \leq k \leq \lambda_1\}$$

Ejemplo 5.4.4:

Consideremos Λ, el semigrupo $\langle 2, 3\rangle$, (llamado elíptico). Entonces, $E(\Lambda, 2) = 1 + min\{\gamma_k \mid 1 \leq k \leq 2\}$, con,

$$\gamma_1 = |\{\rho \notin \Lambda \mid \rho + 1 \in \Lambda\}| = |\{1\}| = 1, \quad \gamma_2 = |\{\rho \notin \Lambda \mid \rho + 2 \in \Lambda\}| = |\{1\}| = 1$$

Por tanto, $E(\Lambda, 2) = 2$, y $\delta_{FR}^2(m) = \lambda_m + 3 - 2g$ para $\lambda_m \geq 2c - 1$.

Teorema 5.4.9: Sea Λ un semigrupo con género g y conductor c. Sea $r \geq 2$. Entonces, para todo $\lambda_m \geq c$, tenemos que:

$$\delta_{FR}^r(m) \geq \lambda_m + 1 - 2g + E(\Lambda, r)$$

Demostración: El teorema 5.3.6 trata el caso $\lambda_m \geq 2c - 1$, donde vimos que se da la igualad. Para el caso $c \leq \lambda_m \leq 2c - 1$, usamos el mismo método para contar que usamos en la demostración de dicho teorema, excepto que debemos considerar:

$$\gamma'_{\mathbf{k}}(s_1) = \Big|\Big\{s \in S \;\Big|\; s_1 - s \notin S, \text{ pero } s_1 - s + \sum_{i=1}^{j} k_i \in S \text{ para cierto } j = 1, 2, \ldots, r-1\Big\}\Big|.$$

Vemos que, por cómo esta definido $\gamma'_{\mathbf{k}}(s_1)$, es el número de elementos del conjunto $D(s_1, s_2, \ldots, s_r)\backslash D(s_1)$ en el intervalo $[0, s_1]$.
Así mismo, y puesto que $\nu_1 \geq c$, tenemos que $\nu_{s_1} = s_1+1-2g+F(s_1)$ (Por la proposición 5.3.5).

Denotemos por $\overline{\gamma'_{\mathbf{k}}}$ al conjunto para le cual hemos definido $\overline{\gamma_{\mathbf{k}}}$ como su cardinal. Si ρ es un elemento de $\overline{\gamma_{\mathbf{k}}}$, pero tal que $s := s_1-\rho \notin \overline{\gamma'_{\mathbf{k}}}$, entonces (recordando la demostración del teorema 5.3.6), tiene que suceder que $s \notin S$ (ya que, como vimos, $s_1-s \notin S$ y $s_1-s+\sum_{i=1}^{j} k_i \in S$ para cierto j, si $s_1-\rho \geq 0$, $\rho \in \overline{\gamma_{\mathbf{k}}}$). Por tanto, $s_1 = \rho + s$, donde ρ y s son lagunas y, así, tenemos que, $(s, \rho) \in F(s_1)$. Por tanto, $F(s_1) + \gamma'_{\mathbf{k}} \geq \gamma_{\mathbf{k}}$. Juntando todo lo anterior, concluimos,

$$\nu_{s_1,s_2,\ldots,s_r} = s_1 + 1 - 2g + F(s_1) + \gamma'_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}} \geq s_1 + 1 - 2g + \gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}}.$$

Aplicando la definición de $\delta^r_{FR}(m)$, y calculando los mínimos de forma separada (como hicimos en el teorema 5.3.6) obtenemos el resultado.

□

Pesos de Hamming Generalizados:

Recordamos, que en la sección 3.8.14, introdujimos el concepto de peso de Hamming generalizado. En esta sección, vamos a discutir cotas inferiores para dicho peso, basadas en la distancia de Feng-Rao, y la distancia de Feng-Rao generalizada. Aunque el cálculo de las anteriores no es trivial, es en general, más sencillo que el cálculo del peso de Hamming generalizado, cuyo coste computacional es alto.

Lema 5.4 Si $\mathcal{C}'$ es un subcódigo lineal de $\mathcal{C}$, y tiene a lo sumo, co-dimensión v en C, entonces $d_{u+v}(\mathcal{C}) \geq d_u(\mathcal{C}')$.

Demostración: Sea $\mathcal{D}$ un código, subespacio vectorial de $\mathcal{C}$, de dimensión $u + v$; tal que $|sop(\mathcal{D})| = d_{u+v}(\mathcal{C})$ (es decir, en $\mathcal{D}$ se alcanza el mínimo de la definición de d_r). Sea $\mathcal{D}' := \mathcal{D} \cap \mathcal{C}'$, entonces, $dim(\mathcal{D}') \geq u$, al tener $\mathcal{C}'$ a lo sumo, co-dimensión v en $\mathcal{C}$. Por tanto, $|sop(\mathcal{D}')| \geq d_u(\mathcal{C}')$. Como el soporte de $\mathcal{D}'$ está contenido en el soporte de $\mathcal{D}$, tenemos que, $d_{u+v}(\mathcal{C}) \geq d_u(\mathcal{C}')$.

□

Teorema 5.5.10: Sea $\mathcal{C}_s$ el código AG clásico en un punto, P (ver definición 5.2.1.4), tenemos que $d_r(\mathcal{C}_s) \geq \delta_{FR}(r + s - 1)$, para todo $r, s \in \mathbb{N}_{>0}$.

Demostración: Sea $\mathcal{C} = \mathcal{C}_s$ y $\mathcal{C}' = \mathcal{C}_{r+s-1}$, entonces, C' es un subcódigo de C, y tiene

co-dimensión a lo sumo $r-1$ en C. Aplicando el lema 5.4, con $u=1$ y $v=r-1$, obtenemos que:

$$d_r(\mathcal{C}_s) \geq d_1(\mathcal{C}_{s+r-1}),$$

Y como indicamos en los comentarios, tras la proposición 5.3.5, $d_1(\mathcal{C}_{s+r-1}) = d(\mathcal{C}_{s+r-1}) \geq \delta_{FR}(r+s-1)$.

□

Obtenemos así, una relación entre la distancia de Feng-Rao y los pesos de Hamming generalizados. El siguiente resultado, que no demostraremos (ver teorema 3.14 [15]), nos da una cota basada en la distancia generalizada.

Teorema 5.5.11: Sea $\mathcal{C}_m$ un código clásico en un punto. Entonces:

$$d_r(\mathcal{C}_m) \geq \delta^r_{FR}(m)$$

Así, con las dos últimas proposiciones, hemos obtenido dos cotas inferiores, que nos permiten aproximar los valores de los pesos de Hamming generalizados. Como hemos tratado en la sección 3.8, esto tiene aplicaciones directas al problema "Wire-Tap Channel II". En virtud del teorema 3.8.13, podemos, para un nivel de información seleccionado (Δ), saber la cantidad de bits a los que el espía debe tener acceso para obtener ese nivel de información. Dicha estimación requiere poder calcular los valores de pesos de Hamming generalizados. Si esto no fuera posible, es posible usar la cota dada por los teoremas 5.5.11 y 5.5.10.

Bibliografía

[1] L. H. Ozarow y A. D. Wyner. "Wire-Tap Channel II". En: (1984).

[2] P.A. García-Sánchez Abdallah Assi Marco D'Anna. *Numerical semigroups and applications*. Springer, 2020. Cap. Chapter 3, Ideals.

[3] Maria Bras-Amorós. "Ideals of Numerical Semigroups and Error-Correcting Codes". En: *Symmetry* (2019).

[4] Maria Bras-Amorós. *Numerical Semigroups and Codes*. E. Martinez-Moro, 2013. Cap. Chapter 5 of Algebraic Geometry Modeling in Information Theory.

[5] J.I. Farrán y C. Munuera. "Goppa-like bounds for the generalized Feng–Rao distances". En: (2003).

[6] Prof. Dr. Wolfram Decker. *Commutative Algebra*. Cap. 2, Corollary 2.3.6.

[7] Manuel Delgado y Pedro A. Garcia-Sanchez y Jose Morais. *NumericalSgps, a GAP package for numerical semigrups*. URL: https://github.com/gap-packages/numericalsgps.

[8] William Fulton. *Algebraic Curves, An Introduction to Algebraic Geometry*. 2008.

[9] P.A. García-Sánchez J.C. Rosales. *Numerical Semigroups*. Vol. 20. Springer, 2009.

[10] Carlos Munuera y Juan Tena. *Codificación de Información*.

[11] Michael E. O'Sullivan Maria Bras-Amorós. "The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting". En: *Springer-Verlag* (2006).

[12] Carlos Munuera. "On the Generalized Hamming Weights of Geometric Goppa Codes". En: *IEEE Transactions Information Theory, vol. 40, NO. 6* (1994).

[13] Jorge Angulo Rodriguez. *Repositorio, código de semigrupos, TFG informática*. URL: https://github.com/Ataraxta/TFG-informatica.

[14] Christoph Kirfel y Ruud Pellikaan. "The minimum distance of codes in an array coming from telescopic semigroups". En: *IEEE Transactions Information Theory, vol. 41* (1995).

[15] Petra Heijnen y Ruud Pellikaan. "Generalized Hamming weights of q-ary Reed-Muller codes". En: (1998).

[16] Jacobus H. van Lint Tom Høholdt y Ruud Pellikaan. *Algebraic geometry codes*. 2011.ª ed. 1998.

[17] Victor K. Wei. “Generalized Hamming Weights for Linear Codes”. En: (1991).