Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Polinomios linealizados y códigos de Gabidulin

Autor: Ángela de Arriba Martín

Tutor: Umberto Martínez Peñas

Año: 2025

Índice general

Resumen: El trabajo tiene como objetivo principal el estudio de los polinomios linealizados y de los códigos de Gabidulin. Comienza sentando la base algebraica, profundizando en la estructura y propiedades de los cuerpos finitos y continuando con una introducción a los códigos lineales, en la que además se relaciona ambas partes entre sí. Después, se introducen los polinomios linealizados abordando sus propiedades algebraicas y se explica en profundidad la métrica del rango. Todo ello es esencial para definir los códigos de Gabidulin, basados en la evaluación de polinomios linealizados en la métrica del rango. Por último, se exponen dos algoritmos para la descodificación de estos particulares códigos y se adjunta un análisis de su complejidad computacional.

Palabras clave: cuerpo finito, código lineal, polinomio linealizado, métrica del rango, código de Gabidulin, descodificación, reconstrucción.

Abstract: The aim of this project is to study linearized polynomials and Gabidulin codes. It begins by establishing the algebraic foundations, exploring the structure and properties of finite fields, and proceeds with an introduction to linear codes, highlighting their connection to the underlying algebraic structures. Then, linearized polynomials are introduced, focusing on their algebraic properties, and the rank metric is explained in detail. These elements are essential for the definition of Gabidulin codes, which are based on the evaluation of linearized polynomials under the rank metric. Finally, two decoding algorithms for these specific codes are presented, along with an analysis of their computational complexity.

Key words: finite field, linear code, linearized polynomial, rank metric, Gabidulin code, decoding, reconstruction.

Introducción

Los códigos en métrica de rango han sido objeto de estudio creciente a lo largo de las últimas décadas, tanto desde una perspectiva teórica como aplicada. En gran medida se debe a sus prometedoras aplicaciones en áreas como la codificación de redes (network coding), la criptografía, la codificación espacio-temporal y el almacenamiento distribuido tolerante a fallos. Estas aplicaciones aprovechan la capacidad de los códigos en la métrica de rango para detectar y corregir errores que afectan a subespacios, en lugar de posiciones individuales, lo que los hace especialmente eficaces en escenarios donde los errores están altamente correlacionados, como en transmisiones por redes o en memorias distribuidas.

Desde el punto de vista histórico, la métrica de rango fue introducida por Delsarte en los años 70 en su estudio de las formas bilineales sobre cuerpos finitos y sus aplicaciones en teoría de códigos ([1]). Posteriormente, Gabidulin propuso en 1985 una familia de códigos lineales construidos a partir de polinomios linealizados, que equivalen a los códigos de Reed–Solomon a la métrica de rango ([2]). Roth amplió el marco teórico en los años 90, aportando nuevas herramientas algebraicas para el análisis y la decodificación de estos códigos ([11]). Los códigos que surgieron de estos trabajos, que se conocen hoy en día como códigos de Gabidulin, se caracterizan por alcanzar la cota de Singleton en métrica de rango, lo cual los convierte en códigos óptimos en términos de distancia.

En cuanto a la distribución de este trabajo, se comienza estableciendo un marco teórico a través de un primer capítulo de preliminares. En él se presenta la estructura de los cuerpos finitos, $\mathbb{F}_q$, garantizando su existencia y unicidad, así como las propiedades relevantes de las raíces de polinomios en $\mathbb{F}_q[x]$. A continuación, se definen los códigos lineales, se introduce la distancia de Hamming y se describen los parámetros fundamentales de un código. Se incluye también la representación mediante matrices generadora y de control, el concepto de código dual, y el procedimiento general de decodificación. Finalmente, se introduce la cota de Singleton para la distancia mínima, lo que motiva la definición de códigos MDS, entre los cuales destacan los códigos de Reed-Solomon por su relevancia teórica y práctica, así como por su relación con el tema central del trabajo.

A continuación, se introducen los polinomios linealizados o q-polinomios sobre $\mathbb{F}_{q^m}$, examinando la estructura del conjunto de sus raíces, las operaciones que les confieren una estructura de anillo y el concepto de irreducibilidad. Se presentan también, entre otros conceptos, el de q-módulo y raíz q-primitiva, con el fin de dar resultados esenciales, como la construcción de una base de un q-módulo a partir de una raíz q-primitiva de un polinomio linealizado sobre $\mathbb{F}_q$.

Posteriormente, se introduce la métrica de rango, detallando la noción de distancia mínima de rango. Se presenta una cota superior para el cardinal M de un código sobre $\mathbb{F}_{q^m}$, análoga a la cota de Singleton en la métrica de Hamming. Esta cota conduce a la definición de los códigos MRD, entre los cuales se encuentran los códigos de Gabidulin. Además, se incluye una cota superior y otra inferior para el cardinal máximo de un código en bloque. Finalmente, se ofrece una descripción detallada de las palabras de los códigos de Gabidulin, utilizando la aplicación

invertible q-transformada, así como bases normales y duales, con el fin de establecer una correspondencia entre polinomios linealizados y sus q-transformados. Asimismo, se introduce la noción de matriz de q-Vandermonde para definir una matriz generadora de esta clase de códigos.

Por último, se estudian posibles algoritmos de descodificación de códigos de Gabidulin, con el objetivo de encontrar un análogo al algoritmo de Welch-Berlekamp, diseñado para la descodificación de códigos de Reed-Solomon en la métrica de Hamming. Se establece la equivalencia entre la solución del problema de descodificación y el de reconstrucción de polinomios linealizados y se muestran dos algoritmos destinados a la resolución de este último. Para ambos algoritmos se analiza la complejidad computacional, destacándose que el segundo algoritmo, de estructura más elaborada, resulta ser más eficiente.

Capítulo 1

Preliminares

1.1. Cuerpos finitos

En este capítulo abordaremos el tema de los cuerpos finitos, es decir, aquellos con un número finito de elementos. Analizaremos sus propiedades y algunos resultados que serán fundamentales para el desarrollo de este trabajo (ver [12], capítulo 5).

En primer lugar, nos referiremos a cuerpos finitos con un número primo de elementos. Veremos que tienen una estructura sencilla y probaremos tanto su existencia dado un número primo cualquiera en la siguiente proposición, como su unicidad a continuación.

Proposición 1.1. *Para todo número primo p, existe un cuerpo finito con p elementos, el anillo cociente $\mathbb{Z}/p\mathbb{Z}$.*

Demostración. Veamos que el anillo cociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Basta ver que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es una unidad. En efecto, todo $m \in \mathbb{Z}/p\mathbb{Z}$ no nulo es primo con p, luego, según el algoritmo de Euclides, existen enteros λ y μ tales que $\lambda m + \mu p = mcd(m, p) = 1$. Trasladando esta igualdad a $\mathbb{Z}/p\mathbb{Z}$ obtenemos $\lambda m = 1$, luego $\lambda = m^{-1}$, esto es, m es unidad. □

Definición 1.1. Denominaremos al cuerpo descrito en la proposición anterior *cuerpo primo* de p elementos, y lo denotaremos por $\mathbb{F}_p$. Más adelante probaremos su unicidad.

Ahora, trataremos de generalizar a cuerpos finitos de cualquier cardinal, para lo que precisamos de algunos resultados.

Proposición 1.2. *Si q es el cardinal de un cuerpo finito, existen un primo p y un número natural r tales que $q = p^r$.*

Demostración. Sea K un cuerpo finito de cardinal q. Sea 1_K su elemento unidad y consideramos

$$\varphi : \mathbb{Z} \to K,$$

la aplicación dada por

$$\varphi(n) = n \cdot 1_K.$$

Para n positivo, se define $n \cdot 1_K$ como $\underbrace{1_K + 1_K + \cdots + 1_K}_{n \text{ veces}}$.
Para n negativo, tomamos $n \cdot 1_K$ como el opuesto de la anterior suma.
El núcleo de φ no es trivial: como $\mathbb{Z}$ es infinito y K es un cuerpo finito, existe un entero no nulo n tal que $n \cdot 1_K = 0$, es decir

$$\ker(\varphi) = \{n \in \mathbb{Z} \mid n \cdot 1_K = 0\} \neq \{0\}.$$

Además, φ es homomorfismo de anillos, de modo que su núcleo $\ker(\varphi)$ es un ideal de $\mathbb{Z}$. Por tanto, debe ser un ideal principal de la forma $d\mathbb{Z}$ para algún $d \in \mathbb{N}$. Sea p el menor entero positivo en $\ker(\varphi)$, es decir, el menor entero positivo tal que $p \cdot 1_K = 0$. Entonces, el núcleo es el conjunto de los múltiplos de p, es decir, $p\mathbb{Z}$. Para ver que p es necesariamente un número primo, razonamos por reducción al absurdo. Supongamos que p no es primo, es decir, que se puede escribir como $p = ab$ con $a, b > 1$. Así,

$$(a \cdot 1_K)(b \cdot 1_K) = p \cdot 1_K = 0,$$

de modo que se anulan $a \cdot 1_K$ o $b \cdot 1_K$ por ser K un cuerpo. Habríamos llegado a que el menor entero positivo en el núcleo es menor que p, lo que es absurdo.
Por tanto, el núcleo de φ consiste en un ideal de la forma $p\mathbb{Z}$, donde p es un número primo.

De lo anterior deducimos que K debe contener un subcuerpo de cardinal p que es isomorfo a $\mathbb{Z}/p\mathbb{Z}$, de forma que K puede considerarse un espacio vectorial sobre este subcuerpo de dimensión finita. Así, siendo r la dimensión del espacio vectorial K sobre el subcuerpo, el cardinal de K es $q = p^r$.

□

De esta proposición podemos extraer dos conclusiones importantes: por un lado, que el cuerpo primo es único (salvo isomorfismo); y por otro, que todo *cuerpo finito de q elementos* contiene un único cuerpo primo $\mathbb{F}_p$, puesto que su cardinal es una potencia de p.

Proponemos una definición relacionada que resultará útil. En ella denotaremos al cuerpo finito de q elementos por $\mathbb{F}_q$, teniendo en cuenta que más adelante probaremos que se trata del único cuerpo finito de tal cardinal, salvo isomorfismo.

Definición 1.2. Diremos que el cuerpo $\mathbb{F}_q$, donde $q = p^r$ y p es primo, tiene *característica p*.

Continuemos con la caracterización del cuerpo $\mathbb{F}_q$. Al igual que en el caso primo, construiremos explícitamente un cuerpo finito de cardinal q cualquiera con el fin de asegurar su existencia. Para ello, precisamos de un resultado sobre anillos cociente.

Lema 1.1. *Sea K un cuerpo y $f(x)$ un polinomio irreducible de $K[x]$, entonces el anillo cociente $K[x]/\langle f(x)\rangle$ es un cuerpo.*

Demostración. Basta ver que un representante cualquiera $g(x)$ de un elemento no nulo del anillo cociente es unidad. Como $f(x)$ es irreducible en $K[x]$, sus únicos divisores son el propio $f(x)$ y los elementos de K. Por tanto, $\mathrm{mcd}(f(x), g(x)) = 1$ y, según el algoritmo de Euclides en $K[x]$, existen polinomios $\lambda(x), \mu(x)$ con

$$\lambda(x)g(x) + \mu(x)f(x) = 1.$$

En el anillo cociente, esta igualdad equivale a $\lambda(x)g(x) = 1$, es decir, $\lambda(x)$ es el inverso de $g(x)$. □

Este resultado aplicado al anillo de polinomios de un cuerpo primo, $\mathbb{F}_p[x]$, siendo $f(x)$ un polinomio irreducible del anillo, nos lleva a concluir que el anillo cociente $\mathbb{F}_p[x]/\langle f(x)\rangle$ es un cuerpo.

Teorema 1.1. *Para todo $q = p^r$, existe un cuerpo finito con q elementos.*

Demostración. Consideramos el cuerpo $A = \mathbb{F}_p[x]/\langle f(x)\rangle$. Tomamos $f(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado r. Omitimos por brevedad la prueba de que debe existir tal polinomio (viene dada en [12], Corolario 9.3.7).
Veamos que todo polinomio en $\mathbb{F}_p[x]$ posee un único representante en A de grado menor que r.

Sea $g(x) \in \mathbb{F}_p[x]$, aplicando el algoritmo de división euclídea, existe un único par de polinomios $q(x), h(x) \in \mathbb{F}_p[x]$ tal que:

$$g(x) = q(x)f(x) + h(x),$$

donde $h(x)$ tiene grado menor que r. En el cuerpo A, esta igualdad se traduce en

$$g(x) = h(x) \quad (\text{mód } f(x)).$$

Concluimos que cada clase de equivalencia en A tiene un representante único dado por un polinomio de grado menor que r. Dicho de otro modo, A puede identificarse con el conjunto de polinomios de $\mathbb{F}_p[X]$ de grado $< r$, luego su cardinal es p^r.

□

Una vez establecida la existencia de cuerpos finitos para cualquier cardinal, profundizaremos en la estructura del anillo de polinomios de un cuerpo finito y el concepto de polinomios irreducibles. Nuestro objetivo será caracterizar de manera precisa los elementos de un cuerpo finito y, finalmente, demostrar su unicidad.

Lema 1.2. *Sea $\mathbb{F}_q$ un subcuerpo del cuerpo finito $\mathbb{F}_s$ y sea α un elemento no nulo de $\mathbb{F}_s$. Existe un único polinomio no nulo en $\mathbb{F}_q[X]$ que tiene a α por raíz y es mónico e irreducible.*

Demostración. $\mathbb{F}_s$ es un espacio vectorial de dimensión finita r sobre $\mathbb{F}_q$, de modo que el conjunto $\{1, \alpha, \ldots, \alpha^r\}$ es linealmente dependiente sobre $\mathbb{F}_q$, es decir, existen coeficientes $a_i \in \mathbb{F}_q$, no todos nulos, para los que se verifica

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r = 0.$$

Siendo esta una combinación lineal no trivial, podemos considerar el siguiente polinomio en x no nulo que tiene a α por raíz:

$$a_0 + a_1x + a_2x^2 + \cdots + a_rx^r.$$

Sea entonces $f(x)$ un polinomio mónico no nulo tal que admite a α como raíz y es de grado mínimo (menor o igual a r).
Veamos que entonces $f(x)$ es también irreducible por reducción al absurdo. Supongamos que $f(x) = f_1(x)f_2(x)$, donde $f_1(x)$ y $f_2(x)$ son ambos polinomios de grado mayor que 0. Entonces, α es raíz de $f_1(x)$ o bien de $f_2(x)$, lo que contradice que $f(x)$ sea el polinomio de grado mínimo que tiene a α por raíz.
Veamos ahora que todo polinomio $g(x)$ que admite a α como raíz es múltiplo de $f(x)$. Mediante el algoritmo de división euclídea obtenemos dos polinomios $h(x)$ y $c(x)$ tales que

$$g(x) = f(x)c(x) + h(x),$$

donde $h(x)$ es un polinomio de grado menor que el de $f(x)$. Evaluando en α obtenemos que

$$0 = g(\alpha) = h(\alpha).$$

El polinomio $h(x)$ debe ser el polinomio nulo, dado que se anula en α y tiene grado menor que $f(x)$, es decir $h(x) = 0$. Por tanto, $g(x)$ es múltiplo de $f(x)$. Esto equivale a decir que $f(x)$ es el único polinomio no nulo, mónico e irreducible en $\mathbb{F}_q[X]$ que admite a α como raíz. □

Una manera alternativa de expresar el resultado anterior es decir que el conjunto de polinomios en $\mathbb{F}_q[x]$ que tienen a α por raíz no se reduce al polinomio cero y coincide con el de múltiplos de un polinomio mónico irreducible. Daremos una definición para este polinomio a continuación.

Definición 1.3. El polinomio $f(x)$, cuya existencia y unicidad viene asegurada por el lema anterior, se denomina el *polinomio mínimo o irreducible* de α sobre $\mathbb{F}_q$. Lo denotaremos por $\mathrm{Irr}(\alpha, \mathbb{F}_q)$.

Antes de seguir profundizando en los polinomios en $\mathbb{F}_q[x]$, daremos un resultado que usaremos en la proposición que sigue y en resultados posteriores.

Corolario 1.1. *Todo elemento $a \in \mathbb{F}_q$ verifica que $a^q = a$.*

Demostración. Para el caso $a = 0$ la igualdad es obvia. Por otro lado, si $a \neq 0$, consideramos el grupo formado por los elementos no nulos de $\mathbb{F}_q$, esto es, el grupo multiplicativo $\mathbb{F}_q^*$. Por el Teorema de Lagrange, como $a \in \mathbb{F}_q^*$, el orden de a divide al orden de $\mathbb{F}_q^*$, que es $q - 1$. Por tanto, $a^{q-1} = 1$, esto es, $a^q = a$.

□

Proposición 1.3. *El polinomio $x^q - x$ factoriza completamente sobre el cuerpo $\mathbb{F}_q$, es decir,*

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

Demostración. En el corolario anterior comprobamos que cada $a \in \mathbb{F}_q$ verifica que $a^q = a$. Así, queda probado que todo elemento de $\mathbb{F}_q$ es raíz de $x^q - x$.

Además, como el grado del polinomio es q, necesariamente las raíces de $x^q - x$ coinciden con los elementos de $\mathbb{F}_q$ y se cumple lo enunciado. □

La proposición anterior nos sugiere una definición alternativa de $\mathbb{F}_q$ como el conjunto de raíces de $x^q - x \in \mathbb{F}_p[x]$. Esta será válida si existen esas raíces en algún cuerpo de característica p.

Proposición 1.4. *Un polinomio irreducible $f(x) \in \mathbb{F}_q[x]$ de grado r factoriza completamente sobre $\mathbb{F}_{q^r}$, siendo q la potencia de un número primo.*

Demostración. Consideramos el anillo cociente $\mathbb{F}_q[x]/\langle f(x)\rangle$, que se trata de un cuerpo con q^r elementos. Sea $\bar{x}$ la clase de x en el anillo cociente. Como $\bar{x}$ es una raíz de $f(x)$ y este es un polinomio irreducible en $\mathbb{F}_q[x]$, podemos escribir $f(x) = \mathrm{Irr}(\bar{x}, \mathbb{F}_q)$.
Por la Proposición 1.3, las raíces de $x^{q^r} - x$ coinciden con los elementos de $\mathbb{F}_{q^r}$, luego $\bar{x}$ es también raíz de $x^{q^r} - x$ y este polinomio factoriza completamente sobre el cuerpo $\mathbb{F}_{q^r}$. Además, por el Lema 1.2, $x^{q^r} - x$ es múltiplo del irreducible $f(x)$, de modo que $f(x)$ tiene sus r raíces en $\mathbb{F}_{q^r}$, es decir, factoriza completamente sobre $\mathbb{F}_{q^r}$.

□

Veamos un resultado necesario para probar el corolario que sigue.

Lema 1.3. *Sea q la potencia de un primo y r, s enteros positivos. Entonces, $\mathbb{F}_{q^r}$ es un subcuerpo de $\mathbb{F}_{q^s}$ si y sólo si r divide a s.*

Demostración. Probaremos la doble implicación.

- $\Leftarrow$ Supongamos que r divide a s. Sabemos que los elementos de $\mathbb{F}_{q^r}$ son las raíces del polinomio $x^{q^r} - x$, que divide a $x^{q^s} - x$. Como $\mathbb{F}_{q^s}$ contiene a todas las raíces de $x^{q^s} - x$, en particular contiene a las de $x^{q^r} - x$, y por tanto contiene a $\mathbb{F}_{q^r}$. Además, $\mathbb{F}_{q^r}$ es un cuerpo, por lo que es un subcuerpo de $\mathbb{F}_{q^s}$.

- $\Rightarrow$ Supongamos ahora que $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s}$. Entonces, $\mathbb{F}_{q^s}$ es un espacio vectorial sobre $\mathbb{F}_{q^r}$, por lo que $q^s = q^{rt}$ para cierto entero positivo t, es decir, r divide a s.

□

A continuación, enunciamos un resultado derivado, referido a polinomios no necesariamente irreducibles en $\mathbb{F}_q[x]$.

Corolario 1.2. *Un polinomio $f(x) \in \mathbb{F}_q[x]$ no nulo factoriza completamente sobre $\mathbb{F}_{q^r}$, siendo q la potencia de un número primo y $r := r_1 \cdot r_2 \cdots r_t$, donde $r_i := \deg(f_i(x))$, para $1 \leq i \leq t$, y los $f_i(x)$ son los polinomios de la factorización en irreducibles de $f(x)$.*

Demostración. Sabemos que existen polinomios $f_1(x), f_2(x), \dots f_t(x) \in \mathbb{F}_q[x]$ no nulos e irreducibles con $r_i := \deg(f_i(x))$ para $1 \leq i \leq t$ tales que

$$f(x) = f_1(x) \cdot f_2(x) \cdots f_t(x) \text{ y } r = r_1 \cdot r_2 \cdots r_t.$$

Entonces, $\mathbb{F}_{q^{r_i}}$ es una extensión del cuerpo $\mathbb{F}_q$ que contiene todas las raíces de $f_i(x)$ (por el teorema anterior, cada irreducible factoriza completamente sobre $\mathbb{F}_{q^{r_i}}$). Por tanto, como r es múltiplo de r_i, $\mathbb{F}_{q^{r_i}} \subseteq \mathbb{F}_{q^r}$ para cada $1 \leq i \leq t$ (por el Lema 1.3), y se tiene que $f(x)$ factoriza completamente sobre $\mathbb{F}_{q^r}$. □

Corolario 1.3. *Sea $f(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado r y sea $q = p^r$. Como espacio vectorial, $\mathbb{F}_q$ es igual al conjunto de expresiones polinómicas $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}$, siendo α una raíz cualquiera de $f(x)$ en $\mathbb{F}_q$ y $a_i \in \mathbb{F}_p$.*

Demostración. Basta probar que el conjunto $\{1, \alpha, \dots, \alpha^{r-1}\}$ constituye una base de $\mathbb{F}_q$ como espacio vectorial sobre $\mathbb{F}_p$. Razonemos por reducción al absurdo.
Supongamos que se trata de un conjunto linealmente dependiente sobre $\mathbb{F}_q$. Entonces, $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} = 0$, para ciertos $a_i \in \mathbb{F}_p$. Así, α sería raíz de un polinomio de grado menor que r, lo cual contradice la elección de $f(x)$. Por tanto, se trata de un conjunto libre y

$$\mathbb{F}_q = \left\{ \sum_{i=0}^{r-1} a_i \alpha^i \mid a_i \in \mathbb{F}_p \right\},$$

siendo $\alpha \in \mathbb{F}_q$ una raíz cualquiera de $f(x)$.

□

Finalmente estamos en condiciones de probar la unicidad de cuerpos finitos de cualquier cardinal.

Teorema 1.2. *Para toda potencia q de un número primo existe, salvo isomorfismo, un solo cuerpo finito con q elementos.*

Demostración. Sea $q = p^r$ y $f(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado r. Basta ver que $\mathbb{F}_q$ es isomorfo a $\mathbb{F}_p[x]/\langle f(x) \rangle$.
En virtud del corolario 1.3, los elementos de $\mathbb{F}_q$ pueden expresarse en la forma $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}$, con $a_i \in \mathbb{F}_p$, siendo α una raíz de $f(x)$. Sea la siguiente aplicación

$$\varphi : \mathbb{F}_q \to \mathbb{F}_p[x]/\langle f(x) \rangle$$

dada por

$$\varphi\left(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}\right) = a_0 + a_1 x + \cdots + a_{r-1}x^{r-1} \pmod{f(x)}$$

Concluimos que φ es el isomorfismo de cuerpos buscado.

□

Para concluir esta sección preliminar sobre cuerpos finitos, daremos una propiedad que verifican los elementos del cuerpo finito y que será útil más adelante.

Proposición 1.5. *Si $\mathbb{F}_q$ es un cuerpo de característica p, entonces para cada par de elementos $a, b \in \mathbb{F}_q$ y cada entero positivo s, se verifica que*

$$(a+b)^{p^s} = a^{p^s} + b^{p^s}.$$

Demostración. Por la fórmula del binomio de Newton, válida en cualquier cuerpo conmutativo (todo cuerpo finito es conmutativo), tenemos:

$$(a+b)^{p^s} = \sum_{i=0}^{p^s} \binom{p^s}{i} a^i b^{p^s-i}.$$

Los coeficientes binomiales se definen como:

$$\binom{p^s}{i} = \frac{p^s!}{i!(p^s-i)!}.$$

Para $0 < i < p^s$ este coeficiente se anula, ya que es múltiplo de p y estamos en el cuerpo $\mathbb{F}_q$ de característica p. Es decir,

$$\binom{p^s}{i} \equiv 0 \pmod{p}, \quad \text{para } 0 < i < p^s.$$

Así, en la suma del binomio de Newton, todos los términos intermedios desaparecen en $\mathbb{F}_q$, dejando únicamente los términos correspondientes a $i = 0$ y $i = p^s$, y resulta:

$$(a+b)^{p^s} = a^{p^s} + b^{p^s}.$$

□

1.2. Códigos lineales

En esta sección, introduciremos los procesos de transmisión de la información y los relacionaremos con la teoría de cuerpos finitos presentada en el capítulo anterior. Daremos algunas definiciones clave y dotaremos a los códigos de una estructura algebraica, con el objetivo de optimizar computacionalmente los procesos de codificación y descodificación de mensajes (ver [12], Capítulo 6).

Definición 1.4. El alfabeto en que está escrita originalmente la información recibe el nombre de *alfabeto fuente*; el alfabeto en que será codificada, recibe el de *alfabeto código*.

Nosotros usaremos el cuerpo $\mathbb{F}_q$ como alfabetos fuente y código.

Definición 1.5. Llamaremos *palabra* escrita en el alfabeto $\mathbb{F}_q$ a cualquier secuencia finita de elementos o *letras* de $\mathbb{F}_q$. Denotaremos el conjunto de palabras escritas en $\mathbb{F}_q$ por $\mathcal{P}(\mathbb{F}_q)$.

Ahora bien, para poder dar una definición de código lineal, el tema central de la sección, y poder describirlo adecuadamente, es necesario introducir las siguientes definiciones.

Definición 1.6. La *longitud* de una palabra es el número de símbolos que la componen. Si todas las palabras de un código son de la misma longitud n, se dice que este es un *código en bloque* de longitud n.

Veamos ahora cómo podemos dotar a un código en bloque de una estructura algebraica conveniente.

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

Recordaremos el concepto de distancia para, a continuación, introducir esa idea en el contexto de los códigos lineales, lo que nos permitirá medir la separación entre palabras.

Definición 1.8. Una *distancia* o *métrica* en un conjunto X es una aplicación d con espacio de partida $X \times X$ que asigna a cada par de elementos $\mathbf{x}, \mathbf{y} \in X$ un valor $d(\mathbf{x}, \mathbf{y})$, y que satisface las siguientes propiedades para cualesquiera elementos $\mathbf{x}, \mathbf{y}, \mathbf{z} \in X$:

(i) $d(\mathbf{x}, \mathbf{y}) \geq 0$ y, además, $d(\mathbf{x}, \mathbf{y}) = 0$ si y sólo si $\mathbf{x} = \mathbf{y}$.

(ii) *Simetría:* $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

(iii) *Desigualdad triangular:* $d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$.

Sabemos que es posible definir diversas aplicaciones que cumplan las tres condiciones mencionadas. En este capítulo, nos centraremos en la distancia más clásica: la *distancia de Hamming*. Esta métrica nos permitirá analizar en profundidad las propiedades de los códigos lineales, además de sentar las bases para introducir una distancia algo más compleja en capítulos posteriores.

Definición 1.9. Sean $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, con $\mathbf{x} = (x_1, \cdots, x_n)$, $\mathbf{y} = (y_1, \cdots, y_n)$, llamaremos *distancia de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$ a

$$d(\mathbf{x}, \mathbf{y}) = \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\},$$

es decir, al número de índices para los cuales difieren las coordenadas de ambos vectores.

Proposición 1.6. *La aplicación d definida como antes es efectivamente una distancia en $\mathbb{F}_q^n$.*

Demostración. La aplicación d satisface claramente

(i) d es no negativa, por tratarse del número de elementos de un conjunto. Además, $d(\mathbf{x}, \mathbf{y}) = 0 \Leftrightarrow \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\} = 0 \Leftrightarrow x_i = y_i \; \forall i \in \{1, \ldots, n\}; \Leftrightarrow \mathbf{x} = \mathbf{y}$.

(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$. En efecto,

$$d(\mathbf{x}, \mathbf{y}) = \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\} = d(\mathbf{y}, \mathbf{x}).$$

(iii) $d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$. En efecto,

$$d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) = \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\} + \#\{i \mid 1 \leq i \leq n, y_i \neq z_i\}$$

$$\geq \#\{i \mid 1 \leq i \leq n, x_i \neq z_i\} = d(\mathbf{x}, \mathbf{z}).$$

Esto se debe a que, dado un índice $i \in \{1, \ldots, n\}$, si se tiene $x_i \neq z_i$ entonces debe ser $i \in \{i \mid x_i \neq y_i\}$ o bien $i \in \{i \mid y_i \neq z_i\}$ (de no ser así, tendríamos $i \in \{i \mid x_i = y_i, y_i = z_i\}$, llegando a contradicción). Así, cada índice que se encuentra en el conjunto de la derecha de la desigualdad, debe encontrarse en al menos uno de los conjuntos de la izquierda.

para todo $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$ □

Definición 1.10. Llamaremos *distancia mínima* del código $\mathcal{C}$ a

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

Definición 1.11. Los *parámetros fundamentales* de un código lineal $\mathcal{C}$ sobre $\mathbb{F}_q$ como espacio vectorial son: su longitud n, su *dimensión* k y la distancia mínima d. Diremos que el código es de tipo $[n,k]$ o $[n,k,d]$ y su cardinal es q^k.

Definición 1.12. Otros dos parámetros importantes, dado un código lineal de tipo $[n,k]$ son: la *redundancia* $r = n-k$; y la *tasa de transmisión de información* $R(\mathcal{C}) = \frac{k}{n}$.

Sigamos profundizando en la estructura algebraica, ahora describiendo una aplicación de codificación.

Definición 1.13. Sea $\mathcal{C}$ un código lineal de tipo $[n,k]$, visto como un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k. Puede ser interpretado como imagen de una (no única) aplicación lineal inyectiva

$$f : \mathbb{F}_q^k \to \mathbb{F}_q^n,$$

la *aplicación de codificación* de la fuente $\mathbb{F}_q^k$ con el código $\mathcal{C}$.

Así, dados n, k enteros positivos, *codificar* una palabra del código fuente $\mathbb{F}_q^k$ con el código $\mathcal{C} \subseteq \mathbb{F}_q^n$ será dar una aplicación lineal inyectiva f como la descrita arriba.

Esta interpretación motiva la siguiente definición.

Definición 1.14. Llamaremos *matriz generatriz* de $\mathcal{C}$ a la matriz de una aplicación lineal inyectiva

$$f : \mathbb{F}_q^k \to \mathcal{C} \subset \mathbb{F}_q^n,$$

es decir, a una matriz $k \times n$ cuyas filas son una base de $\mathcal{C}$.

Es claro que la matriz generatriz no es única (no es única la base de $\mathcal{C}$) y tampoco lo es la aplicación f. Sin embargo, las matrices generatrices tienen la particularidad de que, dadas dos de ellas G_1, G_2, existe una matriz invertible P tal que $G_1 = PG_2$.

Una matriz generatriz G proporciona tanto un código como una codificación. Dado un mensaje $\mathbf{a} \in \mathbb{F}_q^k$, se codifica por $\mathbf{a}G \in \mathbb{F}_q^n$ y $\mathcal{C} = \{\mathbf{a}G \mid \mathbf{a} \in \mathbb{F}_q^k\}$, donde $\mathbf{a}$ es un vector fila. Así, la codificación para los códigos lineales requiere el almacenamiento en memoria de la matriz G, con nk elementos de $\mathbb{F}_q$, y no de nq^k, como sería el caso de un código en bloque no lineal con el mismo cardinal.

Definición 1.15. Diremos que dos códigos $\mathcal{C}_1, \mathcal{C}_2$, de la misma longitud, n, sobre $\mathbb{F}_q$, son *equivalentes* si existe una permutación σ del conjunto $\{1, \ldots, n\}$ tal que

$$\mathcal{C}_2 = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1\}.$$

Entendemos esta permutación como la reordenación de las coordenadas de las palabras, es decir, $\sigma(c_1, \ldots, c_n) = (c_{\sigma(1)}, \ldots, c_{\sigma(n)})$.

Otra forma de expresar la definición anterior sobre códigos equivalentes es decir que lo son si reordenando las columnas de una matriz generatriz del primero obtenemos una matriz generatriz del segundo. Por otro lado, dos permutaciones distintas no producen necesariamente códigos distintos, lo que nos lleva a dar la siguiente definición.

Definición 1.16. El *grupo de automorfismos* de $\mathcal{C}$ es el subgrupo de S_n

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\},$$

donde S_n es el *grupo simétrico* de orden n, es decir, el grupo de las $n!$ permutaciones del conjunto $\{1, \ldots, n\}$.

Hemos visto que un subespacio vectorial de $\mathbb{F}_q^n$ puede describirse mediante un sistema de generadores. Sin embargo, también puede describirse a través de unas ecuaciones implícitas, surgiendo el concepto siguiente.

Definición 1.17. Una matriz de rango máximo H es una *matriz de control* del código $\mathcal{C}$ si para todo vector $\mathbf{x} \in \mathbb{F}_q^n$ se verifica que $\mathbf{x} \in \mathcal{C}$ si y sólo si $H\mathbf{x}^t = 0$. Si $\mathcal{C}$ está definido sobre $\mathbb{F}_q$ y es de tipo $[n, k]$, entonces también H está definida sobre $\mathbb{F}_q$, es de tamaño $(n-k) \times n$ y su rango es $n-k$.

Explicaremos en la siguiente proposición la relación entre las matrices generatriz y de control de un código.

Proposición 1.7. *Si G es matriz generatriz y H matriz de control del código $\mathcal{C}$, entonces $GH^t = 0$.*

Demostración. La matriz generatriz G de $\mathcal{C}$ está construida de manera que sus filas son una base del código $\mathcal{C}$. Así, cada fila de G es un vector $\mathbf{x} \in \mathcal{C}$, de modo que satisface la ecuación $H\mathbf{x}^t = 0$. Podemos concluir que $GH^t = 0$. □

Veamos ahora un método de codificación sencillo, que nos llevará a introducir los términos de matriz generatriz y matriz de control *en forma estándar*.

Definición 1.18. La *codificación sistemática* se basa en codificar una palabra $\mathbf{a} \in \mathbb{F}_q^k$ de modo que la palabra codificada contenga a esta palabra original como subpalabra.

Por ejemplo, podemos considerar que la palabra codificada correspondiente a la palabra $\mathbf{a} \in \mathbb{F}_q^k$ sea de la forma $(\mathbf{a}, \mathbf{z})$, $\mathbf{z} \in \mathbb{F}_q^{n-k}$. Así, los k primeros símbolos de la palabra contienen la información y los siguientes son de control. Esto permite que la descodificación sea automática en caso de no haber errores y que la matriz generatriz tenga una estructura sencilla concreta, que da lugar a la siguiente definición:

Definición 1.19. Cuando la codificación es sistemática, existe una matriz generatriz del código lineal, denominado *código sistemático*, de la forma $G = (I_k, Z)$, donde I_k denota la matriz identidad $k \times k$. Esta forma de G es conocida como *forma estándar*.

La importancia de estas definiciones se materializa en la siguiente proposición.

Proposición 1.8. *Todo código es equivalente a uno sistemático.*

Demostración. Sea $\mathcal{C}$ un código de dimensión k y G una matriz generatriz de $\mathcal{C}$, que será $k \times n$ y de rango k. Supongamos que las k primeras columnas son linealmente independientes (de no ser las k primeras, podríamos hacer una permutación), de modo que $G = (A, B)$ con A regular, de tamaño $k \times k$.

Ahora, con el método de Gauss, que consiste en realizar operaciones elementales por filas sobre A (ver el método de Gauss en [4]), transformamos A en la matriz identidad I_k. Realizamos estas operaciones elementales sobre G y obtenemos una matriz en forma estándar $G' = (I_k, Z)$ cuyas filas generan el mismo espacio que las de G. En conclusión, G' es una matriz generatriz de un código sistemático equivalente al que tiene a G por matriz generatriz. □

Describimos ahora la matriz generatriz de un código sistemático $\mathcal{C}$. Sea G una matriz generatriz de $\mathcal{C}$ dada en forma estándar, $G = (I_k, Z)$ y consideramos la matriz $H = (-Z^t, I_{n-k})$. H tiene tamaño $(n-k) \times n$, rango $n-k$ y verifica $GH^t = 0$, luego es una matriz de control para $\mathcal{C}$. Así, daremos la siguiente definición.

Definición 1.20. Una matriz de control está en forma estándar si es de la forma (B, I_{n-k}).

Daremos ahora varias definiciones imprescindibles para probar que la distancia mínima de un código puede ser obtenida a partir de su matriz de control.

Definición 1.21. Sea $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. Llamamos *soporte* de $\mathbf{x}$ al conjunto

$$\text{sop}(\mathbf{x}) = \{i \mid 1 \leq i \leq n, x_i \neq 0\},$$

es decir, el conjunto de índices correspondientes a las coordenadas no nulas del vector $\mathbf{x}$.

Definición 1.22. Llamamos *peso de Hamming* de $\mathbf{x}$ a

$$w(\mathbf{x}) = \#\text{sop}(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) = d(\mathbf{x}, (0, \cdots, 0)).$$

Dicho de otro modo, se trata del número de coordenadas no nulas del vector $\mathbf{x}$. Además, la aplicación w es una norma en $\mathbb{F}_q^n$ y d es la distancia asociada a esta norma.

Análogamente a la distancia mínima de un código, damos la siguiente definición asociada al peso de Hamming.

Definición 1.23. Llamamos *peso mínimo* de un código $\mathcal{C}$ a

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

Lema 1.4. *En un código lineal, la distancia mínima es igual al peso mínimo.*

Demostración. Un código lineal es un espacio vectorial y sabemos que $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. Por tanto, se verifica

$$w(\mathcal{C}) = \text{mín}\{w(\mathbf{x} - \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\} = \text{mín}\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\} = d(\mathcal{C})$$

□

Proposición 1.9. *Sea $\mathcal{C}$ un código lineal con matriz de control H y distancia mínima d, y sea r un número natural. Entonces $d > r$ si y sólo si cualesquiera r columnas de H son linealmente independientes.*

Demostración. Probaremos la doble implicación.

$\Rightarrow$ Supongamos que existen r columnas linealmente dependientes en H, entonces hay una combinación lineal de ellas que podemos igualar a cero. Siendo $\mathbf{x}$ el vector de coeficientes de la combinación lineal, tenemos que $H\mathbf{x}^t = 0$. Luego $\mathbf{x} \in \mathcal{C}$ y tiene peso $\leq r$, esto es, $d \leq r$.

$\Leftarrow$ Supongamos que cualesquiera r columnas de H son independientes. Entonces ningún vector no nulo de peso $\leq r$ puede pertenecer a $\mathcal{C}$, con lo que su distancia mínima es mayor que r.

□

Una conclusión que podemos extraer del resultado anterior es que la distancia mínima de un código con matriz de control H coincide con el menor cardinal de un conjunto de columnas linealmente dependientes en H.

Sea $\mathcal{C}$ un código lineal con matriz de control H. Como tiene rango máximo, podemos interpretar H como una matriz generatriz de otro código sobre $\mathbb{F}_q$. Esto nos lleva a dar la siguiente definición.

Definición 1.24. Llamamos *código dual* de $\mathcal{C}$ (código lineal con matriz de control H) al código lineal, denotado por $\mathcal{C}^\perp$, con H por matriz generatriz. Además, si G es una matriz generatriz de $\mathcal{C}$, G es una matriz de control para $\mathcal{C}^\perp$, ya que $GH^t = 0 \Rightarrow HG^t = 0$. Así, si $\mathcal{C}$ tiene dimensión k, $\mathcal{C}^\perp$ tiene dimensión $n - k$.

Proposición 1.10. *Si $\mathcal{C}$ es un código lineal, entonces su dual $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$.*

Demostración. Recordemos en primer lugar que dos vectores $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ son *ortogonales* si $\mathbf{x} \bullet \mathbf{y} = 0$, donde $\bullet$ es la forma bilineal sobre $\mathbb{F}_q^n$ dada por

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

Sea G matriz generatriz y H de control de $\mathcal{C}$. Partimos de que $GH^t = 0$, esto es, el espacio generado por las filas de G es ortogonal al espacio generado por las filas de H. Además, el rango$(G) = k$ y el rango$(H) = n - k$, luego rango(G)+ rango$(H) = n$. Como H es la matriz generatriz de $\mathcal{C}^\perp$ (sus filas son una base de $\mathcal{C}^\perp$) podemos afirmar que es el ortogonal de $\mathcal{C}$. □

Algunas propiedades del código dual son las siguientes:

- $(\mathcal{C}^\perp)^\perp = \mathcal{C}$, es decir, el dual del dual de un código es el propio código. Se debe a que la forma bilineal $\mathbf{x} \bullet \mathbf{y}$ es simétrica y no degenerada.
- Se puede dar que $\mathcal{C} \cap \mathcal{C}^\perp \neq \{0\}$, e incluso que $\mathcal{C} = \mathcal{C}^\perp$. En este último caso, diremos que un código lineal es *autodual*.

Veamos ahora una nueva forma de relacionar un código $\mathcal{C}$ y su dual, teniendo en cuenta los pesos de las palabras de $\mathcal{C}$. Sea n la longitud de $\mathcal{C}$, consideramos los enteros

$$a_i = a_i(\mathcal{C}) = \#\{\mathbf{c} \in \mathcal{C} \mid w(\mathbf{c}) = i\},$$

para $1 \leq i \leq n$. Evidentemente $a_0 = 1$, $a_i = 0$ para todo $0 < i < d$ y $\sum_{i=0}^{n} a_i = q^k$ (el cardinal del código).

Definición 1.25. Llamamos *polinomio de pesos* al polinomio

$$W(X) = \sum_{i=0}^{n} a_i X^i = \sum_{c \in C} X^{w(c)}.$$

Otra forma de expresarlo es en dos variables, homogeneizando el anterior:

$$W(X, Y) = \sum_{i=0}^{n} a_i X^i Y^{n-i}.$$

El polinomio de pesos de un código determina unívocamente el polinomio de pesos de su dual. Veamos de qué manera.

Teorema 1.3. *Sean $\mathcal{C}$ un código lineal $[n, k]$ sobre $\mathbb{F}_q$ y $\mathcal{C}^\perp$ su dual. Si $W(X, Y)$ y $W^\perp(X, Y)$ son los polinomios de pesos de $\mathcal{C}$ y $\mathcal{C}^\perp$ respectivamente, entonces*

$$W^\perp(X, Y) = q^{-k} W(Y - X, Y + (q - 1)X).$$

Se trata de la Identidad de MacWilliams.

Demostración. Una demostración completa no procede en el desarrollo de este trabajo, pero se puede encontrar en [12], Apéndice i) del Capítulo 6. □

Pasaremos a centrarnos en la descodificación de los códigos lineales, aportando un método general que nos permita llevar a cabo este proceso.

Sea C un código lineal $[n, k, d]$ sobre $\mathbb{F}_q$. Supongamos emitida una palabra $\mathbf{c} \in \mathcal{C}$ y recibido un vector $\mathbf{y} \in \mathbb{F}_q^n$. Para descodificar, seguiremos el *principio de distancia mínima*, es decir, calcularemos la distancia de Hamming de $\mathbf{y}$ a cada palabra de $\mathcal{C}$ y descodificaremos $\mathbf{y}$ por la palabra de $\mathcal{C}$ más próxima a $\mathbf{y}$. El error cometido durante la transmisión será $\mathbf{e} = \mathbf{y} - \mathbf{c}$.

Veremos en la proposición siguiente la importancia del parámetro de distancia mínima a la hora de medir la capacidad de corrección de errores de un código en bloque. Más adelante, lo trasladaremos al contexto de los códigos lineales.

Proposición 1.11. *Sea $\mathcal{C}$ un código en bloque de longitud n y distancia mínima d y sea $\mathbf{y}$ una n-upla recibida. Si tomamos $t \geq 0$ con $2t < d$, entonces el método de descodificación descrito arriba permite corregir cualquier configuración de t errores.*

Demostración. Recordamos que el método funciona correctamente para $\mathbf{y}$ cuando $\mathbf{c}$ es la (única) palabra de $\mathcal{C}$ más próxima a $\mathbf{y}$. Supongamos que $\mathbf{y}$ contiene t errores y $2t < d$. Por definición de distancia mínima, las bolas con centro en las palabras código y radio $(d-1)/2$ son disjuntas. Entonces, $\mathbf{y}$ estará en una y sólo una de tales bolas, que tendrá por centro la palabra código más cercana. Por tanto, tendríamos $d(\mathbf{y}, \mathbf{c}) < d(\mathbf{y}, \mathbf{x})$ para todo $\mathbf{x} \in \mathcal{C}$.
Lo vemos en detalle: supongamos que no es así, es decir, que existe $\mathbf{x} \in \mathcal{C}$, $\mathbf{x} \neq \mathbf{c}$ tal que $d(\mathbf{y}, \mathbf{x}) \leq d(\mathbf{y}, \mathbf{c}) \leq (d-1)/2$. Por ser d una distancia, $d(\mathbf{c}, \mathbf{x}) \leq d - 1$, lo que contradice la definición de d.

□

Considerando lo demostrado, planteamos la siguiente definición:

Definición 1.26. Si d es la distancia mínima de $\mathcal{C}$, diremos entonces que $\mathcal{C}$ *corrige* $\left\lfloor \frac{d-1}{2} \right\rfloor$ *errores.*

En conclusión, el número de errores que puede corregir un código depende exclusivamente de la distancia mínima d. De hecho, a medida que este valor aumenta, la corrección de errores mejora. Esto motiva el estudio de una cota superior para d y la caracterización de un conjunto de códigos que, en este sentido, sean óptimos (ver [12], Capítulo 8).

Teorema 1.4. *Si $\mathcal{C}$ es un código de tipo $[n, k, d]$ sobre $\mathbb{F}_q$, entonces*

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

Este valor es denominado Cota de Singleton.

Demostración. Sea H una matriz de control de $\mathcal{C}$. Como sabemos, la distancia mínima de $\mathcal{C}$ coincide con el mínimo número de columnas linealmente dependientes de H. Como el rango de H es $n - k$, este número es a lo sumo $n - k + 1$, luego $d \leq n - k + 1$. □

Este teorema inspira la siguiente definición.

Definición 1.27. Los códigos para los que se alcanza la igualdad $d = n - k + 1$ son llamados de *máxima distancia de separación* o *códigos MDS.*

Otra forma de expresar la definición anterior es decir que un código $\mathcal{C}$ es MDS si y solo si cada conjunto de $n - k$ columnas de una matriz de control de $\mathcal{C}$ es linealmente independiente. Relacionaremos ahora este concepto con el dual de un código.

Proposición 1.12. *Si un código $\mathcal{C}$ es MDS entonces también su dual $\mathcal{C}^\perp$ es MDS.*

Demostración. Sea $\mathcal{C}$ un código MDS de tipo $[n,k]$, si tomamos $n-k$ columnas de una matriz de control suya serán linealmente independientes. Razonaremos por reducción al absurdo.

Supongamos que $\mathcal{C}^\perp$ no es MDS. La dimensión de $\mathcal{C}^\perp$ es $n-k$. Por tanto, para el código dual $d < n-(n-k)+1 = k+1$, es decir, la distancia mínima (el peso mínimo) es, a lo sumo, k, luego existe un vector $\mathbf{x} \in \mathcal{C}^\perp$ de peso $0 < w(\mathbf{x}) \leq k$.

Ampliamos $\mathbf{x}$ a una base de $\mathcal{C}^\perp$ y con ella construimos una matriz H generatriz de $\mathcal{C}^\perp$, es decir, de control para $\mathcal{C}$. Tomamos $n-k$ columnas de H con ceros en las coordenadas correspondientes de $\mathbf{x}$. Como $\mathcal{C}$ es MDS, estas columnas son linealmente independientes, pero llegamos a una contradicción, dado que se trata de $n-k$ elementos de $\mathbb{F}_q^{n-k}$ con la primera coordenada nula. □

Cabe destacar que para cualquier entero n existen siempre códigos MDS de longitud n y dimensiones $1, n-1$ y n; los llamaremos *MDS triviales*. Se sabe que, sobre $\mathbb{F}_2$, estos son los únicos que existen. Además, el objetivo de describir con detalle estos códigos que alcanzan la Cota de Singleton nos conduce a la siguiente definición.

Definición 1.28. Sea $\mathcal{C}$ un código lineal en $\mathbb{F}_q^n$ de tipo $[n,k]$ y sea $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, con $a_i \neq a_j$ para $i \neq j$ $(n \leq q)$. Entonces, $\mathcal{C}$ se trata de un *código de Reed-Solomon* de dimensión k si verifica

$$RS_{k,n}(\mathbf{a}) = \{(f(a_1), \ldots, f(a_n)) \mid f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}],\ \deg(f(\mathbf{x})) < k\}.$$

Para poder dar un resultado que muestre la relevancia de estos códigos, es preciso dar una definición previa.

Definición 1.29. Dado un polinomio $f \in \mathbb{F}_q[\mathbf{x}]$, definimos el *conjunto de ceros de* f de la siguiente manera:

$$Z(f) = \{a \in \mathbb{F}_q \mid f(a) = 0\}.$$

En particular, el *número de ceros de* f es el cardinal de este conjunto, denotado por $\mid Z(f) \mid$.

Proposición 1.13. *Sean $a_1, \ldots, a_n \in \mathbb{F}_q$ distintos dos a dos y $\mathbf{a} = (a_1, \ldots, a_n)$. El código de Reed Solomon $RS_{k,n}(\mathbf{a})$ es un código lineal de dimensión k y distancia mínima $d = n-k+1$, es decir, es un código MDS.*

Demostración. Veamos en primer lugar que se trata de un código lineal; a continuación, que tiene dimensión k; y por último, que se trata de un código MDS.

1. *Linealidad*: Sea $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$, tomo $\lambda, \mu \in \mathbb{F}_q$ y $f, h \in \mathbb{F}_q[\mathbf{x}]_{<k}$, veamos que la siguiente combinación lineal es una palabra del código $\mathcal{C}$:

   $$\lambda(f(a_1), \ldots, f(a_n)) + \mu(h(a_1), \ldots, h(a_n)) = (g(a_1), \ldots, g(a_n)),$$

   donde $g = \lambda f + \mu h$ y g es claramente un polinomio de $\mathbb{F}_q[\mathbf{x}]$ con grado $< k$.

2. *Dimensión k*: Consideramos la aplicación

   $$\varphi : \mathbb{F}_q[\mathbf{x}]_{<k} \to \mathbb{F}_q^n \text{ dada por } \varphi(f) = (f(a_1), \ldots, f(a_n)).$$

   φ es una aplicación $\mathbb{F}_q$-lineal. La demostración es análoga a la del apartado anterior: sean $f, g \in \mathbb{F}_q[\mathbf{x}]_{<k}$ y $\lambda, \mu \in \mathbb{F}_q$, tenemos:

   $$\varphi(\lambda f + \mu g) = ((\lambda f + \mu g)(a_1), \ldots, (\lambda f + \mu g)(a_n))$$
   $$= (\lambda f(a_1) + \mu g(a_1), \ldots, \lambda f(a_n) + \mu g(a_n)) = \lambda\varphi(f) + \mu\varphi(g).$$

Por lo tanto, φ es $\mathbb{F}_q$-lineal. Además, como φ es una aplicación entre espacios vectoriales sobre $\mathbb{F}_q$ podemos decir que es lineal.

Por tanto, para ver que φ es inyectiva basta ver que el núcleo de φ es trivial, es decir, que $\ker(\varphi) = \{0\}$. Sea $f \in \ker(\varphi)$, se trata de un polinomio en $\mathbb{F}_q[\mathbf{x}]_{<k}$ tal que $f(a_i) = 0 \quad \forall i = 1, \ldots, n$. De este modo, f es un polinomio de grado menor que k que tiene n raíces distintas $a_1, \ldots, a_n$. Por tanto, f es necesariamente el polinomio nulo.

Así, podemos concluir que $RS_{k,n}(\mathbf{a}) = \text{Im}\varphi$ y su dimensión es k (dimension del espacio de partida $\mathbb{F}_q[\mathbf{x}]_{<k}$).

3. *Código MDS*: Veamos que $d(RS_{k,n}(\mathbf{a})) = n - k + 1$. Sea $\mathbf{c} \in RS_{k,n}(\mathbf{a})$, $\mathbf{c} \neq \mathbf{0}$, vamos a comprobar que $w(\mathbf{c}) \geq n - k + 1$. Si así fuera, tendríamos $d \geq n - k + 1$, y como $d \leq n - k + 1$ para todo código lineal, se daría la igualdad que caracteriza a los códigos MDS.

   Sea $f \in \mathbb{F}_q[\mathbf{x}]$ no nulo de grado menor que k y sea $\mathbf{c} = (f(a_1), \ldots, f(a_n)) \in RS_{k,n}(\mathbf{a})$. El número de componentes nulas de $\mathbf{c}$ es menor o igual que el número de raíces de f, $\mid Z(f) \mid$. Luego $n - w(\mathbf{c}) \leq \mid Z(f) \mid$. Además, sabemos que el número de raíces de un polinomio no nulo no puede ser mayor que su grado y, recordando que el $\deg(f) < k$, resulta:

$$n - w(\mathbf{c}) \leq k - 1 \Rightarrow w(\mathbf{c}) \geq n - k + 1.$$

□

En resumen, los códigos de Reed Solomon son códigos lineales de máxima distancia de separación, que tienen la particularidad de corregir el mayor número de errores cuando tratamos con la distancia de Hamming.

Volviendo a los procesos de descodificación, consideremos un código lineal $\mathcal{C}$ de tipo $[n, k, d]$ sobre $\mathbb{F}_q$ que, como sabemos, corrige $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errores. Nos podemos encontrar las situaciones siguientes:

1. Si durante la transmisión se han cometido a lo sumo t errores, entonces $d(\mathbf{c}, \mathbf{y}) = w(\mathbf{e}) \leq t$ y $\mathbf{c}$ es la única palabra del código con tal propiedad y la descodificación sería correcta.
2. Si $t < w(\mathbf{e}) < d$, podemos detectar que se han producido errores (puesto que $\mathbf{y} \notin \mathcal{C}$), pero no corregirlos en general.
3. Si $w(\mathbf{e}) \geq d$ la descodificación fallará (eventualmente).

A continuación, vamos a describir un algoritmo de corrección de errores genérico, que funciona para cualquier código lineal. Sin embargo, veremos que su complejidad es demasiado alta para ser implementado de forma práctica.

Consideramos la matriz de control H del código $\mathcal{C}$, la palabra emitida $\mathbf{c}$ y la recibida $\mathbf{y} = \mathbf{c} + \mathbf{e}$, y comenzamos por estudiar cómo podemos guardar la mayor información acerca del error cometido.

Definición 1.30. Llamaremos *síndrome* de $\mathbf{y}$ al vector

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

Notemos que un vector está en el código $\mathcal{C}$ si y solo si su síndrome es el vector nulo. Por tanto, al ser el síndrome una aplicación lineal, se tiene que $s(\mathbf{y}) = s(\mathbf{c} + \mathbf{e}) = s(\mathbf{c}) + s(\mathbf{e}) = \mathbf{0} + s(\mathbf{e}) = s(\mathbf{e})$. Así, basta recibir $\mathbf{y}$ para conocer el síndrome del error cometido.

La siguiente proposición nos puede aportar información en casos sencillos para deducir el error $\mathbf{e}$ y el mensaje enviado $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

Proposición 1.14. *El síndrome del vector recibido* $\mathbf{y}$ *es una combinación lineal de las columnas de* H *correspondientes a las posiciones en las que han ocurrido errores.*

Sigamos profundizando en la estructura algebraica construyendo un espacio vectorial cociente, con el fin de dar un algoritmo de descodificación en términos de las clases de equivalencia. Consideramos en $\mathbb{F}_q^n$ la relación de equivalencia: $\mathbf{u} \sim \mathbf{v}$ si y sólo si $\mathbf{u}-\mathbf{v} \in \mathcal{C}$, que da lugar al espacio cociente $\mathbb{F}_q^n/\mathcal{C}$. Los elementos de $\mathbb{F}_q^n/\mathcal{C}$ son clases de equivalencia $\mathbf{u}+\mathcal{C} = \{\mathbf{u}+\mathbf{x} \mid \mathbf{x} \in \mathcal{C}\}$. Como cada clase posee $\#\mathcal{C} = q^k$ representantes, el cardinal de $\mathbb{F}_q^n/\mathcal{C}$ es q^{n-k} y su dimensión es $n-k$.

Notemos que $\mathbf{u}, \mathbf{v}$ están en la misma clase si y solo si $\mathbf{u}-\mathbf{v} \in \mathcal{C}$, es decir, si y solo si $s(\mathbf{u}) = s(\mathbf{v})$. Así, recibido $\mathbf{y}$, al conocer $s(\mathbf{y})$ conocemos la clase a la que pertenece el error cometido.

Definición 1.31. Si en una clase existe un único elemento de peso mínimo, este recibe el nombre de *líder de la clase*.

No toda clase tendrá líder, ya que el elemento de peso mínimo puede no ser único. Por otro lado, si una clase contiene un elemento de peso $\leq t$, este es el líder de la clase, como asegura la siguiente proposición.

Proposición 1.15. *Cada clase de* $\mathbb{F}_q^n/\mathcal{C}$ *posee a lo sumo un elemento de peso* $\leq t$.

Demostración. Supongamos que existen $\mathbf{u}, \mathbf{v}$ en la misma clase, ambos de peso $\leq t$. Entonces $\mathbf{u}-\mathbf{v} \in \mathcal{C}$ y $w(\mathbf{u}-\mathbf{v}) \leq w(\mathbf{u})+w(\mathbf{v}) \leq 2t < d(\mathcal{C})$, lo cual implica que $\mathbf{u}-\mathbf{v} = \mathbf{0} \Rightarrow \mathbf{u} = \mathbf{v}$. □

Además, la descodificación es posible si y solo si la clase del vector recibido $\mathbf{y}$ posee líder, y el error es asumido como el líder de la clase. En efecto, todos los vectores $\mathbf{y}-\mathbf{x}$, con $\mathbf{x} \in \mathcal{C}$, están en la clase de $\mathbf{y}$ en $\mathbb{F}_q^n/\mathcal{C}$, y el mínimo de $d(\mathbf{y}, \mathbf{x})$ se obtiene cuando $\mathbf{y}-\mathbf{x}$ es el líder de la clase.

Para llevar a cabo el proceso de descodificación de cualquier vector, construimos una tabla con dos columnas y q^{n-k} filas, tantas como clases hay en $\mathbb{F}_q^n/\mathcal{C}$:

- En la primera columna, escribimos el síndrome de un elemento cualquiera de cada una de las clases (recordamos que el síndrome de dos elementos de la misma clase es el mismo).
- En la segunda columna, escribimos el líder de la clase correspondiente (si existe).

Ahora, recibido $\mathbf{y}$, ejecutamos el siguiente algoritmo

1. Calcular $s(\mathbf{y})$ y buscarlo en la columna de síndromes.
2. Si la clase correspondiente a $s(\mathbf{y})$ no tiene líder, la decodificación falla.
3. Si la clase posee líder $\mathbf{e}$, el error es asumido como $\mathbf{e}$.
4. La palabra descodificada es $\mathbf{y}-\mathbf{e}$.

Como bien fue adelantado, podemos comprobar a simple vista que este algoritmo de corrección de errores genérico (para cualquier código lineal) tiene una complejidad demasiado alta. En efecto, para poder completarlo tuvimos que construir una tabla con q^{n-k} filas, de modo que las complejidades espacial y computacional serían $\mathcal{O}(q^{n-k})$, es decir, la complejidad sería exponencial en $n-k$.

Capítulo 2

Polinomios linealizados

En este capítulo nos volveremos a referir a polinomios sobre cuerpos finitos. En particular, analizaremos los polinomios linealizados (ver [5], Capítulo 3) . Estos se distinguen por la propiedad de que los exponentes que aparecen en ellos son potencias del tamaño q de un cuerpo finito, es decir, son potencias de la potencia de un número primo. Tras definir los polinomios linealizados y caracterizarlos, comprobaremos la relevancia de su concreta estructura y, en el capítulo siguiente, los relacionaremos con los códigos lineales.

A lo largo del capítulo denotaremos por q a una potencia de un número primo p.

2.1. Definición y conjunto de raíces

Definición 2.1. Un polinomio de la forma

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i} \tag{2.1}$$

con coeficientes en un cuerpo $\mathbb{F}_{q^m}$, se llama *q-polinomio* sobre $\mathbb{F}_{q^m}$ o bien *polinomio linealizado* (si q ha sido fijado) sobre $\mathbb{F}_{q^m}$. El mayor índice i tal que el coeficiente α_i es distinto de cero se conoce como el *q-grado* del polinomio y se denota por $\deg_q L(x)$.

Para entender de dónde surge esta terminología, relacionada con un comportamiento lineal de la aplicación L inducida por el polinomio descrito arriba, vemos las dos propiedades recogidas en la siguiente proposición.

Proposición 2.1. *Sea el cuerpo $\mathbb{F}_{q^m}$ y sea $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ un polinomio linealizado sobre $\mathbb{F}_{q^m}$, entonces:*

$$1. \quad L(\gamma + \beta) = L(\gamma) + L(\beta), \quad \forall \beta, \gamma \in \mathbb{F}_{q^m}, \tag{2.2}$$

$$2. \quad L(c\beta) = cL(\beta), \quad \forall c \in \mathbb{F}_q, \ \forall \beta \in \mathbb{F}_{q^m}. \tag{2.3}$$

Demostración. En primer lugar, recordamos dos resultados del Capítulo 1. Por un lado, para cada par $\gamma, \beta \in \mathbb{F}_q$, se verifica que $(\gamma + \beta)^{p^s} = \gamma^{p^s} + \beta^{p^s}$ (dado s entero positivo, por la Proposición 1.5), luego es cierto también que $(\gamma + \beta)^{q^i} = \gamma^{q^i} + \beta^{q^i}$ para $i \geq 0$. Por otro lado, se tiene que para cada $c \in \mathbb{F}_q$ se verifica que $c^q = c$ (ver el Corolario 1.1, Capítulo 1). Por tanto, dado $c \in \mathbb{F}_q$, $(c\beta)^{q^i} = c^{q^i} \beta^{q^i} = c\beta^{q^i}$ para $i \geq 0$.

Viendo $\mathbb{F}_{q^m}$ como espacio vectorial sobre $\mathbb{F}_q$, el polinomio linealizado $L(x)$ induce un operador lineal en $\mathbb{F}_{q^m}$. Lo vemos con detalle, considerando el polinomio linealizado $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$, con $\alpha, \beta \in \mathbb{F}_{q^m}$, $c \in \mathbb{F}_q$:

1. Como $(\gamma+\beta)^{q^i}=\gamma^{q^i}+\beta^{q^i}$, entonces $\forall \beta,\gamma\in\mathbb{F}_{q^m}$ es cierto que

$$L(\gamma+\beta)=\sum_{i=0}^{n}\alpha_i(\gamma_i+\beta_i)^{q^i}=\sum_{i=0}^{n}\alpha_i\gamma_i^{q^i}+\sum_{i=0}^{n}\alpha_i\beta_i^{q^i}=L(\gamma)+L(\beta).$$

2. Como $(c\beta)^{q^i}=c\beta^{q^i}$, entonces $\forall c\in\mathbb{F}_q, \forall\beta\in\mathbb{F}_{q^m}$ es cierto que

$$L(c\beta)=\sum_{i=0}^{n}c\,\alpha_i\beta^{q^i}=cL(\beta).$$

□

Comenzaremos por describir el conjunto de las raíces de un polinomio linealizado. Veremos que la estructura del conjunto nos ayudará a determinar las propias raíces.

Teorema 2.1. *Sea $L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$ un polinomio linealizado no nulo sobre $\mathbb{F}_{q^m}$. Consideremos una extensión $\mathbb{F}_{q^s}$ del cuerpo $\mathbb{F}_{q^m}$ que contiene todas las raíces de $L(x)$ (sabemos que existe tal extensión por el Corolario 1.2). Entonces,*

- *Todas las raíces de $L(x)$ tienen la misma multiplicidad:* 1 *o bien una potencia de q.*
- *El conjunto de las raíces de $L(x)$ conforma un subespacio de $\mathbb{F}_{q^s}$, visto como un espacio vectorial sobre $\mathbb{F}_q$.*

Demostración. Se deduce de las identidades anteriores que cualquier combinación lineal de raíces con coeficientes en $\mathbb{F}_q$ es nuevamente una raíz, por lo que las raíces de $L(x)$ forman un subespacio lineal de $\mathbb{F}_{q^s}$. Escribiendo $L(x)=\sum_{i=0}^{n}\alpha_i x^{q^i}$, entonces su derivada es $L'(x)=\alpha_0$, teniendo en cuenta que $\frac{d}{dx}x^{q^i}=q^i x^{q^i-1}=0$ para todo $i\geq 1$ en el cuerpo $\mathbb{F}_q$. Tenemos los casos:

- Si $\alpha_0\neq 0$, $L(x)$ solo tiene raíces simples.
- Si $\alpha_0=0$, al tratarse de un polinomio no nulo, existe un $k\geq 1$ tal que $\alpha_k\neq 0$, y podemos escribir:

$$L(x)=\sum_{i=k}^{n}\alpha_i x^{q^i}=\sum_{i=k}^{n}\alpha_i^{q^{mk}}x^{q^i}=\left(\sum_{i=k}^{n}\alpha_i^{q^{(m-1)k}}x^{q^{i-k}}\right)^{q^k}. \tag{2.4}$$

  Se trata de la q^k-ésima potencia de un polinomio linealizado con solo raíces simples. Es decir, en este caso, cada raíz de $L(x)$ tiene multiplicidad q^k.

□

Con la intención de ver un resultado muy relacionado con el anterior, debemos hacer referencia a la siguiente propiedad de los determinantes de matrices con elementos en el cuerpo $\mathbb{F}_{q^m}$.

Lema 2.1. *Sean $\beta_1,\beta_2,\ldots,\beta_n$ elementos de $\mathbb{F}_{q^m}$. Entonces,*

$$\begin{vmatrix}\beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{n-1}}\\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{n-1}}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \beta_n & \beta_n^q & \beta_n^{q^2} & \cdots & \beta_n^{q^{n-1}}\end{vmatrix}=\beta_1\prod_{j=1}^{n-1}\prod_{c_1,\ldots,c_j\in\mathbb{F}_q}\left(\beta_{j+1}-\sum_{k=1}^{j}c_k\beta_k\right), \tag{2.5}$$

y el determinante es distinto de cero si y solo si $\beta_1,\beta_2,\ldots,\beta_n$ son linealmente independientes sobre $\mathbb{F}_q$.

Demostración. Sea D_n el determinante, la parte izquierda de la igualdad en (2.5). Razonamos por inducción sobre n, siendo trivial el caso $n = 1$.

Supongamos que es cierta para $n \neq 1$. Consideramos el polinomio

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \cdots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ x & x^q & x^{q^2} & \cdots & x^{q^{n-1}} & x^{q^n} \end{vmatrix}. \tag{2.6}$$

Desarrollando por la última fila obtenemos

$$D(x) = D_n x^{q^n} + \sum_{i=0}^{n-1} \alpha_i x^{q^i}$$

para ciertos $\alpha_i \in \mathbb{F}_{q^m}$, para $0 \leq i \leq n-1$. Distinguimos dos casos:

- Si$\beta_1, \ldots, \beta_n$ son linealmente independientes sobre $\mathbb{F}_q$, tenemos que $D(\beta_k) = 0$ para $1 \leq k \leq n$. Además, como $D(x)$ es un q-polinomio sobre $\mathbb{F}_{q^m}$, las combinaciones lineales $c_1\beta_1 + \cdots + c_n\beta_n$, con $c_k \in \mathbb{F}_q$ para $1 \leq k \leq n$, son raíces de $D(x)$. Así, $D(x)$ tiene q^n raíces distintas y obtenemos una factorización

$$D(x) = D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k\beta_k \right). \tag{2.7}$$

- Si $\beta_1, \ldots, \beta_n$ son linealmente dependientes sobre $\mathbb{F}_q$, entonces $D_n = 0$ y $\sum_{k=1}^{n} b_k\beta_k = 0$ para ciertos $b_1, \ldots, b_n \in \mathbb{F}_q$, no todos nulos. Se deduce que

$$\sum_{k=1}^{n} b_k \beta_k^{q^j} = \left(\sum_{k=1}^{n} b_k\beta_k \right)^{q^j} = 0, \quad \text{para } j = 0, 1, \ldots, n.$$

  Vemos de esta forma que las primeras n filas en el determinante que define $D(x)$ son linealmente dependientes sobre $\mathbb{F}_q$. Esto implica que $D(x) = 0$, y que la identidad (2.7) se satisface en todos los casos.

Como consecuencia, podemos deducir de (2.7) lo siguiente para el caso $n + 1$:

$$D_{n+1} = D(\beta_{n+1}) = D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} \left(\beta_{n+1} - \sum_{k=1}^{n} c_k\beta_k \right),$$

y queda probado el resultado de (2.5) para todo n. También queda visto que el determinante es distinto de cero si y solo si $\beta_1, \beta_2, \ldots, \beta_n$ son linealmente independientes sobre $\mathbb{F}_q$. □

Teorema 2.2. *Sea U un subespacio de $\mathbb{F}_{q^m}$, considerado como un espacio vectorial sobre $\mathbb{F}_q$. Entonces, para cualquier entero no negativo k, el polinomio*

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

es un polinomio linealizado sobre $\mathbb{F}_{q^m}$.

Demostración. La q^k-ésima potencia de un polinomio linealizado sobre $\mathbb{F}_{q^m}$ es un polinomio linealizado, luego basta probar el resultado para el caso $k = 0$.

Sea $\{\beta_1, \ldots, \beta_s\}$ una base de U sobre $\mathbb{F}_q$. Entonces, el determinante D_n en el lado izquierdo de (2.7) es no nulo por el lema anterior. Para $k = 0$, por (2.7), tenemos que

$$L(x) = \prod_{\beta \in U} (x - \beta) = \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right) = D_n^{-1} D(x).$$

Esta igualdad muestra que $L(x)$ es un polinomio linealizado sobre $\mathbb{F}_{q^m}$, ya que $D(x)$ es un polinomio linealizado sobre $\mathbb{F}_{q^m}$. □

Veamos ahora un *método para determinar raíces de polinomios linealizados*, para lo que tendremos en cuenta las propiedades estudiadas acerca de estos particulares polinomios. Sea $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ un polinomio linealizado sobre $\mathbb{F}_{q^m}$. Supongamos que queremos encontrar todas las raíces de $L(x)$ en la extensión finita $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$.

Como comprobamos al comienzo del capítulo, la aplicación $L : \beta \mapsto L(\beta)$ en $\mathbb{F}_{q^m}$ funciona como un operador lineal en el espacio vectorial $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Así, L puede ser representada por una matriz sobre $\mathbb{F}_q$. Veamos de qué manera. Sea $\{\beta_1, \ldots, \beta_m\}$ una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Todo $\beta \in \mathbb{F}_{q^m}$ se puede escribir en la forma

$$\beta = \sum_{j=1}^{m} c_j \beta_j, \quad c_j \in \mathbb{F}_q, \quad \text{para } 1 \leq j \leq m.$$

Entonces,

$$L(\beta) = \sum_{j=1}^{m} c_j L(\beta_j).$$

Ahora, definimos

$$L(\beta_j) = \sum_{k=1}^{m} b_{jk}\, \beta_k, \quad \text{para } 1 \leq j \leq m,$$

donde $b_{jk} \in \mathbb{F}_q$ para $1 \leq j, k \leq m$.

Sea B la matriz $m \times m$ sobre $\mathbb{F}_q$ construida con los elementos b_{jk}. Entonces, si

$$(c_1, \ldots, c_m)B = (d_1, \ldots, d_m),$$

se tiene

$$L(\beta) = \sum_{j=1}^{m} c_j \left(\sum_{k=1}^{m} b_{jk}\, \beta_k \right) = \sum_{k=1}^{m} d_k \beta_k. \tag{2.8}$$

Por lo tanto, la ecuación $L(\beta) = 0$ es equivalente a

$$(c_1, \ldots, c_m)B = (0, \ldots, 0). \tag{2.9}$$

Este es un sistema homogéneo de m ecuaciones lineales para las incógnitas $c_1, \ldots, c_m$. Si r es el rango de la matriz B, entonces el sistema tiene q^{m-r} soluciones. Cada vector solución $(c_1, \ldots, c_m)$ proporciona una raíz $\beta = \sum_{j=1}^{m} c_j \beta_j$ de $L(x)$ en $\mathbb{F}_{q^m}$.

En conclusión, el problema de encontrar las raíces de $L(x)$ en $\mathbb{F}_{q^m}$ se reduce al problema de resolver un sistema homogéneo de ecuaciones lineales.

Podemos aplicar este método para encontrar raíces a otra clase de polinomios, los *polinomios afines* sobre $\mathbb{F}_{q^m}$.

Definición 2.2. Un *polinomio afín* sobre $\mathbb{F}_{q^m}$ es un polinomio de la forma $A(x) = L(x) - \alpha$, donde $L(x)$ es un polinomio linealizado sobre $\mathbb{F}_{q^m}$ y $\alpha \in \mathbb{F}_{q^m}$.

Se deduce de la definición que el elemento $\beta \in \mathbb{F}_{q^m}$ es raíz del polinomio $A(x)$ si y sólo si $L(\beta) = \alpha$. Además, recordamos que la ecuación $L(\beta) = \alpha$ es equivalente a $(c_1, \ldots, c_m)B = (d_1, \ldots, d_m)$, donde $\alpha = \sum_{i=1}^{m} d_i\beta_k$ (con la notación de (2.8)). Este sistema de ecuaciones se resuelve para $c_1, \ldots, c_m$, y cada solución vectorial $(c_1, \ldots, c_m)$ se corresponde con una raíz $\beta = \sum_{j=1}^{m} c_j\beta_j$ de $A(x)$ en $\mathbb{F}_{q^m}$.

El hecho de que las raíces de los polinomios afines se determinen más fácilmente sugiere el siguiente *método para hallar las raíces* en $\mathbb{F}_{q^m}$ de un polinomio cualquiera $f(x)$ no nulo sobre $\mathbb{F}_{q^m}$. Veamos en tres pasos cómo se haría:

1. Se determina un polinomio afín no nulo $A(x)$ sobre $\mathbb{F}_{q^m}$ divisible por $f(x)$. Veamos cómo lo haríamos.

   Sea $n \geq 1$ el grado de $f(x)$. Para cada $i = 0, 1, \ldots, n-1$, se calcula el único polinomio $r_i(x) \in \mathbb{F}_{q^m}[x]$ de grado menor que n tal que $x^{q^i} \equiv r_i(x) \mod f(x)$. Este polinomio existe y es único para cada i, por la división euclídea de x^{q^i} por $f(x)$.

   A continuación, se determinan elementos $\alpha_i \in \mathbb{F}_{q^m}$, no todos nulos, tales que $\sum_{i=0}^{n-1} \alpha_i r_i(x)$ sea un polinomio constante. De este modo, tenemos un sistema homogéneo de $n-1$ ecuaciones lineales con n incógnitas $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$. Por tanto, debe tener al menos una solución.

   Así, llegamos a una solución no trivial y podemos definir $\alpha = \sum_{i=0}^{n-1} \alpha_i r_i(x)$ con $\alpha \in \mathbb{F}_{q^m}$. Por tanto,

   $$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n-1} \alpha_i r_i(x) \equiv \alpha \mod f(x),$$

   y en consecuencia, tenemos que

   $$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$$

   es un polinomio afín no nulo sobre $\mathbb{F}_{q^m}$, divisible por $f(x)$. Además, es claro que podemos tomar $A(x)$ como un polinomio mónico.

2. Se hallan todas las raíces de $A(x)$ en $\mathbb{F}_{q^m}$ mediante el método descrito anteriormente (para encontrar raíces de polinomios afines).

3. Se calcula $f(\beta)$ para todas las raíces $\beta \in \mathbb{F}_{q^m}$ de $A(x)$, teniendo en cuenta que las raíces de $f(x)$ están entre las raíces de $A(x)$, con el fin de localizarlas.

Al igual que hicimos para los polinomios linealizados, describiremos el conjunto de las raíces de un polinomio afín.

Teorema 2.3. *Sea $A(x)$ un polinomio afín no nulo sobre $\mathbb{F}_{q^m}$. Consideremos una extensión $\mathbb{F}_{q^s}$ del cuerpo $\mathbb{F}_{q^m}$, que contiene todas las raíces de $A(x)$ (sabemos que existe tal extensión por el Corolario 1.2). Entonces,*

- *Todas las raíces de $A(x)$ tienen la misma multiplicidad: 1 o bien una potencia de q.*
- *El conjunto de las raíces de $A(x)$ conforma un subespacio afín (es decir, una traslación de un espacio lineal) de $\mathbb{F}_{q^s}$, visto como espacio vectorial sobre $\mathbb{F}_q$.*

Demostración. El primer punto, sobre la multiplicidad de las raíces, se demuestra de manera similar para el Teorema 2.1.

Por otro lado, sea $A(x) = L(x) - \alpha$, donde $L(x)$ es un polinomio linealizado sobre $\mathbb{F}_{q^m}$. Tomamos una raíz β de $A(x)$. Entonces $\gamma \in \mathbb{F}_{q^s}$ es raíz de $A(x)$ si y sólo si $L(\gamma) = \alpha = L(\beta)$, lo cual ocurre si y sólo si $L(\gamma - \beta) = 0$, es decir, si $\gamma \in \beta + U$, donde U es el subespacio lineal de $\mathbb{F}_{q^s}$ formado por las raíces de $L(x)$ (ver el Teorema 2.1). Por lo tanto, las raíces de $A(x)$ forman un subespacio afín de $\mathbb{F}_{q^s}$.

□

Teorema 2.4. *Sea T un subespacio afín de $\mathbb{F}_{q^m}$, visto como espacio vectorial sobre $\mathbb{F}_q$. Entonces, para cualquier entero $k \geq 0$, el polinomio*

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k}$$

es un polinomio afín sobre $\mathbb{F}_{q^m}$.

Demostración. Sea $T = \eta + U$, donde U es un subespacio lineal de $\mathbb{F}_{q^m}$. Entonces:

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

es un polinomio linealizado sobre $\mathbb{F}_{q^m}$, según el Teorema 2.2. Además,

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k} = \prod_{\beta \in U} (x - \eta - \beta)^{q^k} = L(x - \eta),$$

y $L(x - \eta)$ es claramente un polinomio afín sobre $\mathbb{F}_{q^m}$. □

2.2. Operaciones e irreducibilidad

El producto de polinomios linealizados no es necesariamente un polinomio linealizado. Sin embargo, la composición de dos polinomios linealizados $L_1(x), L_2(x)$ sobre $\mathbb{F}_{q^m}$ sí lo es. Por tanto, definiremos la *operación de composición*

$$L_1(x) \circ L_2(x) = L_1(L_2(x)).$$

Daremos otra definición relacionada con esta operación, teniendo en cuenta que no se trata de una operación conmutativa.

Definición 2.3. Diremos que el polinomio linealizado $L(x)$ es *divisible por la derecha* (para la operación de composición) o bien *divisible simbólicamente por la derecha* por el q-polinomio $L_2(x)$ si existe un q-polinomio $L_1(x)$ tal que $L(x) = L_1(x) \circ L_2(x)$. De manera análoga definimos la divisibilidad por la izquierda.

La siguiente proposición concreta la estructura que tendrá este conjunto de polinomios, con las operaciones de suma y composición descritas.

Proposición 2.2. *El conjunto de q-polinomios sobre $\mathbb{F}_{q^m}$ forma un anillo con la suma habitual y la composición como operaciones. Además, el elemento unidad en este anillo es el polinomio x y lo denotaremos por $\mathbb{L}_{q^m}[x]$.*

Definición 2.4. Los polinomios

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{y} \quad L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

sobre $\mathbb{F}_{q^m}$ son *polinomios asociados* entre sí. Más específicamente, $l(x)$ es el *polinomio asociado convencional* de $L(x)$, y $L(x)$ es el *polinomio asociado linealizado* de $l(x)$.

Veamos ahora una interesante propiedad relacionada con la anterior definición.

Lema 2.2. *Sean $L_1(x)$ y $L_2(x)$ polinomios linealizados sobre $\mathbb{F}_q$, con asociados convencionales $l_1(x)$ y $l_2(x)$ respectivamente. Entonces, $l(x) = l_1(x)l_2(x)$ y $L(x) = L_1(x) \circ L_2(x)$ son también asociados entre sí.*

Demostración. Las igualdades

$$l(x) = \sum_i a_i x^i = \sum_j b_j x^j \sum_k c_k x^k = l_1(x)l_2(x)$$

y

$$L(x) = \sum_i a_i x^{q^i} = \sum_j b_j \left(\sum_k c_k x^{q^k} \right)^{q^j} = \sum_j b_j \sum_k c_k x^{q^{j+k}} = L_1(x) \circ L_2(x)$$

son verdaderas si, y sólo si,

$$a_i = \sum_{j+k=i} b_j c_k \quad \text{para todo } i.$$

□

El siguiente criterio es una consecuencia inmediata del Lema 2.2.

Corolario 2.1. *Sean $L_1(x)$ y $L(x)$ polinomios linealizados sobre $\mathbb{F}_q$ con polinomios asociados convencionales $l_1(x)$ y $l(x)$ respectivamente. Entonces, $L_1(x)$ divide simbólicamente a $L(x)$ si, y sólo si, $l_1(x)$ divide a $l(x)$.*

Demostración. Se deduce directamente de la demostración del lema anterior. Lo vemos brevemente:

- Si $L_1(x)$ divide simbólicamente a $L(x)$ entonces existe $L_2(x)$ tal que $L(x) = L_1(x) \circ L_2(x)$, es decir,

  $$L(x) = \sum_i a_i x^{q^i} = \sum_j b_j \left(\sum_k c_k x^{q^k} \right)^{q^j} = \sum_j b_j \sum_k c_k x^{q^{j+k}} = L_1(x) \circ L_2(x).$$

  Por tanto, es cierto que

  $$l(x) = \sum_i a_i x^i = \sum_j b_j x^j \sum_k c_k x^k = l_1(x)l_2(x)$$

- Si $l_1(x)$ divide a $l(x)$, se probaría de manera similar que $L_1(x)$ divide simbólicamente a $L(x)$.

□

Ahora trataremos de ampliar el resultado anterior para seguir avanzando en la búsqueda de las similitudes entre los conceptos de divisibilidad respecto de la operación de producto habitual y respecto de la operación de composición para polinomios linealizados.

Teorema 2.5. *Sean $L_1(x)$ y $L(x)$ q-polinomios sobre $\mathbb{F}_q$ con q-asociados convencionales $l_1(x)$ y $l(x)$. Entonces, las siguientes propiedades son equivalentes:*

(i) $L_1(x)$ divide simbólicamente a $L(x)$.

(ii) $L_1(x)$ divide a $L(x)$ en el sentido ordinario.

(iii) $l_1(x)$ *divide a* $l(x)$.

Demostración. La equivalencia de (i) y (iii) se estableció en el Corolario 2.1. Basta probar la equivalencia de (i) y (ii).

($\Rightarrow$) Supongamos que $L_1(x)$ divide simbólicamente a $L(x)$, entonces

$$L(x) = L_1(x) \circ L_2(x) = L_2(x) \circ L_1(x) = L_2(L_1(x))$$

para cierto q-polinomio $L_2(x) = \sum_{i=0}^{n} a_i x^{q^i}$ sobre $\mathbb{F}_q$. Entonces,

$$L(x) = a_0 L_1(x) + a_1 L_1(x)^q + \cdots + a_n L_1(x)^{q^n},$$

y es claro que $L_1(x)$ divide a $L(x)$ en el sentido ordinario.

($\Leftarrow$) Si $L_1(x)$, supuesto no nulo, divide a $L(x)$ en el sentido ordinario. Usando el algoritmo de división euclídea, escribimos $l(x) = k(x)l_1(x) + r(x)$, donde $\deg(r(x)) < \deg(l_1(x))$. Tomando los q-asociados linealizados obtenemos

$$L(x) = K(x) \circ L_1(x) + R(x).$$

Por hipótesis $L_1(x)$ divide a $K(x) \circ L_1(x)$ y a $R(x)$ (en el sentido ordinario). Sin embargo, $\deg(R(x)) < \deg(L_1(x))$, luego $R(x)$ debe ser el polinomio cero. Así, concluimos que $L(x) = K(x) \circ L_1(x)$ y $L_1(x)$ divide simbólicamente a $L(x)$.

□

Aplicamos este resultado en el contexto de los polinomios irreducibles, con el objetivo de establecer una relación entre estos y los factores irreducibles de sus q-asociados linealizados. Para ello, damos en primer lugar una definición asociada a polinomios.

Definición 2.5. Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio no constante tal que $f(0) \neq 0$. El *orden* de $f(x)$, denotado por $\mathrm{ord}(f(x))$, es el menor entero positivo e tal que

$$f(x) \mid x^e - 1.$$

En caso de que $f(0) = 0$, se define el $\mathrm{ord}(f(x)) = 0$.

Teorema 2.6. *Sea* $f(x)$ *irreducible en* $\mathbb{F}_q[x]$ *y sea* $F(x)$ *su q-asociado linealizado. Entonces el grado de todo factor irreducible de* $F(x)/x$ *en* $\mathbb{F}_q[x]$ *es igual al orden de* $f(x)$.

Demostración. Veamos dos casos:

- Si $f(0) = 0$, entonces $x \mid f(x)$ y, necesariamente, $f(x) = x$ por ser $f(x)$ irreducible en $\mathbb{F}_q[x]$. Además, su q-asociado linealizado es $F(x) = x$, y por tanto,

  $$\frac{F(x)}{x} = \frac{x}{x} = 1,$$

  que es un polinomio irreducible de grado 0. Además, según la Definición 2.5, $\mathrm{ord}(f(x)) = 0$ en este caso particular.

- Asumimos ahora que $f(0) \neq 0$. Sea $e = \mathrm{ord}(f(x))$, entonces $f(x)$ divide a $x^e - 1$, y por el Teorema 2.5, su asociado linealizado $F(x)$ divide a $x^{q^e} - x$.

  Ahora, tomamos $h(x) \in \mathbb{F}_q[x]$ un factor irreducible de $F(x)/x$ de grado d, de modo que $h(x)$ divide $x^{q^e} - x$. El polinomio $h(x) \in \mathbb{F}_q[x]$ es entonces un factor irreducible de $x^{q^e} - x$. Veamos que de ello deriva que $\deg(h(x)) = d$ divide a e.

Sea α una raíz de h en la extensión de $\mathbb{F}_q$ que contiene todas las raíces de f. Entonces, $\alpha^{q^d} = \alpha$, luego $\alpha \in \mathbb{F}_{q^d}$. Por tanto, como el grado de la extensión $\mathbb{F}_q(\alpha)$ sobre $\mathbb{F}_q$ es d y el grado de la extensión $\mathbb{F}_{q^e}$ sobre $\mathbb{F}_q$ es e, necesariamente d divide a e.

Por otro lado, por el algoritmo de división euclídea,

$$x^d - 1 = g(x)f(x) + r(x),$$

con $g(x), r(x) \in \mathbb{F}_q[x]$ y $\deg(r(x)) < \deg(f(x))$.

Tomando los q-asociados linealizados, obtenemos

$$x^{q^d} - x = G(x) \circ F(x) + R(x),$$

y como $h(x)$ (polinomio irreducible de grado d) divide a $x^{q^d} - x$ y a $G(x) \circ F(x)$, se sigue que $h(x)$ divide a $R(x)$.

Supongamos que $r(x) \neq 0$, entonces $r(x)$ y $f(x)$ son coprimos (dado que $f(x)$ es irreducible), y por la identidad de Bézout, existen polinomios $s(x), k(x) \in \mathbb{F}_q[x]$ tales que

$$s(x)r(x) + k(x)f(x) = 1.$$

Tomando los q-asociados linealizados,

$$S(x) \circ R(x) + K(x) \circ F(x) = x.$$

Como $h(x)$ divide tanto a $R(x)$ como a $F(x)$, esto implicaría que $h(x)$ divide a x, lo cual es imposible. Por tanto, $r(x) = 0$, y $f(x)$ divide a $x^d - 1$. Veamos ahora que esto implica que $e = \mathrm{ord}(f(x))$ divide a d.

Si $f(x)$ divide a $x^d - 1$, $e = \mathrm{ord}(f(x)) \leq d$, luego por el algoritmo de división euclídea, $d = me + r$, con $m \in \mathbb{N}$ y $0 \leq r < e$, y tenemos que

$$x^d - 1 = (x^{me+r} - 1) = (x^{me} - 1)x^r + (x^r - 1).$$

Por tanto, $f(x)$ divide a $x^r - 1$ y, necesariamente, debe ser $r = 0$. Así, concluimos que e divide a d.

En conjunto, hemos llegado a que $d = e$.

□

Daremos ahora varias definiciones y resultados relacionados con la irreducibilidad de polinomios, dada la operación de composición de polinomios linealizados.

Definición 2.6. Decimos que un q-polinomio $L(x)$ sobre $\mathbb{F}_q$ de grado mayor que 1 es *simbólicamente irreducible* sobre $\mathbb{F}_q$ si la única descomposición de la forma $L(x) = L_1(x) \circ L_2(x)$ con q-polinomios $L_1(x), L_2(x)$ sobre $\mathbb{F}_q$ es aquella donde uno de los factores tiene grado 1.

Como observación, un polinomio simbólicamente irreducible es siempre reducible en el sentido ordinario, ya que todo polinomio linealizado de grado mayor que 1 tiene el factor no trivial x. Veamos ahora de qué manera están relacionados los polinomios q-asociados en cuanto a irreducibilidad simbólica.

Proposición 2.3. *Sea $L(x)$ un q-polinomio, es simbólicamente irreducible sobre $\mathbb{F}_q$ si y solo si su q-asociado convencional $l(x)$ es irreducible sobre $\mathbb{F}_q$.*

Demostración. Se demuestra inmediatamente del Lema 2.2. □

Proposición 2.4. *Todo q-polinomio $L(x)$ sobre $\mathbb{F}_q$ de grado mayor que 1 tiene una factorización simbólica en q-polinomios simbólicamente irreducibles sobre $\mathbb{F}_q$, y esta factorización es única (salvo reordenación de factores y multiplicación por elementos no nulos de $\mathbb{F}_q$).*

Demostración. Para obtener la factorización simbólica de $L(x)$, basta escribir la factorización canónica en $\mathbb{F}_q[x]$ de su q-asociado convencional $l(x)$, que es única, y tomar los q-asociados linealizados (empleando la correspondencia entre polinomios linealizados asociados del Lema 2.2). □

Continuamos con otra definición relevante y algunos resultados derivados de ella.

Definición 2.7. Dados dos o más q-polinomios sobre $\mathbb{F}_q$, no todos ellos nulos, podemos definir su *máximo común divisor simbólico* como el q-polinomio mónico sobre $\mathbb{F}_q$ de mayor grado que divide simbólicamente a todos ellos.

Tratamos ahora de relacionar este nuevo concepto con el de máximo común divisor ordinario analizando el conjunto de sus raíces.

Proposición 2.5. *El máximo común divisor ordinario y el máximo común divisor simbólico son idénticos.*

Demostración. Dados dos o más q-polinomios sobre $\mathbb{F}_q$, no todos ellos nulos, sabemos que las raíces de su máximo común divisor son exactamente las raíces comunes de los q-polinomios dados. Como la intersección de subespacios lineales es otro subespacio lineal, el conjunto de las raíces del máximo común divisor forman un subespacio lineal en alguna extensión $\mathbb{F}_{q^m}$, visto como espacio vectorial sobre $\mathbb{F}_q$.

Además, aplicando la primera parte del Teorema 2.1 a los q-polinomios dados, concluimos que cada raíz del máximo común divisor tiene la misma multiplicidad, que es 1 o una potencia de q. Por lo tanto, el Teorema 2.2 asegura que el máximo común divisor es un q-polinomio.

Se deduce entonces del Teorema 2.5 que el máximo común divisor ordinario y el máximo común divisor simbólico coinciden, dado que los conceptos de divisibilidad para polinomios linealizados basados en las operaciones de multiplicación ordinaria y simbólica son equivalentes. □

Para calcular el máximo común divisor (simbólico) de q-polinomios sobre $\mathbb{F}_q$ se pueden considerar sus q-asociados convencionales, determinar su máximo común divisor ordinario, y luego considerar el q-asociado linealizado.

Definición 2.8. Un espacio vectorial de dimensión finita M sobre $\mathbb{F}_q$, contenido en alguna extensión de $\mathbb{F}_q$, se denomina *q-módulo* si verifica la siguiente propiedad: la q-ésima potencia de cualquier elemento de M pertenece también a M.

Partiendo de este concepto, podemos establecer el siguiente criterio que nos permitirá identificar polinomios linealizados sobre $\mathbb{F}_q$.

Teorema 2.7. *El polinomio mónico $L(x)$ es un q-polinomio sobre $\mathbb{F}_q$ si y solo si cada raíz de $L(x)$ tiene la misma multiplicidad, que es 1 o una potencia de q, y además las raíces forman un q-módulo.*

Demostración. Veamos cada una de las implicaciones:

($\Rightarrow$) Si $L(x)$ es un q-polinomio mónico no nulo, sabemos por el Teorema 2.1 que cada raíz de $L(x)$ tiene la misma multiplicidad, que es 1 o una potencia de q, y que sus raíces sobre $\mathbb{F}_q$ forman un espacio vectorial sobre $\mathbb{F}_q$. Además, verifican que la q-ésima potencia de una raíz es también una raíz de $L(x)$, dado que la aplicación $x \longrightarrow x^q$ sobre el espacio de raíces es $\mathbb{F}_q-$lineal.

($\Leftarrow$) Si cada raíz de $L(x)$ tiene la misma multiplicidad, que es 1 o una potencia de q, y las raíces forman un q-módulo M, entonces, por el Teorema 2.2, $L(x)$ es un q-polinomio sobre alguna extensión de $\mathbb{F}_q$. Por tanto,

$$L(x) = \prod_{\beta \in M} (x - \beta)^{q^k}$$

para algún entero $k \geq 0$. Como $M = \{\beta^q : \beta \in M\}$, se tiene

$$L(x)^q = \prod_{\beta \in M} (x^q - \beta^q)^{q^k} = \prod_{\beta \in M} (x^q - \beta)^{q^k} = L(x^q).$$

Por otro lado, si

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i},$$

entonces

$$\sum_{i=0}^{n} \alpha_i^q x^{q^{i+1}} = L(x)^q = L(x^q) = \sum_{i=0}^{n} \alpha_i x^{q^{i+1}}.$$

De este modo, para todo $0 \leq i \leq n$ se tiene que $\alpha_i^q = \alpha_i$, luego $\alpha_i \in \mathbb{F}_q$. En conclusión, $L(x)$ es un q-polinomio sobre $\mathbb{F}_q$.

□

Cualquier q-polinomio sobre $\mathbb{F}_q$ de grado q es simbólicamente irreducible sobre $\mathbb{F}_q$. Veamos cómo podemos caracterizar polinomios simbólicamente irreducibles de grado mayor que q empleando la noción de q-módulo.

Teorema 2.8. *Un q-polinomio $L(x)$ sobre $\mathbb{F}_q$ de grado mayor que q es simbólicamente irreducible sobre $\mathbb{F}_q$ si y sólo si se verifican las siguientes condiciones:*

- *Las raíces de $L(x)$ son simples.*
- *El q-módulo M formado por las raíces de $L(x)$ no contiene ningún q-módulo distinto de $\{0\}$ y de sí mismo.*

Demostración. Veamos las dos implicaciones:

($\Rightarrow$) Supongamos que $L(x)$ es simbólicamente irreducible sobre $\mathbb{F}_q$.

En primer lugar, razonamos por reducción al absurdo para ver que $L(x)$ tiene únicamente raíces simples. Supongamos que tiene raíces múltiples. Por el Teorema 2.7, $L(x) = L_1(x)^q$ siendo $L_1(x)$ un q-polinomio sobre $\mathbb{F}_q$ de grado mayor que 1. Entonces sería $L(x) = x^q \circ L_1(x)$, lo que contradice la irreducibilidad simbólica de $L(x)$. Así, $L(x)$ tiene sólo raíces simples.

En segundo lugar, tomamos N un q-módulo contenido en M. De nuevo, el Teorema 2.7 muestra que

$$L_2(x) = \prod_{\beta \in N} (x - \beta)$$

es un q-polinomio sobre $\mathbb{F}_q$. Como $L_2(x)$ divide a $L(x)$ en el sentido ordinario, entonces $L_2(x)$ divide simbólicamente a $L(x)$ por el Teorema 2.5. Además, partimos de que $L(x)$ es simbólicamente irreducible sobre $\mathbb{F}_q$, por lo que $\deg(L_2(x))$ debe ser 1 o $\deg(L(x))$. Esto equivale a decir que N es o bien $\{0\}$ o bien M.

($\Leftarrow$) Tomamos una descomposición simbólica $L(x) = L_1(x) \circ L_2(x)$, siendo $L_1(x), L_2(x)$ q-polinomios sobre $\mathbb{F}_q$. Así, $L_1(x)$ divide simbólicamente a $L(x)$, y también lo divide en el sentido ordinario por el Teorema 2.5.

Se sigue que $L_1(x)$ solo tiene raíces simples y que el q-módulo N formado por las raíces de $L_1(x)$ está contenido en M. En consecuencia, N es $\{0\}$ o M. Por tanto, $\deg(L_1(x))$ es 1 o $\deg(L(x))$, lo que implica que $L_1(x)$ o bien $L_2(x)$ tiene grado 1. En conclusión, $L(x)$ es simbólicamente irreducible sobre $\mathbb{F}_q$.

□

Definición 2.9. Sea $L(x)$ un q-polinomio no nulo sobre $\mathbb{F}_{q^m}$. Una raíz ζ de $L(x)$ se denomina *raíz q-primitiva sobre $\mathbb{F}_{q^m}$* si no es raíz de ningún otro q-polinomio sobre $\mathbb{F}_{q^m}$ no nulo y de menor grado.

Otra forma de entender el concepto anterior es la siguiente. Sea $g(x)$ el polinomio mínimo de ζ sobre $\mathbb{F}_{q^m}$. Entonces ζ es una raíz q-primitiva de $L(x)$ sobre $\mathbb{F}_{q^m}$ si y solo si $g(x)$ divide a $L(x)$ y $g(x)$ no divide a ningún otro q-polinomio sobre $\mathbb{F}_{q^m}$ no nulo y de menor grado.

Proposición 2.6. *Sea ζ un elemento de una extensión finita del cuerpo $\mathbb{F}_{q^m}$. Siempre se puede encontrar un q-polinomio no nulo sobre $\mathbb{F}_{q^m}$ para el cual ζ sea una raíz q-primitiva sobre $\mathbb{F}_{q^m}$.*

Demostración. Buscamos tal q-polinomio. Sea $g(x)$ el polinomio mínimo de ζ sobre $\mathbb{F}_{q^m}$, y sea n el grado de $g(x)$. Para $i = 0, 1, \ldots, n$, se calcula el único polinomio $r_i(x)$ de grado menor que n tal que $x^{q^i} \equiv r_i(x) \mod g(x)$. Luego se determinan elementos $\alpha_i \in \mathbb{F}_{q^m}$, no todos nulos, tales que $\sum_{i=0}^{n} \alpha_i r_i(x) = 0$. Esto nos lleva a un sistema homogéneo de n ecuaciones lineales, ya que $\deg(r_i(x)) \leq n-1$ y tendremos n coeficientes (que acompañan a los x^j, con $0 \leq j \leq n-1$) que se deben anular. Además, el sistema tiene $n+1$ incógnitas $\alpha_0, \ldots, \alpha_n$, lo que nos lleva a concluir que existe solución no trivial. Así obtenemos

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n} \alpha_i r_i(x) \equiv 0 \mod g(x),$$

que se trata de un q-polinomio no nulo sobre $\mathbb{F}_{q^m}$ divisible por $g(x)$. Si se eligen los α_i de manera que $L(x)$ sea mónico y de menor grado posible, entonces ζ es una raíz q-primitiva de $L(x)$ sobre $\mathbb{F}_{q^m}$. □

En la siguiente definición damos nombre al polinomio $L(x)$ al que hacemos referencia en la proposición anterior.

Definición 2.10. Denominamos *polinomio q-mínimo* de ζ sobre $\mathbb{F}_{q^m}$ al único q-polinomio no nulo para el cual ζ es una raíz q-primitiva sobre $\mathbb{F}_{q^m}$. Dicho de otro modo, es el q-polinomio de menor grado positivo y divisible por el polinomio mínimo de ζ sobre $\mathbb{F}_{q^m}$.

Teorema 2.9. *Sea ζ un elemento de una extensión finita del cuerpo $\mathbb{F}_{q^m}$, y sea $M(x)$ su polinomio q-mínimo sobre $\mathbb{F}_{q^m}$. Entonces un q-polinomio $K(x)$ sobre $\mathbb{F}_{q^m}$ tiene a ζ como raíz si y sólo si $K(x) = L(x) \circ M(x)$ para algún q-polinomio $L(x)$ sobre $\mathbb{F}_{q^m}$.*

En particular, cuando $m = 1$, esto significa que $K(x)$ tiene a ζ como raíz si y sólo si $K(x)$ es simbólicamente divisible por $M(x)$.

Demostración. La primera implicación es sencilla de probar: si $K(x) = L(x) \circ M(x) = L(M(x))$, se tiene inmediatamente que $K(\zeta) = L(M(\zeta)) = L(0) = 0$, por ser $M(x)$ polinomio q-mínimo de ζ.

Veamos la implicación recíproca. Sea el q-polinomio mónico

$$M(x) = \sum_{j=0}^{t} \gamma_j x^{q^j}, \quad \text{con } \gamma_t = 1,$$

y supongamos que

$$K(x) = \sum_{h=0}^{r} \alpha_h x^{q^h}, \quad \text{con } r \geq t,$$

tiene a ζ como raíz.

Sea $s = r - t$ y $\gamma_j = 0$ si $j < 0$. Consideramos el siguiente sistema de $s+1$ ecuaciones lineales en las $s+1$ incógnitas $\beta_0, \beta_1 \ldots, \beta_s$:

$$\begin{aligned}
\beta_0 + \gamma_{t-1}^{q}\beta_1 + \gamma_{t-2}^{q^2}\beta_2 + \cdots + \gamma_{t-s}^{q^s}\beta_s &= \alpha_t \\
\beta_1 + \gamma_{t-1}^{q^2}\beta_2 + \cdots + \gamma_{t-s+1}^{q^s}\beta_s &= \alpha_{t+1} \\
&\vdots \\
\beta_{s-1} + \gamma_{t-1}^{q^s}\beta_s &= \alpha_{r-1} \\
\beta_s &= \alpha_r.
\end{aligned}$$

De este sistema obtenemos los valores únicos $\beta_0, \beta_1 \ldots, \beta_s \in \mathbb{F}_{q^m}$. Definimos

$$L(x) = \sum_{i=0}^{s} \beta_i x^{q^i}, \quad \text{y} \quad R(x) = K(x) - L(M(x)).$$

Entonces,

$$\begin{aligned}
R(x) &= \sum_{h=0}^{r} \alpha_h x^{q^h} - \left(\sum_{i=0}^{s} \beta_i \left(\sum_{j=0}^{t} \gamma_j x^{q^j} \right)^{q^i} \right) \\
&= \sum_{h=0}^{r} \alpha_h x^{q^h} - \sum_{i=0}^{s} \beta_i \sum_{j=0}^{t} \gamma_j^{q^i} x^{q^{i+j}} \\
&= \sum_{h=0}^{r} \alpha_h x^{q^h} - \sum_{h=0}^{r} \left(\sum_{i=0}^{s} \gamma_{h-i}^{q^i} \beta_i \right) x^{q^h} \\
&= \sum_{h=0}^{r} \left(\alpha_h - \sum_{i=0}^{s} \gamma_{h-i}^{q^i} \beta_i \right) x^{q^h}.
\end{aligned}$$

Por lo tanto, se anulan los coeficientes que acompañan a x^{q^h}, para $t \leq h \leq r$ (teniendo en cuenta las combinaciones lineales del sistema de ecuaciones de arriba), luego $R(x)$ tiene grado menor que q^t . Pero como $R(\zeta) = K(\zeta) - L(M(\zeta)) = 0 - 0 = 0$, $R(x)$ es necesariamente el polinomio nulo por definición de $M(x)$ como polinomio q-mínimo sobre $\mathbb{F}_{q^m}$, y se sigue que

$$K(x) = L(M(x)) = L(x) \circ M(x).$$

□

2.3. Elementos normales y raíces q-primitivas

Nos enfrentamos ahora al problema de determinar el *número N_L de raíces q-primitivas* sobre $\mathbb{F}_q$ de un q-polinomio no nulo $L(x)$ sobre $\mathbb{F}_q$.

Proposición 2.7. *El número de raíces q-primitivas sobre $\mathbb{F}_q$ de un q-polinomio no nulo $L(x)$ sobre $\mathbb{F}_q$ es*

$$q^n(1-q^{-n_1})(1-q^{-n_2})\cdots(1-q^{-n_s}),$$

para ciertos $n_1,\ldots,n_s$.

Demostración. Distinguimos los dos siguientes casos:

- Si $L(x)$ tiene raíces múltiples, entonces por el Teorema 2.7 podemos escribir $L(x) = L_1(x)^q$, para cierto q-polinomio $L_1(x)$ sobre $\mathbb{F}_q$. Como toda raíz de $L(x)$ es también raíz de $L_1(x)$, se tiene $N_L = 0$.

- Suponemos que $L(x)$ tiene sólo raíces simples. En primer lugar, si $L(x)$ tiene grado 1 es claro que $N_L = 1$. Veamos el caso de que tenga grado $q^n > 1$ (lo consideramos mónico s.p.g). Sea

$$L(x) = \underbrace{L_1(x)\circ\cdots\circ L_1(x)}_{e_1}\circ\cdots\circ\underbrace{L_r(x)\circ\cdots\circ L_r(x)}_{e_r}$$

la factorización simbólica de $L(x)$ con $L_i(x)$ mónicos, irreducibles simbólicamente y distintos sobre $\mathbb{F}_q$. Obtenemos N_L restando del número total de raíces (q^n) el número de raíces de $L(x)$ que ya lo son de algún q-polinomio no nulo sobre $\mathbb{F}_q$ de grado menor que q^n. Veamos cómo podemos hallar este número.

Si ζ es una raíz de $L(x)$ de este último tipo y $M(x)$ es el polinomio q-mínimo de ζ sobre $\mathbb{F}_q$, entonces $\deg(M(x)) < q^n$ y $M(x)$ divide simbólicamente a $L(x)$ por el Teorema 2.9.

Consideramos los polinomios $K_i(x)$, para cada $1 \le i \le r$, donde cada uno se obtiene al omitir los e_i factores $L_i(x)$ de la factorización simbólica de $L(x)$. Como $M(x)$ divide simbólicamente a $L(x)$, $M(x)$ divide simbólicamente a al menos uno de los polinomios $K_i(x)$, para el cual se verificará $K_i(\zeta) = 0$ (por el Teorema 2.9). Como toda raíz de $K_i(x)$ es también raíz de $L(x)$, se deduce que N_L es igual a q^n menos el número de elementos ζ que son raíces de algún $K_i(x)$.

Si q^{n_i} es el grado de $L_i(x)$, entonces el número de raíces de $K_i(x)$, es q^{n-n_i}. Tomamos los $i_1,\ldots,i_s$ índices distintos para los que $K_{i_t}(\zeta) = 0$. Entonces el número de raíces comunes de $K_{i_1}(x),\ldots,K_{i_s}(x)$ es igual al grado del máximo común divisor, que es también el grado del máximo común divisor simbólico por la Proposición 2.5.

Utilizando factorizaciones simbólicas, este grado es igual a

$$q^{n-n_{i_1}-\cdots-n_{i_j}}.$$

Aplicando el principio de inclusión-exclusión obtenemos:

$$N_L = q^n - \sum_{i=1}^{r} q^{n-n_i} + \sum_{1\le i<j\le r} q^{n-n_i-n_j} + \cdots + (-1)^r q^{n-n_1-\cdots-n_r},$$

es decir,

$$N_L = q^n(1-q^{-n_1})(1-q^{-n_2})\cdots(1-q^{-n_r}).$$

□

La expresión anterior, que da el valor de N_L también puede interpretarse de otra manera. Sea $l(x)$ el q-asociado convencional de $L(x)$ y sea la factorización canónica de $l(x)$ en $\mathbb{F}_q[x]$

$$l(x) = l_1(x)^{e_1} \cdots l_r(x)^{e_r},$$

donde $l_i(x)$ es el q-asociado convencional de $L_i(x)$.

Para realizar esta segunda interpretación es preciso recordar la definición de la función de Euler.

Definición 2.11. Dado $m \in \mathbb{N}$, la *función de Euler* $\phi(m)$ se define como el número de enteros k, con $1 \leq k \leq m$ tales que $\text{mcd}(k, m) = 1$.

Ahora, introducimos el concepto anterior en el contexto de los polinomios en $\mathbb{F}_q[x]$.

Definición 2.12. Dado un polinomio $f \in \mathbb{F}_q[x]$ no nulo, definimos la función

$$\Phi_q(f(x)) = \Phi_q(f)$$

donde $\Phi_q(f)$ es el número de polinomios en $\mathbb{F}_q[x]$ de grado menor que el de f y coprimos con f.

Ahora bien, dada la función Φ de arriba, se cumple la siguiente identidad para el número N_L de raíces q-primitivas sobre $\mathbb{F}_q$ de un q-polinomio no nulo $L(x)$ (siendo $l(x)$ su q-asociado convencional), que probaremos a continuación:

$$N_L = \Phi_q(l(x)).$$

Lema 2.3. *La función Φ_q definida para polinomios no nulos en $\mathbb{F}_q[x]$ tiene las siguientes propiedades:*

(i) $\Phi_q(f) = 1$ *si* $\deg(f) = 0$*;*

(ii) $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$ *siempre que f y g sean coprimos;*

(iii) Si $\deg(f) = n \geq 1$*, entonces*

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}),$$

donde los n_i son los grados de los polinomios mónicos irreducibles que aparecen en la factorización canónica de f en $\mathbb{F}_q[x]$.

Demostración.

- La propiedad (i) es trivial.
- Para la propiedad (ii), sea $\Phi_q(f) = s$ y $\Phi_q(g) = t$, y sean $f_1, \ldots, f_s$ y $g_1, \ldots, g_t$ los polinomios contados por $\Phi_q(f)$ y $\Phi_q(g)$, respectivamente. Dicho de otro modo, los polinomios en $\mathbb{F}_q[x]$ coprimos con f de grado $< \deg(f)$ y coprimos con g de grado $< \deg(g)$, respectivamente.

  Si $h \in \mathbb{F}_q[x]$ es un polinomio con $\deg(h) < \deg(fg)$ y $\text{mcd}(fg, h) = 1$, entonces $\text{mcd}(f, h) = \text{mcd}(g, h) = 1$. Por tanto $h \equiv f_i \mod f$, $h \equiv g_j \mod g$ para un único par ordenado (i, j), con $1 \leq i \leq s$, $1 \leq j \leq t$.

  De manera recíproca, dado un par (i, j), por el teorema de los restos chinos existe un único $h \in \mathbb{F}_q[x]$ tal que $h \equiv f_i \mod f$, $h \equiv g_j \mod g$, y $\deg(h) < \deg(fg)$. Este h satisface $\text{mcd}(f, h) = \text{mcd}(g, h) = 1$, luego $\text{mcd}(fg, h) = 1$.

  Así, hay una correspondencia biyectiva entre los st pares ordenados (i, j) y los polinomios $h \in \mathbb{F}_q[x]$ con $\deg(h) < \deg(fg)$ y $\text{mcd}(fg, h) = 1$. En consecuencia, $\Phi_q(fg) = st = \Phi_q(f)\Phi_q(g)$, como queríamos probar.

- La propiedad (iii) se deduce de la propiedad (ii) teniendo en cuenta lo siguiente. Consideramos la factorización canónica de f en $\mathbb{F}_q[x]$ y analizamos cada uno de los polinomios mónicos irreducibles $b \in \mathbb{F}_q[x]$. Sea m su grado y e un entero positivo (la potencia del polinomio en la factorización).

  En este caso, podemos calcular $\Phi_q(b^e)$ directamente. Los polinomios $h \in \mathbb{F}_q[x]$ con $\deg(h) < \deg(b^e) = em$ que no son coprimos con b^e son exactamente aquellos divisibles por b, y por tanto de la forma $h = gb$ con $\deg(g) < em - m$. Como hay q^{em-m} elecciones distintas para g, obtenemos $\Phi_q(b^e) = q^{em} - q^{em-m} = q^{em}(1 - q^{-m})$.

□

El siguiente teorema se deduce directamente del lema anterior y la Proposición 2.7.

Teorema 2.10. *Sea $L(x)$ un q-polinomio no nulo sobre $\mathbb{F}_q$ con q-asociado convencional $l(x)$. Entonces, el número de raíces q-primitivas de $L(x)$ sobre $\mathbb{F}_q$ es*

- $N_L = 0$ *si $L(x)$ tiene raíces múltiples*
- $N_L = \Phi_q(l(x))$ *si $L(x)$ tiene raíces simples.*

Corolario 2.2. *Todo q-polinomio no nulo sobre $\mathbb{F}_q$ con raíces simples tiene al menos una raíz q-primitiva sobre $\mathbb{F}_q$.*

El siguiente teorema nos permite aplicar el corolario anterior para construir una base de un q-módulo.

Teorema 2.11. *Sea M un q-módulo de dimensión $m \geq 1$ sobre $\mathbb{F}_q$. Entonces existe un elemento $\zeta \in M$ tal que $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ es una base de M sobre $\mathbb{F}_q$.*

Demostración. Según el Teorema 2.7, $L(x) = \prod_{\beta \in M}(x - \beta)$ es un q-polinomio sobre $\mathbb{F}_q$. Por el Corolario 2.2, $L(x)$ tiene una raíz q-primitiva ζ sobre $\mathbb{F}_q$ y los $\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}$ son elementos de M.

Razonaremos por reducción al absurdo suponiendo que estos elementos son linealmente dependientes sobre $\mathbb{F}_q$. En este caso, ζ es una raíz de un q-polinomio no nulo sobre $\mathbb{F}_q$ de grado menor que $q^m = \deg(L(x))$, lo que contradice la definición de raíz q-primitiva de $L(x)$ sobre $\mathbb{F}_q$. Por tanto, estos m elementos son linealmente independientes sobre $\mathbb{F}_q$ y forman una base de M sobre $\mathbb{F}_q$, dado que m es la dimensión del q-módulo M. □

Teorema 2.12. *En $\mathbb{F}_{q^m}$ existen exactamente $\Phi_q(x^m - 1)$ elementos ζ para los cuales*

$$\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\} \text{ es una base de } \mathbb{F}_{q^m} \text{ sobre } \mathbb{F}_q.$$

Demostración. Como $\mathbb{F}_{q^m}$ puede considerarse como un q-módulo, podemos aplicarle el argumento de la demostración del Teorema 2.11. Recordando la Proposición 1.3, consideramos

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^m}} (x - \beta) = x^{q^m} - x.$$

Cada raíz q-primitiva ζ de $L(x)$ sobre $\mathbb{F}_q$ genera una base de la forma $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$. Por otro lado, si $\zeta \in \mathbb{F}_{q^m}$ no es una raíz q-primitiva de $L(x)$, entonces $\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}$ son linealmente dependientes sobre $\mathbb{F}_q$, y por tanto no forman una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

En consecuencia, el número de elementos $\zeta \in \mathbb{F}_{q^m}$ tales que $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ conforma una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ es igual al número de raíces q-primitivas de $L(x)$ sobre $\mathbb{F}_q$, que viene dado por $\Phi_q(x^m - 1)$ según el Teorema 2.10. □

Capítulo 3

Códigos de Gabidulin

En este capítulo, ofreceremos una introducción a la métrica del rango (ver [13], Sección 2.3) y sus propiedades fundamentales aprovechando las nociones previas sobre cuerpos finitos, códigos lineales y polinomios linealizados. Incluiremos una versión análoga en el contexto de esta nueva métrica de determinados resultados, definiciones y cotas para los parámetros de un código definidas en la sección de Códigos Lineales [sección 1.2]. Entre otros conceptos, introduciremos el equivalente a la cota de Singleton en la métrica del rango y el de códigos de máxima distancia de rango (códigos MRD).

A continuación, definiremos los códigos de Gabidulin a través de la evaluación de polinomios linealizados. Estos códigos destacan por ser considerados el análogo, en la métrica de rango, de los códigos de Reed–Solomon que describimos en la métrica de Hamming. Esta analogía se basa en varios aspectos, como su construcción a partir de la evaluación de polinomios y su óptima distancia mínima. De hecho, veremos que los códigos de Gabidulin alcanzan una cota de tipo Singleton adaptada al contexto de la métrica de rango.

3.1. Métrica del rango

Para poder describir la métrica del rango y sus propiedades, debemos dar algunas definiciones y aclaraciones de notación. Empezaremos por describir el conjunto de todos los subespacios de $\mathbb{F}_q^m$ de dimensión $\tau \leq m$, que denotaremos por $\mathcal{G}_q(m,\tau)$. Denominaremos *coeficiente q-binomial* o *coeficiente binomial Gaussiano* al cardinal de $\mathcal{G}_q(m,\tau)$ y daremos un resultado que determina su valor.

Lema 3.1. *El número de subespacios de dimensión τ de $\mathbb{F}_q^m$ es*

$$\binom{m}{\tau}_q := |\mathcal{G}_q(m,\tau)| = \prod_{i=0}^{\tau-1} \frac{q^m - q^i}{q^\tau - q^i},$$

y se conoce como coeficiente q-binomial (ver [8]).

Demostración. Primero, elegimos un subespacio de dimensión τ del espacio de las filas $\mathbb{F}_q^m$. El número de formas de escoger una base de este subespacio, es decir, de escoger τ-uplas de vectores linealmente independientes en $\mathbb{F}_q^m$, es:

$$(q^m - 1)(q^m - q)\cdots(q^m - q^{\tau-1}) = \prod_{i=0}^{\tau-1}(q^m - q^i).$$

Sin embargo, hay diferentes bases que generan el mismo subespacio, por lo que debemos dividir

entre el número de bases ordenadas de $\mathbb{F}_q^\tau$, que es:

$$(q^\tau - 1)(q^\tau - q)\cdots(q^\tau - q^{\tau-1}) = \prod_{i=0}^{\tau-1}(q^\tau - q^i).$$

Así, el número total de subespacios de dimensión τ en $\mathbb{F}_q^m$ es el coeficiente q-binomial:

$$\binom{m}{\tau}_q = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{\tau-1})}{(q^\tau-1)(q^\tau-q)\cdots(q^\tau-q^{\tau-1})} = \frac{\prod_{i=0}^{\tau-1}(q^m-q^i)}{\prod_{i=0}^{\tau-1}(q^\tau-q^i)}.$$

□

Además, en este capítulo usaremos $\mathbb{F}_q^{s\times n}$ para denotar el conjunto de todas las matrices $s \times n$ sobre $\mathbb{F}_q$ y $\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{1\times n}$ para denotar el conjunto de todos los vectores fila de longitud n sobre $\mathbb{F}_{q^m}$.

Siguiendo con detalles de notación, vamos describir una aplicación biyectiva, que lleva elementos $\mathbf{a} \in \mathbb{F}_{q^m}^n$ en matrices $A \in \mathbb{F}_q^{m\times n}$.

Definición 3.1. Sea $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Fijamos un orden para esta base $\beta = (\beta_0\ \beta_1\ \ldots\ \beta_{m-1})$ y sea $\mathbf{a} \in \mathbb{F}_{q^m}^n$ un vector. La *extensión de* $\mathbf{a}$ *sobre el cuerpo base* viene dada por la siguiente aplicación biyectiva:

$$\mathrm{ext}_\beta : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n}$$

$$\mathbf{a} = (a_0\ a_1\ \ldots\ a_{n-1}) \mapsto A = \begin{pmatrix} A_{0,0} & A_{0,1} & \ldots & A_{0,n-1} \\ A_{1,0} & A_{1,1} & \ldots & A_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m-1,0} & A_{m-1,1} & \ldots & A_{m-1,n-1} \end{pmatrix}$$

donde $A \in \mathbb{F}_q^{m\times n}$ está definida de manera que satisface que:

$$a_j = \sum_{i=0}^{m-1} A_{i,j}\beta_i, \quad \forall j \in [0, n-1].$$

Dicho de otro modo, $\mathbf{a} = \beta \cdot A$.

Como observacion, vemos que si aplicamos ext_β a un único elemento $a \in \mathbb{F}_{q^m}$, este se transforma en un vector columna $\mathrm{ext}_\beta(a) \in \mathbb{F}_q^{m\times 1}$. Además, a lo largo del capítulo, llamaremos *palabras* a los vectores $\mathbf{a} \in \mathbb{F}_{q^m}^n$ y usaremos las siguientes notaciones para alternar entre la representación vectorial y matricial y las usaremos de forma intercambiable:

$$A = \mathrm{ext}_\beta(\mathbf{a}), \quad \mathbf{a} = \mathrm{ext}_\beta^{-1}(A).$$

Además, denotamos por $\mathrm{rk}(\mathbf{a})$ al rango de $A = \mathrm{ext}_\beta(\mathbf{a})$ sobre $\mathbb{F}_q$, y por $\mathcal{R}_q(A)$ y $\mathcal{C}_q(A)$ al espacio fila y al espacio columna de A sobre $\mathbb{F}_q$. El núcleo por columnas (núcleo derecho, $\ker(\mathbf{A}) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{Ax} = \mathbf{0}\}$) de una matriz se escribirá como $\ker(A)$, y por notación:

$$\ker(\mathbf{a}) = \ker(\mathrm{ext}_\beta(\mathbf{a})) = \ker(A).$$

Para cualquier matriz $A \in \mathbb{F}_q^{m\times n}$ (o bien vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$) se verifica:

$$\dim(\ker(A)) + \mathrm{rk}(A) = n.$$

Basándonos en esta biyectividad entre cada vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ y la matriz correspondiente $A \in \mathbb{F}_q^{m\times n}$, podemos dar las siguientes dos definiciones de peso y distancia en la métrica del rango.

Definición 3.2. Sean $\mathbf{a} = (a_0\ a_1\ \dots\ a_{n-1})$, $\mathbf{b} = (b_0\ b_1\ \dots\ b_{n-1}) \in \mathbb{F}_{q^m}^n$ y sean $A = \mathrm{ext}_\beta(\mathbf{a})$, $B = \mathrm{ext}_\beta(\mathbf{b}) \in \mathbb{F}_q^{m\times n}$ las representaciones matriciales con respecto a una base $\mathcal{B}$ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Se definen:

- El *peso de rango* de $\mathbf{a}$ como el rango de su representación matricial sobre $\mathbb{F}_q$, es decir,

$$\mathrm{wt}_R(\mathbf{a}) := \mathrm{rk}(\mathbf{a}) = \mathrm{rk}(A).$$

- La *distancia de rango* entre $\mathbf{a}$ y $\mathbf{b}$ como el rango de la diferencia de las dos representaciones matriciales, es decir,

$$d_R(\mathbf{a}, \mathbf{b}) := \mathrm{rk}(\mathbf{a} - \mathbf{b}) = \mathrm{rk}(A - B).$$

A continuación, probamos que la distancia del rango efectivamente cumple las condiciones necesarias para ser una distancia.

Lema 3.2. *La distancia de rango d_R descrita arriba es una métrica.*

Demostración. Dadas $A, B, C \in \mathbb{F}_q^{m\times n}$, se verifican las siguientes propiedades:

- No negatividad: El rango de cualquier matriz es un número entero no negativo, es decir,

$$\mathrm{rk}(A - B) \geq 0.$$

  Además, $\mathrm{rk}(A - B) = 0$ si y solo si $A - B$ es la matriz nula, lo que equivale a $A = B$.

- Simetría: Observamos que

$$\mathrm{rk}(A - B) = \mathrm{rk}(-(B - A)) = \mathrm{rk}(B - A),$$

  ya que el rango de una matriz no cambia al multiplicarla por un escalar no nulo, en particular por -1.

- Desigualdad triangular. Se utiliza la propiedad de que el rango de la suma de dos matrices no puede exceder a la suma de sus rangos individuales:

$$\mathrm{rk}(A + B) \leq \mathrm{rk}(A) + \mathrm{rk}(B), \quad \forall A, B \in \mathbb{F}_q^{m\times n}.$$

  Observamos que $A - C = (A - B) + (B - C)$, luego por lo anterior,

$$\mathrm{rk}(A - C) = \mathrm{rk}((A - B) + (B - C)) \leq \mathrm{rk}(A - B) + \mathrm{rk}(B - C).$$

Por lo tanto, la función $d_R(\mathbf{a}, \mathbf{b}) = \mathrm{rk}(A - B)$ satisface todas las propiedades de una métrica. □

Atendiendo a la métrica del rango, una *esfera de radio τ alrededor de una palabra* $\mathbf{a} \in \mathbb{F}_{q^m}^n$, $S_R^\tau(\mathbf{a}) = S_R^\tau(A)$, es el conjunto de todas las palabras a distancia de rango exactamente τ de $\mathbf{a}$; y una *bola de radio τ con centro la palabra* $\mathbf{a}$, $B_R^\tau(\mathbf{a}) = B_R^\tau(A)$, es el conjunto de todas las palabras a distancia de rango $\leq \tau$ de $\mathbf{a}$.

De este modo, el cardinal de $B_R^\tau(\mathbf{a})$ se puede obtener sumando los cardinales de las esferas en torno a $\mathbf{a}$ de radio desde $\mathbf{0}$ hasta τ. Para poder dar una fórmula concreta, hemos de dar un resultado previo.

Lema 3.3. *El número de matrices $m \times n$ sobre $\mathbb{F}_q$ de rango exactamente τ es*

$$\binom{m}{\tau}_q \prod_{j=0}^{\tau-1}(q^n - q^j),$$

donde $\binom{m}{\tau}_q$ es el coeficiente q-binomial (ver en [8]).

Demostración. Primero, para construir una matriz de rango τ, recordamos que el número total de subespacios de dimensión τ en $\mathbb{F}_q^m$ es el coeficiente q-binomial:

$$\binom{m}{\tau}_q = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{\tau-1})}{(q^\tau-1)(q^\tau-q)\cdots(q^\tau-q^{\tau-1})} = \frac{\prod_{i=0}^{\tau-1}(q^m-q^i)}{\prod_{i=0}^{\tau-1}(q^\tau-q^i)}.$$

Fijado un subespacio de dimensión τ en $\mathbb{F}_q^m$, consideramos una matriz $B \in \mathbb{F}_q^{m\times\tau}$ tal que sus columnas generan dicho subespacio. Entonces, todas las matrices en $\mathbb{F}_q^{m\times n}$ que tienen a dicho subespacio como espacio columna son de la forma $M = BA$, donde $A \in \mathbb{F}_q^{\tau\times n}$ recorre todas las matrices de rango τ. El número de formas de escoger una matriz de este tipo es

$$\prod_{j=0}^{\tau-1}(q^n - q^j).$$

Por lo tanto, el número total de matrices $m \times n$ de rango exactamente τ es:

$$\binom{m}{\tau}_q \prod_{j=0}^{\tau-1}(q^n - q^j).$$

□

Ayudándonos del lema anterior podemos determinar con facilidad los cardinales de la bola y la esfera de radio τ con centro en una palabra $\mathbf{a}$. Obtenemos lo siguiente:

$$|S_R^\tau(\mathbf{a})| = \binom{m}{\tau}\prod_{j=0}^{\tau-1}(q^n - q^j), \tag{3.1}$$

$$|B_R^\tau(\mathbf{a})| = \sum_{i=0}^{\tau}|S_R^i(\mathbf{a})| = \sum_{i=0}^{\tau}\binom{m}{i}\left(\prod_{j=0}^{i-1}(q^n - q^j)\right). \tag{3.2}$$

Observamos que los cardinales de $B_R^\tau(\mathbf{a})$ y $S_R^\tau(\mathbf{a})$ son independientes de la elección de la palabra central.

Introducimos ahora la idea de código en la métrica de rango. Recordamos la Definición 1.6 de código en bloque de longitud n y la Definición 1.7 de código lineal sobre $\mathbb{F}_{q^m}$ y sus parámetros fundamentales, $[n, k, d]$ (longitud n, dimensión k y distancia mínima de Hamming d). Vimos que un código lineal $[n, k, d]$ sobre $\mathbb{F}_{q^m}$ puede verse como un subespacio de $\mathbb{F}_{q^m}^n$ de dimensión k, y su cardinal es $M = q^{mk}$.

A continuación, damos las siguientes definiciones análogas para la métrica con la que estamos tratando.

Definición 3.3. Un *código en la métrica de rango* (no necesariamente lineal) sobre $\mathbb{F}_{q^m}$, denotado por $[n, M, d]_R$, es un código de longitud n, cadinal M y distancia mínima para la métrica del rango d.

Un *código lineal en la métrica de rango* de longitud n, dimensión k y distancia mínima d para la métrica del rango es un subespacio vectorial de $\mathbb{F}_{q^m}^n$ de dimensión k. Lo denotaremos por $[n, k, d]_R$.

Como observación, las palabras de los códigos definidos así pueden verse como vectores en $\mathbb{F}_{q^m}^n$, o equivalentemente como matrices en $\mathbb{F}_q^{m\times n}$. Ahora bien, para que lo anterior tenga sentido debemos dar la definición para la distancia mínima en la métrica del rango.

Definición 3.4. Dado un código $\mathcal{C}$, de tipo $[n, M, d]_R$ sobre $\mathbb{F}_q^m$, la *distancia de rango mínimo* viene dada por

$$d := \min_{\substack{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}\\ \mathbf{c}_1\neq\mathbf{c}_2}} \{d_R(\mathbf{c}_1, \mathbf{c}_2)\} = \min_{\substack{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}\\ \mathbf{c}_1\neq\mathbf{c}_2}} \{\mathrm{rk}(\mathbf{c}_1 - \mathbf{c}_2)\}.$$

Continuamos profundizando con algunos resultados para códigos lineales en el contexto de la métrica del rango.

Corolario 3.1. *Para un código lineal $[n, k, d]_R$ sobre $\mathbb{F}_{q^m}$, la distancia de rango mínimo es el peso de rango mínimo:*

$$d = \min_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{c}\neq\mathbf{0}}} \{\mathrm{wt}_R(\mathbf{c})\}.$$

Demostración. La distancia de rango entre dos palabras $\mathbf{c}_1$ y $\mathbf{c}_2$ de un código lineal $\mathcal{C}$ es

$$d_R(\mathbf{c}_1, \mathbf{c}_2) = \mathrm{rk}(\mathbf{c}_1 - \mathbf{c}_2).$$

Además, por la linealidad del código, $\mathbf{c}_1 - \mathbf{c}_2 \in \mathcal{C}$. Así, podemos minimizar la distancia de rango entre dos palabras distintas y equivaldrá a hallar el mínimo rango de una palabra no nula del código, es decir:

$$d = \min_{\substack{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}\\ \mathbf{c}_1\neq\mathbf{c}_2}} \mathrm{rk}(\mathbf{c}_1 - \mathbf{c}_2) = \min_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{c}\neq 0}} \mathrm{rk}(\mathbf{c}),$$

que es la definición de mínimo peso de rango. □

El siguiente teorema muestra que podemos caracterizar la distancia mínima de un código lineal en métrica de rango a partir de su matriz de control.

Teorema 3.1. *Sea $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ la matriz de control del código lineal $[n, k, d]_R$ sobre $\mathbb{F}_{q^m}$. Entonces $\mathcal{C}$ tiene distancia mínima de rango $d = \delta$ si y solo si se verifican las siguientes dos condiciones:*

1. *Para cualquier matriz $A \in \mathbb{F}_q^{(\delta-1)\times n}$ de rango $\delta - 1$, se tiene*

$$\mathrm{rk}(AH^t) = \delta - 1,$$

2. *Existe una matriz $B \in \mathbb{F}_q^{\delta\times n}$ de rango δ tal que*

$$\mathrm{rk}(BH^t) < \delta.$$

(Ver [2], Theorem 1)

Demostración. Tendremos en cuenta la definición de distancia mínima d y el hecho de que un vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ pertenece a $\mathcal{C}$ si y sólo si $H\mathbf{c}^t = 0$.

Por un lado, la condición de que para toda matriz $A \in \mathbb{F}_q^{(\delta-1)\times n}$ de rango $\delta - 1$ se cumpla

$$\mathrm{rk}(AH^t) = \delta - 1$$

equivale a afirmar que no existe ninguna palabra del código $\mathbf{c} \neq \mathbf{0}$ tal que $\mathrm{rk}(\mathbf{c}) < \delta$. En efecto, si existiera una palabra del código $\mathbf{c} \neq \mathbf{0}$ con rango $< \delta$, tendríamos $\mathbf{c} = \mathbf{x}A$ para algún $\mathbf{x} \in F_{q^m}^{\delta-1}$ y alguna matriz $A \in F_q^{\delta-1\times n}$. Por otro lado, como $\mathbf{c}H^t = \mathbf{0}$, entonces $\mathbf{x}AH^t = \mathbf{0}$, por tanto, $\mathrm{rk}(AH^t)$ no puede ser máximo, es decir, $\mathrm{rk}(AH^t) < \delta - 1$ y llegamos a contradicción con la condicion (1.).

Por otro lado, falta asegurar que existe una palabra de código de rango δ. Supongamos que existe una matriz $B \in \mathbb{F}_q^{\delta\times n}$ de rango δ tal que

$$\mathrm{rk}(BH^t) < \delta.$$

Esto implica que existe una combinación lineal no trivial de las filas de B que está en el núcleo de H. Esta combinación lineal conforma una palabra del código lineal $\mathbf{c} \in \mathcal{C}$ que tiene rango a lo sumo δ. Por tanto, como no existen vectores de rango menor que δ, este debe tener rango exactamente δ.

Así, concluimos que la distancia de rango mínima es $d = \delta = \mathrm{rk}(\mathbf{c})$. □

Por otro lado, recordamos el Teorema 1.4, donde definimos la *cota de Singleton*, y la Definición 1.27, donde nos referimos a los códigos MDS como aquellos que para los que se alcanza esa cota, es decir, para los que $d = n - k + 1$. En el siguiente teorema damos el equivalente para la métrica de rango.

Teorema 3.2. *Sea $\mathcal{C}$ un código $[n, M, d]_R$ sobre $\mathbb{F}_{q^m}$. Entonces el cardinal M de $\mathcal{C}$ está acotado de la siguiente manera:*

$$M \leq q^{\min\{n(m-d+1),\, m(n-d+1)\}} = q^{\max\{n,\, m\}\,\cdot\,(\min\{n,m\}-d+1)}. \tag{3.3}$$

(Ver en Theorem 5.4, [1])

Demostración. En el caso $M = 1$, el código tiene una sola palabra y el resultado es trivial, ya que $q^{\max\{n,m\}\,(\min\{n,m\}-d+1)} \geq 1$ para cualquier valor de n, m y d, y no es significativo el concepto de distancia mínima de rango. Suponemos que $M \geq 2$ y consideramos dos palabras distintas $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$. Por definición de distancia mínima de rango, sabemos que

$$\mathrm{rk}(A) = \mathrm{rk}(\mathbf{c}_1 - \mathbf{c}_2) \geq d,$$

siendo $A = \mathrm{ext}(\mathbf{c}_1 - \mathbf{c}_2) \in \mathbb{F}_q^{m\times n}$ la representación matricial de $\mathbf{c}_1 - \mathbf{c}_2$ con respecto a cierta base. Luego podemos afirmar que el $\ker(A)$ tiene dimensión a lo sumo $\min\{n, m\} - d$.

Ahora, fijamos un subespacio $V_0 \subseteq \mathbb{F}_q^n$ de dimensión $\min\{n, m\} - d + 1$ cualquiera. Dado que $\mathbf{c}_1$ y $\mathbf{c}_2$ son distintas, el subespacio V_0 no puede estar completamente contenido en el $\ker(A)$ (se cumple que $\dim(\ker(A)) \leq \min\{n, m\} - d < \dim(V_0)$).

Para cada palabra del código $\mathbf{c} \in \mathcal{C}$ o bien cada matriz asociada B, consideramos la aplicación lineal (de restricción al subespacio V_0):

$$\varphi_B : V_0 \subseteq \mathbb{F}_q^n \to \mathbb{F}_q^m, \quad v \mapsto B_{\mathbf{c}}v,$$

donde $v \in V_0$ es un vector columna. Como el $\ker(\mathbf{c}_1 - \mathbf{c}_2)$ tiene dimensión estrictamente menor que $\dim(V_0)$, existe al menos un vector $v_0 \in V_0$ para el cual $B_{\mathbf{c}_1}v_0 \neq B_{\mathbf{c}_2}v_0$. Dicho de otro modo, palabras distintas tienen restricciones a V_0 distintas.

Por tanto, el número de palabras del código es como mucho el número total de aplicaciones sobre V_0 de restricción como la descrita, lo que equivale a contar las matrices de tamaño $\text{máx}\{n,m\} \times (\text{mín}\{n,m\} - d + 1)$ sobre $\mathbb{F}_q$. Este número es:

$$q^{\text{máx}\{n,m\}\,(\text{mín}\{n,m\}-d+1)}.$$

En conclusión, obtenemos la cota para el cardinal del código:

$$M \leq q^{\text{máx}\{n,m\}\,(\text{mín}\{n,m\}-d+1)}.$$

□

En la siguiente definición damos nombre a aquellos códigos para los que se alcanza la igualdad en (3.3).

Definición 3.5. Un *código de máxima distancia de rango* (MRD) de tipo $[n, M, d]_R$ sobre $\mathbb{F}_{q^m}$ es aquel cuyo cardinal M es igual a $q^{\text{mín}\{n(m-d+1),\, m(n-d+1)\}}$, es decir, su cardinal alcanza la cota dada en (3.3). Lo denotamos por $\text{MRD}(n, M)$.

Como observación, en caso de que el código MRD sobre $\mathbb{F}_{q^m}$ sea lineal de longitud $n \leq m$ y dimensión k, el Teorema 2.6 implica también que $d \leq n - k + 1$. Si además se da la igualdad, $d = n - k + 1$, se denota por $\text{MRD}[n, k, d]$ y tiene cardinal $M = q^{mk}$.

Pasamos ahora a tratar de acotar el cardinal máximo de los códigos en la métrica del rango, partiendo de la siguiente definición.

Definición 3.6. El *cardinal máximo* de un código de longitud n y distancia mínima de rango d sobre $\mathbb{F}_q^m$ se denota por $A^R_{q^m}(n, d)$. Se trata de una cota superior para el cardinal de cualquier código $[n, M, d]_R$ sobre $\mathbb{F}_q^m$, es decir, $M \leq A^R_{q^m}(n, d)$.

Cabe destacar que la definición anterior asume la existencia de un código $[n, M, d]_R$ que verifique $M = A^R_{q^m}(n, d)$. Relacionado con ello está el resultado de abajo, que establece la versión de las cotas de empaquetamiento de esferas de Hamming y de Gilbert–Varshamov en la métrica de rango.

Teorema 3.3. *Sea $A^R_{q^m}(n, d)$ el cardinal máximo de un código en bloque $[n, M, d]_R$ sobre $\mathbb{F}_{q^m}$, y sea $\tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor$. Entonces,*

$$\frac{q^{mn}}{|B_R^{(d-1)}(\mathbf{0})|} \leq A^R_{q^m}(n, d) \leq \frac{q^{mn}}{|B_R^{(\tau_0)}(\mathbf{0})|}. \tag{3.4}$$

(Ver el Apartado III, [3]).

Demostración. La deducción de las cotas de empaquetamiento de esferas y de Gilbert- Varshamov es independiente de la métrica empleada. De este modo, podemos adaptar directamente los argumentos clásicos utilizados en la métrica de Hamming al contexto de la métrica del rango. □

En (3.4), el lado izquierdo se correspondería con la cota de Gilbert–Varshamov en métrica de rango y el lado derecho, con la cota de empaquetamiento de esferas de Hamming. Nótese además que $|B_R^{(\tau_0)}(\mathbf{0})|$ y $|B_R^{(d-1)}(\mathbf{0})|$ son independientes de sus centros.

Daremos a continuación un nombre a aquellos códigos para los cuales se verifica la igualdad correspondiente a la cota de empaquetamiento de esferas en la métrica del rango.

Definición 3.7. Un código es *perfecto en métrica del rango* si cumple la igualdad en el lado derecho de (3.4). Para un código perfecto las bolas de radio $\tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor$ centradas en cada palabra del código son disjuntas y cubren todo el espacio.

Dicho de otro modo, un código perfecto es aquel que logra el empaquetamiento exacto de esferas. Sin embargo, veremos en la siguiente proposición una diferencia clave con los códigos perfectos en la métrica de Hamming.

Proposición 3.1. *No existen códigos perfectos en la métrica del rango (ver [7]).*

Demostración. Razonemos por reducción al absurdo. Supongamos que existe un código perfecto de tipo $[n, M, d]_R$ sobre $\mathbb{F}_{q^m}^n$, es decir, que satisface

$$M \times \mathcal{B}_{\tau_0} = q^{mn},$$

donde $\tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor$ y hemos denotado por $\mathcal{B}_{\tau_0}$ al cardinal de la bola de radio τ_0 en la métrica de rango ($\mid B_R^{\tau_0}(\mathbf{a}) \mid$). Sin pérdida de generalidad, podemos suponer que $n \leq m$. Usaremos la siguiente cota superior para el cardinal de las bolas (*Proposition 1*, [7]):

$$Mq^{(m+n+1)\tau_0 - \tau_0^2 + 1} \geq q^{mn}.$$

Por otro lado, la cota de Singleton establece que

$$M \leq q^{m(n-d+1)}, \text{ y como } \tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor, \text{ se tiene que } M \leq q^{m(n-2\tau_0)}.$$

Juntando ambas desigualdades obtenemos que

$$q^{(m+n+1)\tau_0 - \tau_0^2 + m(n-2\tau_0)+1} \geq q^{mn}.$$

Tomando logaritmos en base q en ambos lados y reordenando los términos, resulta:

$$(n-m)\tau_0 \geq \tau_0^2 - \tau_0 + 1.$$

Como partimos de que $n - m \leq 0$ y $\tau_0 > 0$, debemos tener que $\tau_0^2 - \tau_0 + 1 \leq 0$. Pero esto solo es posible si $\tau_0 = 1$, y en ese caso $n = m$. Analicemos este caso en profundidad.

Para $\tau_0 = 1$ ($n = m$), la fórmula (3.2) para el cardinal de la bola implica que se debe satisfacer

$$M \times \mathcal{B}_1 = q^{n^2}, \text{ donde } \mathcal{B}_1 = 1 + \binom{n}{1}_q (q^m - 1) = 1 + \frac{q^n - 1}{q-1}(q^m - 1) = \frac{q^{2n} - 2q^n + q}{q-1}.$$

Por tanto, teniendo en cuenta que $\tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$, tomamos $d = 3$ (ver la observación de abajo (*)) y tendríamos, atendiendo al Teorema 3.3 y a la Cota de Singleton:

$$q^{n(n-2)} \geq M \geq \frac{q^{2n} - 2q^n + q}{q-1},$$

lo que implica

$$1 - \frac{2}{q^n} + \frac{1}{q^{2n-1}} \geq q - 1.$$

Sin embargo, esta desigualdad no se satisface para $q \geq 2$, lo cual prueba que no pueden existir códigos perfectos en la métrica del rango.

(*) Como observación, si tomáramos $d = 4$, también válido si $\tau_0 = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$, sería aún más complicado satisfacer simultáneamente las cotas que para $d = 3$, dado que quedaría $q^{n(n-3)} \geq M$.

□

Vamos ahora a introducir dos tipos especiales de códigos en la métrica de rango, los *códigos q-cíclicos* y los *códigos de rango constante*. No obstante, debemos de aclarar un detalle de notación: para cualquier entero i, denotaremos las potencias de q con el fin de simplificar visualmente los resultados por $[i] := q^i$.

Definición 3.8. Sea $\mathcal{C}$ un código $[n, M, d]_R$ sobre $\mathbb{F}_{q^m}$ de longitud n, cardinal M y distancia mínima de rango d. Se denomina *código q-cíclico* si

$$(c_{n-j}^{[j]}\ c_{n-j+1}^{[j]}\ \dots\ c_0^{[j]}\ c_1^{[j]}\ \dots\ c_{n-j-1}^{[j]}) \in \mathcal{C},$$

para cualquier entero j y cualquier palabra del código $(c_0\ c_1\ \dots\ c_{n-1}) \in \mathcal{C}$.

Definición 3.9. Un *código de rango constante*, denotado por $\mathrm{CR}_{q^m}[n, M, d, r]$, es un código sobre $\mathbb{F}_{q^m}$ de longitud n, distancia mínima de rango d y cardinal M donde todas las palabras no nulas tienen el mismo rango r. Además, si el código es lineal será $r = d$.

3.2. Códigos de Gabidulin

Los códigos de Gabidulin (ver [2, 1, 11]) son una clase especial de códigos MRD lineales y a menudo se consideran análogos en métrica de rango de los códigos de Reed–Solomon (Definición 1.28). Como bien introdujimos al inicio del capítulo, estos códigos se basan en la evaluación de polinomios linealizados, de modo que haremos un breve inciso que muestre el procedimiento usando la notación introducida en la sección anterior.

Lema 3.4. *Sea $\mathcal{B} = \{\beta_0, \beta_1, \dots, \beta_{m-1}\}$ una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y sea $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$, un polinomio linealizado con coeficientes $\alpha_i \in \mathbb{F}_{q^m}$. Para cualquier $b \in \mathbb{F}_{q^m}$, denotemos su vector representación respecto a la base $\mathcal{B}$ (como en la Definición 3.1) por:*

$$ext_{\mathcal{B}}(b) = (B_0\ B_1\ \dots\ B_{m-1})^t \in \mathbb{F}_q^{m\times 1}.$$

Entonces

$$L(b) = \sum_{i=0}^{m-1} B_i L(\beta_i).$$

A continuación, damos una definición formal de los códigos de Gabidulin.

Definición 3.10. Un código de Gabidulin lineal $\mathrm{Gab}[n, k]$ sobre $\mathbb{F}_{q^m}$ de longitud $n \le m$ y dimensión $k \le n$ es el conjunto de todas las palabras que son evaluaciones de un q-polinomio $f(x) \in \mathbb{L}_{q^m}[x]$ de q-grado menor que k:

$$\mathrm{Gab}[n, k] := \left\{(f(g_0)\ f(g_1)\ \dots\ f(g_{n-1})) = f(\mathbf{g}) \mid f(x) \in \mathbb{L}_{q^m}[x],\ \text{con}\ \deg_q f(x) < k\right\},$$

donde los elementos fijos $g_0, g_1, \dots, g_{n-1} \in \mathbb{F}_{q^m}$ son linealmente independientes sobre $\mathbb{F}_q$ y por $\deg_q f(x)$ denotamos al *q-grado*, es decir, el mayor exponente i de q para el cual no se anula el coeficiente correspondiente en el polinomio linealizado $f(x)$.

No obstante, podemos dar una descripción alternativa de las palabras de los códigos de Gabidulin, basada en la definición de la *aplicación q-transformada* y su inversa. Para ello, introducimos la noción de *base normal* de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Observaremos que la normalidad no es estrictamente necesaria desde un punto de vista teórico, pero su uso permite reducir significativamente la complejidad computacional de la transformación. Además, enunciaremos un resultado que garantice la existencia de dicha base normal.

Definición 3.11. Una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, $\mathcal{B} = \{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$, es *una base normal* si se tiene $\beta_i = \beta^{[i]}$ para todo $i = 0, \cdots, m-1$ y cierto $\beta \in \mathbb{F}_{q^m}$. Además, la denotaremos por $\mathcal{B}_N = \{\beta^{[0]}, \beta^{[1]}, \cdots, \beta^{[m-1]}\}$ y llamaremos a los $\beta \in \mathbb{F}_{q^m}$ *elementos normales*.

El siguiente teorema es esencialmente equivalente al Teorema 2.11, en el que aseguramos la existencia de un elemento ζ en un q-módulo M de dimensión $m \geq 1$ sobre $\mathbb{F}_q$ tal que $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ es una base de M sobre $\mathbb{F}_q$.

Teorema 3.4. *En una extensión $\mathbb{F}_{q^m}$ sobre el cuerpo $\mathbb{F}_q$, existe una base normal de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$ para cada divisor s de m. Además, para el elemento normal de esta base se cumple $\beta = \beta^{[s]}$.*

El concepto de *base dual* $\mathcal{B}^\perp$ de la base $\mathcal{B}$ será necesario para establecer una correspondencia entre polinomios y sus q-transformados. Para describirla es preciso definir la siguiente aplicación.

Definición 3.12. La *aplicación de traza* de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ para un elemento $a \in \mathbb{F}_{q^m}$ viene dada por:

$$\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$$

$$a \mapsto \mathrm{Tr}(a) := \textstyle\sum_{i=0}^{m-1} a^{[i]}.$$

Se trata de una aplicación lineal sobre $\mathbb{F}_q$ bien definida, dado que para $a \in \mathbb{F}_{q^m}$, se tiene $\mathrm{Tr}(a) \in \mathbb{F}_q$.

Definición 3.13. Una base $\mathcal{B}^\perp = \{\beta_0^\perp, \beta_1^\perp, \ldots, \beta_{m-1}^\perp\}$ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se llama *base dual* de $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ si

$$\mathrm{Tr}\ (\beta_i\ \beta_j^\perp) = \begin{cases} 1, & \text{si } i = j, \\ \\ 0, & \text{en otro caso.} \end{cases} \tag{3.5}$$

Lema 3.5. *Para cualquier base $\mathcal{B}$ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, existe una única base dual $\mathcal{B}^\perp$. Además, la base dual de una base normal es también una base normal.*

Demostración. La prueba de este resultado se puede encontrar en la sección *2.3. Traces, Norms, and Bases*, [5].

□

Si una base es dual de sí misma, es decir, si $\mathcal{B} = \mathcal{B}^\perp$, se dice que es una *base autodual*; si además es normal, se denomina *base normal autodual* y $\mathcal{B}_N = \mathcal{B}_N^\perp$.

Explicamos ahora las operaciones matemáticas básicas sobre dos elementos $a, b \in \mathbb{F}_{q^m}$ utilizando una base normal $\mathcal{B}_N = \{\beta^{[0]}, \beta^{[1]}, \ldots, \beta^{[m-1]}\}$ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Empleamos la aplicación ext_β (Definición 3.1) para representar estos dos elementos como vectores en $\mathbb{F}_q$:

$$\begin{pmatrix} A_0 & A_1 & \cdots & A_{m-1} \end{pmatrix}^t := \mathrm{ext}_\beta(a) \in \mathbb{F}_q^{m\times 1},$$

$$\begin{pmatrix} B_0 & B_1 & \cdots & B_{m-1} \end{pmatrix}^t := \mathrm{ext}_\beta(b) \in \mathbb{F}_q^{m\times 1}.$$

Cabe destacar que, al tratarse de una base normal, hacer la q-ésima potencia de un elemento en $\mathbb{F}_{q^m}$ equivale a realizar un desplazamiento cíclico del vector correspondiente $\mathrm{ext}_\beta(a)$ sobre $\mathbb{F}_q$:

$$\mathrm{ext}_\beta\left(a^{[j]}\right) = (A_{m-j}\, A_{m-j+1}\, \ldots\, A_0\, A_1\, \ldots\, A_{m-j-1})^t := \mathrm{ext}_\beta(a)^{\downarrow j} \in \mathbb{F}_q^{m\times 1}, \tag{2.3}$$

donde la flecha hacia abajo indica un desplazamiento cíclico del vector en j posiciones hacia abajo. La eficiencia de los cálculos con bases normales se debe a esta propiedad y al uso de una llamada tabla de multiplicación, que describimos a continuación.

Definición 3.14. Sea $\mathcal{B}_N = \{\beta^{[0]}, \beta^{[1]}, \ldots, \beta^{[m-1]}\}$ una base normal de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. La *tabla de multiplicación* de $\mathcal{B}_N$ es la matriz $\mathbf{T}_m \in \mathbb{F}_q^{m\times m}$ tal que:

$$\beta^{[0]} \cdot \begin{pmatrix}\beta^{[0]} & \beta^{[1]} & \ldots & \beta^{[m-1]}\end{pmatrix}^t = \mathbf{T}_m \cdot \begin{pmatrix}\beta^{[0]} & \beta^{[1]} & \ldots & \beta^{[m-1]}\end{pmatrix}^t.$$

El número de elementos no nulos en $\mathbf{T}_m$ se denomina la *complejidad de* $\mathbf{T}_m$ de la base $\mathcal{B}_N$ y se denota por $\mathrm{comp}(\mathbf{T}_m)$.

Ahora procederemos a explicar de qué manera ayuda esta matriz a aumentar la eficiencia a la hora de realizar operaciones y por qué es apropiada la palabra *complejidad* en la definición anterior.

- La suma $a+b$ en $\mathbb{F}_{q^m}$ puede realizarse componente a componente como $\mathrm{ext}_\beta(a)+\mathrm{ext}_\beta(b) \in \mathbb{F}_q^{m\times 1}$, y es por tanto sencilla de implementar.
- El producto de $a \cdot b \in \mathbb{F}_{q^m}$ puede calcularse sobre el cuerpo base $\mathbb{F}_q$, mediante la tabla de multiplicación, de la siguiente manera:

$$\mathrm{ext}_\beta(a \cdot b) = \sum_{i=0}^{m-1} B_i \left(\mathbf{T}_m^t \cdot \mathrm{ext}_\beta(a)^{\uparrow i}\right)^{\downarrow i} \in \mathbb{F}_q^{m\times 1}, \tag{3.6}$$

  donde las flechas hacia arriba (o bien hacia abajo) indican desplazamientos cíclicos del vector en i posiciones hacia la primera (o bien hacia la última).

  Si uno de los elementos es un elemento de la base, es decir, $b = \beta^{[j]}$, entonces el vector $\mathrm{ext}_\beta(b)$ es nulo excepto en la fila j-ésima, y (3.6) se convierte en:

$$\mathrm{ext}_\beta(a \cdot \beta^{[j]}) = \left(\mathbf{T}_m^t \cdot \mathrm{ext}_\beta(a)^{\uparrow j}\right)^{\downarrow j} \in \mathbb{F}_q^{m\times 1}. \tag{3.7}$$

  De (3.6) y (3.7) se deduce que el número de operaciones en $\mathbb{F}_q$ necesarias para calcular $a \cdot b$ depende directamente del número de elementos no nulos de $\mathbf{T}_m$, es decir, de su complejidad, $\mathrm{comp}(\mathbf{T}_m)$. Por lo tanto, es deseable que $\mathbf{T}_m$ sea dispersa, es decir, que sea grande el número de elementos nulos de la matriz.

Tal como adelantamos, el concepto de base dual está estrechamente relacionado con la aplicación q-transformada de un polinomio linealizado, que presentaremos a continuación.

Definición 3.15. Sea $L(x) = \sum_{i=0}^{s-1} \alpha_i x^{q^i} \in \mathbb{L}_{q^m}[x]$ un polinomio linealizado (o simplemente un vector $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s$), donde $s \mid m$, y sea $\mathcal{B}_N = \{\beta^{[0]}, \beta^{[1]}, \ldots, \beta^{[s-1]}\}$ una base normal de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$.

La *q-transformada de $L(x)$ respecto a $\mathcal{B}_N$* es la aplicación correspondiente al polinomio linealizado $\widehat{L}(x) = \sum_{j=0}^{s-1} \widehat{\alpha}_j x^{q^j}$ (o simplemente al vector $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \widehat{\alpha}_1, \ldots, \widehat{\alpha}_{s-1}) \in \mathbb{F}_q^s$) definido por

$$\widehat{\alpha}_j = L(\beta^{[j]}) = \sum_{i=0}^{s-1} \alpha_i \beta^{[i+j]}, \quad \forall j \in [0, s-1]. \tag{3.8}$$

Denotamos el vector representación de $\alpha_j \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ usando una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ por $\mathrm{ext}_\beta(\alpha_j)$. De manera análoga, el vector representación de $\widehat{\alpha}_j$, denotado por $\mathrm{ext}_\beta(\widehat{\alpha}_j)$, puede expresarse como

$$\mathrm{ext}_\beta(\widehat{\alpha}_j) = \mathrm{ext}_\beta\left(L(\beta^{[j]})\right) = \sum_{i=0}^{d_L} \mathrm{ext}_\beta(\alpha_i)\beta^{[i+j]}, \tag{3.9}$$

donde $d_L = \deg_q L(x) < s$, y $\widehat{\alpha}_j$ puede obtenerse mediante $\mathrm{ext}_\beta^{-1}\left(\mathrm{ext}_\beta(\widehat{\alpha}_j)\right)$.

Para poder invertir la correspondencia entre el q-polinomio y su q-transformado, necesitamos una transformación inversa a la descrita anteriormente. El siguiente teorema muestra que es posible realizar esta operación y recuperar el polinomio original.

Teorema 3.5. *Sea*

$$\widehat{L}(x) = \sum_{j=0}^{s-1} \widehat{\alpha}_j x^{q^j} \in \mathbb{L}_{q^m}[x]$$

el polinomio q-transformado de

$$L(x) = \sum_{i=0}^{s-1} \alpha_i x^{q^i} \in \mathbb{L}_{q^m}[x],$$

donde s divide a m, y sea $\mathcal{B}_N = \{\beta^{[0]}, \beta^{[1]}, \ldots, \beta^{[s-1]}\}$ una base normal en $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Sea $\mathcal{B}_N^{\perp} = \{\beta^{\perp[0]}, \beta^{\perp[1]}, \ldots, \beta^{\perp[s-1]}\}$ una base normal dual de $\mathcal{B}_N$. Entonces,

$$\alpha_i = \widehat{L}\left(\beta^{\perp[i]}\right) = \sum_{j=0}^{m-1} \widehat{\alpha}_j \beta^{\perp[i+j]}, \quad \forall i \in [0, s-1]. \tag{3.10}$$

El vector $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s$ es el vector de coeficientes del llamado polinomio q-transformado inverso de $\widehat{L}(x)$ respecto de la base normal dual $\mathcal{B}_N^{\perp}$.

Demostración. La condición $s \mid m$ garantiza que existe una base normal dual $\mathcal{B}_N^{\perp}$ (ver Lema 3.4). Sean las matrices:

$$\mathbf{B} = \begin{pmatrix} \beta^{[0]} & \beta^{[1]} & \ldots & \beta^{[s-1]} \\ \beta^{[1]} & \beta^{[2]} & \ldots & \beta^{[0]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{[s-1]} & \beta^{[0]} & \ldots & \beta^{[s-2]} \end{pmatrix}, \quad \mathbf{B}^{\perp} = \begin{pmatrix} \beta^{\perp[0]} & \beta^{\perp[1]} & \ldots & \beta^{\perp[s-1]} \\ \beta^{\perp[1]} & \beta^{\perp[2]} & \ldots & \beta^{\perp[0]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{\perp[s-1]} & \beta^{\perp[0]} & \ldots & \beta^{\perp[s-2]} \end{pmatrix}. \tag{3.11}$$

Por definición, $(\widehat{\alpha}_0, \widehat{\alpha}_1, \ldots, \widehat{\alpha}_{s-1}) = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \cdot \mathbf{B}$ (ver (3.8)). Calculando

$$\boldsymbol{\alpha}' = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_{s-1}) \cdot \mathbf{B}^{\perp}, \text{ esto es, } \alpha'_i = \widehat{\alpha}(\beta^{\perp[i]}) \text{ para } i \in [0, s-1],$$

se tiene:

$$\boldsymbol{\alpha}' = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \cdot \mathbf{B} \cdot \mathbf{B}^{\perp}.$$

Además, debido a la definición de la base dual (ver 3.5) y al hecho de que

$$\mathrm{Tr}(\beta^{[i]}\beta^{\perp[i]}) = \mathrm{Tr}(\beta\beta^{\perp})^{[i]} = \mathrm{Tr}(\beta\beta^{\perp}),$$

obtenemos:

$$\mathbf{B} \cdot \mathbf{B}^{\perp} = \begin{pmatrix} \mathrm{Tr}(\beta\beta^{\perp}) & \mathrm{Tr}(\beta\beta^{\perp[1]}) & \cdots & \mathrm{Tr}(\beta\beta^{\perp[s-1]}) \\ \mathrm{Tr}(\beta^{[1]}\beta^{\perp}) & \mathrm{Tr}(\beta^{[1]}\beta^{\perp[1]}) & \cdots & \mathrm{Tr}(\beta^{[1]}\beta^{\perp[s-1]}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\beta^{[s-1]}\beta^{\perp}) & \mathrm{Tr}(\beta^{[s-1]}\beta^{\perp[1]}) & \cdots & \mathrm{Tr}(\beta^{[s-1]}\beta^{\perp[s-1]}) \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Por lo tanto, se concluye que $\boldsymbol{\alpha}' = \boldsymbol{\alpha}$, lo que prueba el resultado. □

Habiendo introducido las nociones necesarias, estamos en condiciones de presentar una descripción de las palabras de un código de Gabidulin, $Gab[n,k]$, alternativa a la que se planteó al inicio del capítulo. En efecto, dichas palabras pueden definirse como la q-transformada inversa (ver el Teorema 3.5) de los polinomios de evaluación $f(x)$ con $\deg_q(f(x)) < k$. Para ello, necesitamos una base normal $\mathcal{B}_N^{\perp} = \{\beta_0^{\perp}, \beta_1^{\perp}, \ldots, \beta_{n-1}^{\perp}\}$ de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Según el Lema 3.4, tal base existe en $\mathbb{F}_{q^m}$ si n divide a m y, en particular, para $n = m$. Los coeficientes de las palabras del código pueden entonces darse mediante la q-transformada inversa de $f(x)$ como en el Teorema 3.5:

$$c_i = f(\beta^{\perp[i]}) = \sum_{j=0}^{n-1} f_j(\beta^{\perp[j+i]}), \quad \forall i \in [0, n-1]. \tag{3.12}$$

Como observación, es claro que una definición más general de la q-transformada (y su inversa) usando una base arbitraria y su base dual es equivalente a la evaluación de un polinomio linealizado.

Tal y como dijimos al comenzar la sección, los códigos de Gabidulin son códigos MRD. Lo comprobaremos tras incidir en determinados conceptos indispensables. En primer lugar, describiremos la matriz de q-Vandermonde (ver [9]), que desempeña un papel importante a la hora de evaluar q-polinomios.

Definición 3.16. Para un vector $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^m}^n$, *la matriz de q-Vandermonde* de tamaño $s \times n$ se obtiene mediante la siguiente aplicación:

$$\begin{gathered} \mathrm{qvan}_s : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^{s\times n} \\ \boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \mapsto \mathrm{qvan}_s(\boldsymbol{\alpha}) := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^{[1]} & \alpha_1^{[1]} & \cdots & \alpha_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{[s-1]} & \alpha_1^{[s-1]} & \cdots & \alpha_{n-1}^{[s-1]} \end{pmatrix}. \end{gathered} \tag{3.13}$$

Recordemos para cualquier polinomio linealizado $L(x)$ de q-grado $d_L < m$ induce una aplicación $\mathbb{F}_q$-lineal $L : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, y el núcleo de esta aplicación se corresponde con el espacio de raíces de $L(x)$ (como vimos en (2.9)), es decir,

$$\ker(L) = \{b \in \mathbb{F}_{q^m} : L(b) = 0\}.$$

Este puede interpretarse como el núcleo por columnas (por la derecha) de una matriz $\mathbf{A}$.

Definición 3.17. La *matriz de evaluación asociada* $\mathbf{A}$ es la matriz que se obtiene evaluando $L(x)$ en una base $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y representando el resultado sobre $\mathbb{F}_q$. Expresado de otro modo,

$$\mathbf{A} := \mathrm{ext}_{\mathcal{B}}\left((L(\beta_0)\ L(\beta_1)\ \ldots\ L(\beta_{m-1}))\right) \in \mathbb{F}_q^{m\times m}.$$

El siguiente lema muestra la conexión entre el espacio de raíces de $L(x)$ y el rango de la matriz asociada.

Lema 3.6. *Sea $L(x) \in \mathbb{L}_{q^m}[x]$ un polinomio linealizado no nulo de q-grado $d_L < m$. Entonces, el rango de la matriz de evaluación asociada satisface:*

$$rk(\mathbf{A}) \geq m - d_L.$$

Demostración. Dado que $\deg_q L(x) = d_L$, el polinomio tiene como máximo q^{d_L} raíces en $\mathbb{F}_{q^m}$ y, por tanto, la dimensión del espacio de raíces es a lo sumo d_L. Este espacio de raíces es equivalente al núcleo por columnas de $\mathbf{A}$, por lo que:

$$\dim(\ker(\mathbf{A})) \leq d_L.$$

Aplicando el hecho de que $\dim(\ker(\mathbf{A})) + \mathrm{rk}(\mathbf{A}) = m$ obtenemos que, efectivamente,

$$\mathrm{rk}(\mathbf{A}) \geq m - d_L.$$

□

Lo siguiente está relacionado con la idea de que el núcleo de la aplicación L es el espacio de raíces de $L(x)$, visto como un subespacio vectorial sobre $\mathbb{F}_q$. Dado un segundo polinomio linealizado $L_2(x)$, la composición $L_2(L(x)) \mod (x^{[m]} - x)$ es, a su vez, una aplicación lineal $L_2 \circ L$, cuyo núcleo contiene el núcleo de L. Lo establecemos formalmente en el lema siguiente.

Lema 3.7. *Sean $a(x)$ y $b(x)$ dos polinomios linealizados en $\mathbb{L}_{q^m}[x]$ con $\deg_q a(x), \deg_q b(x) < m$. Sea $c(x) = b(a(x))$ y sea $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ una base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Definamos*

$$\mathbf{A} = ext_\beta\left((a(\beta_0)\, a(\beta_1)\, \ldots\, a(\beta_{m-1}))\right), \quad \mathbf{C} = ext_\beta\left((c(\beta_0)\, c(\beta_1)\, \ldots\, c(\beta_{m-1}))\right).$$

Entonces, para los espacios de filas se cumple:

$$\mathcal{R}_q(\mathbf{C}) \subseteq \mathcal{R}_q(\mathbf{A}).$$

Demostración. Consideremos los polinomios linealizados como aplicaciones lineales sobre $\mathbb{F}_{q^m}$. Entonces, el núcleo de la aplicación a es equivalente al conjunto de raíces de $a(x)$ en $\mathbb{F}_{q^m}$, considerado como un espacio vectorial sobre $\mathbb{F}_q$. Dado que las raíces de $a(x)$ también son raíces de $c(x) = b(a(x))$, se verifica $\ker(a) \subseteq \ker(c)$. Por lo tanto, también se verifica para las matrices de evaluación asociadas que $\ker(\mathbf{A}) \subseteq \ker(\mathbf{C})$, de modo que los espacios fila cumplen que $\mathcal{R}_q(\mathbf{C}) \subseteq \mathcal{R}_q(\mathbf{A})$. □

Teorema 3.6. *La distancia mínima de rango de un código Gabidulin, $Gab[n,k]$, sobre $\mathbb{F}_{q^m}$ con $n \leq m$ es $d = n - k + 1$.*

Demostración. Cada polinomio de evaluación $f(x)$ tiene q-grado menor que k y, por tanto, la dimensión del espacio de sus raíces sobre $\mathbb{F}_q^m$ es como máximo $k - 1$.

Sea $\mathbf{C} = \mathrm{ext}_\beta(\mathbf{c}) \in \mathbb{F}_q^{m \times n}$ la representación matricial de $\mathbf{c} \in Gab[n,k]$. Por el Lema 3.6, teniendo en cuenta que la dimensión del núcleo de $\mathbf{C}$ es igual a la dimensión del espacio de raíces del correspondiente polinomio de evaluación $f(x)$, se tiene:

$$\mathrm{rk}(\mathbf{C}) \geq n - (k-1) \Rightarrow \dim\ker(\mathbf{c}) \leq k - 1, \quad \forall \mathbf{c} \in Gab[n,k].$$

Existe una palabra del código $\mathbf{c} \in Gab[n,k]$ de rango d. Para esta palabra,

$$\dim\ker(\mathbf{c}) = n - \mathrm{rk}(\mathbf{c}) = n - d.$$

Así, se deduce:

$$n - d \leq k - 1 \quad \Longleftrightarrow \quad d \geq n - k + 1.$$

Por otro lado, la cota de tipo Singleton (ver ecuación (3.3)) implica que $d \leq n - k + 1$. Así, concluimos que

$$d = n - k + 1,$$

y los códigos de Gabidulin son códigos MRD, como queríamos demostrar. □

Basándonos en la Definición 3.10 de código lineal de Gabidulin, podemos dar la matriz generadora de un código de Gabidulin usando los elementos $g_0, g_1, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ linealmente independientes sobre $\mathbb{F}_q$. Se trata de la siguiente matriz

$$\mathbf{G} = \mathrm{qvan}_k((g_0\ g_1\ \ldots\ g_{n-1})) = \begin{pmatrix} g_0^{[0]} & g_1^{[0]} & \cdots & g_{n-1}^{[0]} \\ g_0^{[1]} & g_1^{[1]} & \cdots & g_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{[k-1]} & g_1^{[k-1]} & \cdots & g_{n-1}^{[k-1]} \end{pmatrix}, \tag{3.14}$$

ya que evaluar un polinomio linealizado de q-grado menor que k equivale a multiplicar sus coeficientes por la matriz de tipo q-Vandermonde (3.13).

Ahora, construiremos una *matriz de control* para un código de Gabidulin, aprovechando la estructura algebraica de los polinomios linealizados que definen sus palabras de código.

Lema 3.8. *Sea* $\mathbf{G}$ *una matriz generadora de un código* $Gab[n,k]$ *como en* (3.14)*, donde* $g_0, g_1, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ *son linealmente independientes sobre* $\mathbb{F}_q$*. Sean* $h_0, h_1, \ldots, h_{n-1}$ *una solución no trivial del siguiente sistema de* $n-1$ *ecuaciones lineales:*

$$\sum_{i=0}^{n-1} g_i^{[j]} h_i = 0, \quad \forall j \in \{-n+k+1, \ldots, k-1\}. \tag{3.15}$$

Entonces, la matriz de tamaño $(n-k)\times n$

$$\mathbf{H} = qvan_{n-k}((h_0\ h_1\ \ldots\ h_{n-1})) = \begin{pmatrix} h_0^{[0]} & h_1^{[0]} & \ldots & h_{n-1}^{[0]} \\ h_0^{[1]} & h_1^{[1]} & \ldots & h_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_0^{[n-k-1]} & h_1^{[n-k-1]} & \ldots & h_{n-1}^{[n-k-1]} \end{pmatrix},$$

es una matriz de control del código $Gab[n,k]$*.*

Demostración. Debemos probar que $\mathbf{H}$ verifica $\mathbf{G}\cdot\mathbf{H}^t = \mathbf{0}$. Esta ecuación matricial es equivalente al siguiente sistema de $n-1$ ecuaciones lineales:

$$\sum_{i=0}^{n-1} g_i^{[l]} h_i^{[j]} = 0, \quad \forall l \in \{0,\ldots,k-1\}, \quad j \in \{0,\ldots,n-k-1\},$$

$$\iff \sum_{i=0}^{n-1} g_i^{[j]} h_i = 0, \quad \forall j \in \{-n+k+1,\ldots,k-1\}.$$

Por lo tanto, si $h_0, h_1, \ldots, h_{n-1}$ son linealmente independientes sobre $\mathbb{F}_q$, $\mathbf{H}$ es la matriz buscada (una matriz de control del código y una matriz generadora del código dual $\mathrm{Gab}[n, n-k]$). Veamos que efectivamente son linealmente independientes.

Para demostrar esto, denotemos

$$\tilde{\mathbf{g}} = (g_0^{[-n+k+1]}\ g_1^{[-n+k+1]}\ \ldots\ g_{n-1}^{[-n+k+1]}).$$

Entonces, el sistema de ecuaciones del que partimos, (3.15), es equivalente a:

$$\mathrm{qvan}_{n-1}(\tilde{\mathbf{g}})\cdot(h_0\ h_1\ \ldots\ h_{n-1})^t = \mathbf{0}. \tag{3.16}$$

La matriz $\mathrm{qvan}_{n-1}(\tilde{\mathbf{g}})$ es una matriz de control de un código $\mathrm{Gab}[n,1]$, ya que $g_0^{[-n+k+1]}, g_1^{[-n+k+1]}, \ldots, g_{n-1}^{[-n+k+1]}$ son linealmente independientes sobre $\mathbb{F}_q$ (ver (3.14)). Por tanto, el vector $(h_0\ h_1\ \ldots\ h_{n-1})$ es una palabra del código $\mathrm{Gab}[n,1]$.

Además, este código, $\mathrm{Gab}[n,1]$, tiene distancia mínima $d = n-1+1 = n$, por lo que $\mathrm{rk}((h_0\ h_1\ \ldots\ h_{n-1})) = n$. Por tanto, $h_0, h_1, \ldots, h_{n-1}$ son linealmente independientes sobre $\mathbb{F}_q$ y $\mathbf{H}$ es una matriz generadora del código dual $\mathrm{Gab}[n, n-k]$. Luego $\mathbf{H}$ es una matriz de control del código $\mathrm{Gab}[n,k]$. □

A raíz de la demostración anterior, resulta natural hacer referencia al siguiente resultado, sobre el dual de un código de Gabidulin.

Teorema 3.7. *Sea $\mathcal{C}$ un código de Gabidulin* $\mathrm{Gab}[n,k]$ *definido sobre $\mathbb{F}_{q^m}$ con $n \leq m$. Entonces el código dual $\mathcal{C}^\perp$ es un código* $\mathrm{Gab}[n, n-k]$. *(Ver [2], Teorema 3)*

Demostración. Es consecuencia inmediata del lema anterior: la matriz generadora del dual de un código $\mathrm{Gab}[n,k]$ es la matriz de control de este, H, de tamaño $(n-k)\times n$. □

El siguiente lema profundiza en los códigos q-cíclicos, ahora introduciéndolos en el contexto de los códigos de Gabidulin.

Lema 3.9. *Sea $\mathbf{g} = (g_0, g_1, \ldots, g_{n-1}) = (\beta^{[0]}, \beta^{[1]}, \ldots, \beta^{[n-1]})$ una base normal ordenada de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y sea $Gab[n,k]$ un código de Gabidulin sobre $\mathbb{F}_{q^m}$.*

Entonces, $Gab[n,k]$ es q-cíclico.

Demostración. Recordamos la Definición 3.8 de código q-cíclico. Debemos demostrar que para cualquier entero j y cualquier palabra de código $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathrm{Gab}[n,k]$, la palabra

$$\tilde{\mathbf{c}} = (\tilde{c}_0\, \tilde{c}_1\, \ldots\, \tilde{c}_{n-1}) := (c_{n-j}^{[j]}\, c_{n-j+1}^{[j]}\, \ldots\, c_{n-1}^{[j]}\, c_0^{[j]}\, c_1^{[j]}\, \ldots\, c_{n-j-1}^{[j]})$$

es también una palabra del código $\mathrm{Gab}[n,k]$.

Los elementos de $\tilde{\mathbf{c}}$, como en (3.12), se pueden expresar de la siguiente manera:

$$\tilde{c}_i = c_{i-j}^{[j]} = \left(f(\beta^{\perp[i-j]})\right)^{[j]} = x^{[j]} \circ f(x)\Big|_{x=\beta^{[i-j]}} = x^{[j]} \circ f(x) \circ x^{[-j]}\Big|_{x=\beta^{\perp[i]}} \quad \forall i \in [0, n-1].$$

Por lo tanto, para cada q-polinomio de q-grado $< k$, $f(x) = \sum_{i=0}^{k-1} f_i x^{[i]}$, obtenemos:

$$\tilde{f}(x) := x^{[j]} \circ f(x \circ x^{[-j]}) = f_0^{[j]} x^{[0]} + f_1^{[j]} x^{[1]} + \cdots + f_{k-1}^{[j]} x^{[k-1]},$$

que verifica $\deg_q \tilde{f}(x) = \deg_q f(x) < k$. Así, tenemos que

$$\tilde{\mathbf{c}} = (\tilde{c}_0\, \tilde{c}_1\, \ldots\, \tilde{c}_{n-1}) = \tilde{f}(g) = \left(\tilde{f}(\beta^{[0]})\, \tilde{f}(\beta^{[1]})\, \ldots\, \tilde{f}(\beta^{[n-1]})\right)$$

es una palabra de código de $\mathrm{Gab}[n,k]$. □

El siguiente corolario deriva del Teorema 3.4, en el que probamos la existencia de una base normal de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$ en una extensión $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ si s divide a m.

Corolario 3.2. *Un código de Gabidulin q-cíclico $Gab[n,k]$ de longitud $n \leq m$ y dimensión $k \leq n$ sobre $\mathbb{F}_{q^m}$ existe para cualquier n que divida a m.*

Así, al recordar la ecuación (3.12), vemos que definir los códigos de Gabidulin mediante la q-transformada inversa genera códigos de Gabidulin q-cíclicos.

Lema 3.10. *Sea $Gab[n,k]$ un código de Gabidulin q-cíclico sobre $\mathbb{F}_{q^m}$, donde $\mathbf{g} = (\beta^{\perp[0]}\, \beta^{\perp[1]}\, \ldots\, \beta^{\perp[n-1]})$ es una base normal ordenada de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, con $n \mid m$, y $(\beta^{[0]}\, \beta^{[1]}\, \ldots\, \beta^{[n-1]})$ es una base normal dual de $\mathbf{g}$.*

Entonces, para

$$\mathbf{h} := (\beta^{[k]}\, \beta^{[k+1]}\, \ldots\, \beta^{[k+n-1]}),$$

la matriz $(n-k) \times n$

$$\mathbf{H} = \mathrm{qvan}_{n-k}(\mathbf{h}) = \begin{pmatrix} \beta^{[k]} & \beta^{[k+1]} & \ldots & \beta^{[k+n-1]} \\ \beta^{[k+1]} & \beta^{[k+2]} & \ldots & \beta^{[k]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{[n-1]} & \beta^{[0]} & \ldots & \beta^{[n-2]} \end{pmatrix},$$

es una matriz de control del código $Gab[n,k]$.

Demostración. En primer lugar, recordamos la demostración del Teorema 3.5, dado que nos basaremos en ella para esta prueba. En ella vimos que las palabras del código pueden darse mediante la q-transformada inversa de $f(x)$.

Sean $\mathbf{B}$ y $\mathbf{B}^{\perp}$ las matrices definidas como en (3.11), con $s = n$. Consideramos $\mathbf{H}$ la submatriz formada por las últimas $n-k$ filas de $\mathbf{B}$, y $\mathbf{G}^t$ la submatriz $n \times k$ de $\mathbf{B}^{\perp}$, formada por las primeras k columnas de $\mathbf{B}^{\perp}$.

Entonces, $\mathbf{G}$ es exactamente la matriz generadora de (3.14) y se tiene

$$\mathbf{H} \cdot \mathbf{G}^t = \begin{pmatrix} \beta^{[k]} & \beta^{[k+1]} & \ldots & \beta^{[k+n-1]} \\ \beta^{[k+1]} & \beta^{[k+2]} & \ldots & \beta^{[k]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{[n-1]} & \beta^{[0]} & \ldots & \beta^{[n-2]} \end{pmatrix} \cdot \begin{pmatrix} \beta^{\perp[0]} & \beta^{\perp[1]} & \ldots & \beta^{\perp[k-1]} \\ \beta^{\perp[1]} & \beta^{\perp[2]} & \ldots & \beta^{\perp[k]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{\perp[n-1]} & \beta^{\perp[0]} & \ldots & \beta^{\perp[k-2]} \end{pmatrix} = \mathbf{0},$$

como se probó en la demostración del Teorema 3.5.

Dado que $\mathbf{h} = (\beta^{[k]}\, \beta^{[k+1]}\, \ldots\, \beta^{[k+n-1]})$ consiste en n elementos linealmente independientes, $\mathbf{H}$ es una matriz de control del código $\mathrm{Gab}[n,k]$. □

Capítulo 4

Algoritmo de Loidreau

En este capítulo, estudiaremos el algoritmo de Loidreau (ver [6]). Se trata de una modificación del algoritmo de Welch-Berlekamp (ver [14]), originalmente diseñado para la descodificación de códigos de Reed-Solomon en métrica de Hamming. En concreto, el algoritmo de Loidreau consiste en una adaptación del algoritmo clásico al contexto de los códigos de Gabidulin y la métrica del rango.

En primer lugar, presentaremos el problema de descodificación de los códigos de Gabidulin. A continuación, estableceremos su conexión con el problema de *reconstrucción de polinomios linealizados*, que se basa en una tarea de interpolación bajo ciertas restricciones, y describiremos la estrategia general para resolverlo. Finalmente, expondremos dos algoritmos de descodificación de códigos de Gabidulin, o más bien, dos algoritmos para la obtención de q-polinomios que satisfagan las condiciones impuestas por el problema de reconstrucción.

4.1. Descodificación en la métrica del rango

En esta sección, veremos que el problema de descodificación de códigos de Gabidulin está relacionado con un problema de reconstrucción de q-polinomios. Formularemos ambos individualmente y, a continuación, daremos un resultado que los relaciona.

Antes de comenzar, haremos una breve aclaración de notación, que será empleada a lo largo del capítulo. Tenemos en cuenta que un código de Gabidulin de dimensión k (o bien, su matriz generadora, como en (3.13)) puede venir representado por un conjunto de n elementos de $\mathbb{F}_{q^m}$, $\mathbf{g} = (g_1, \ldots, g_n)$, linealmente independientes sobre el cuerpo $\mathbb{F}_q$. Así, en este capítulo lo denotaremos por $\mathrm{Gab}_k(\mathbf{g})$.

De este modo, en el contexto de la métrica del rango, el problema de descodificación de un código se puede formular de la manera que mostramos a continuación.

Definición 4.1. Recibido un vector $\mathbf{y}$ sobre $\mathbb{F}_{q^m}$ y considerados un código $\mathcal{C}$ sobre $\mathbb{F}_{q^m}$ y un entero positivo t, la *descodificación*$(\mathbf{y}, \mathcal{C}, t)$, si existe, consiste en encontrar una palabra $\mathbf{c} \in \mathcal{C}$ y un vector de error $\mathbf{e}$ tales que

$$\mathrm{Rk}(\mathbf{e}) \leq t \quad \text{verificando} \quad \mathbf{y} = \mathbf{c} + \mathbf{e}.$$

Aquí, siempre que t sea menor o igual a la capacidad de corrección de errores del código $\mathcal{C}$, la solución es única (si existe).

Recordamos que los códigos de Gabidulin se basan en la evaluación de polinomios linealizados, por lo que resulta natural vincular el problema de descodificación a un problema de *reconstrucción* de q-polinomios. Veamos en de qué manera se formula este problema.

Definición 4.2. La *reconstrucción*($\mathbf{y} = (y_1, \ldots, y_n),\ \mathbf{g} = (g_1, \ldots, g_n),\ k,\ t$) de un q-polinomio consiste en en encontrar un par (V, f) donde V es un q-polinomio no nulo de q-grado $\leq t$ y f es un q-polinomio de q-grado $< k$, tales que

$$V(y_i) = V(f(g_i)), \quad \text{para todo } i = 1, \ldots, n.$$

Este problema se puede relacionar con el problema de descodificación de los códigos de Gabidulin mediante el siguiente teorema.

Teorema 4.1. *Dada cualquier solución al problema de reconstrucción*($\mathbf{y}, \mathbf{g}, k, t$)*, donde los g_i son linealmente independientes sobre $\mathbb{F}_q$, se obtiene una solución al problema descodificación*($\mathbf{y}$, $Gab_k(\mathbf{g}), t$) *en tiempo polinomial.*

Demostración. Sea $\mathcal{L}$ el conjunto de soluciones del problema de reconstrucción($\mathbf{y}, \mathbf{g}, k, t$), tomamos $(V_1, f_1) \in \mathcal{L}$. Entonces, para todo $i = 1, \ldots, n$, se cumple que $V_1(y_i) = V_1(f_1(g_i))$. Por linealidad del q-polinomio V_1, se deduce que

$$V_1(y_i - f_1(g_i)) = 0, \quad \text{para todo } i = 1, \ldots, n.$$

Esto equivale a que para todo i, el elemento del cuerpo $\mathbb{F}_{q^m}$

$$e_i := y_i - f_1(g_i)$$

pertenece al núcleo de V_1, es decir, a un espacio vectorial sobre $\mathbb{F}_q$ de dimensión a lo sumo $\deg_q(V_1) \leq t$. Por tanto, el vector de error $\mathbf{e} = (e_1, \ldots, e_n)$ tiene rango a lo sumo t, y $\mathbf{c} := (f_1(g_1), \ldots, f_1(g_n))$ es una palabra del código $\mathrm{Gab}_k(\mathbf{g})$, es decir, una solucion del problema de descodificación($\mathbf{y}, \mathrm{Gab}_k(\mathbf{g}), t$).

Además, todas estas transformaciones pueden realizarse mediante una cantidad de operaciones que crece como una función polinómica de los parámetros del código, es decir, en tiempo polinomial. □

Por lo tanto, diseñar algoritmos para la reconstrucción de polinomios q-lineales permite resolver el problema de decodificación en la métrica de rango.

4.2. Resolución del problema de reconstrucción

En esta sección, describiremos con detalle el problema de reconstrucción de q-polinomios y expondremos el fundamento teórico que respalda la implementación algorítmica de su resolución. Partimos de los siguientes datos:

- Un vector $\mathbf{y} = (y_1, \ldots, y_n)$ de elementos tomados en el cuerpo $\mathbb{F}_{q^m}$,
- un vector $\mathbf{g} = (g_1, \ldots, g_n)$ de elementos tomados en $\mathbb{F}_{q^m}$, linealmente independientes sobre $\mathbb{F}_q$,
- enteros k y t.

Para resolver el problema de reconstrucción($\mathbf{y}, \mathbf{g}, k, t$), necesitamos encontrar q-polinomios V con $\deg_q(V) \leq t$, y f con $\deg_q(f) < k$, tales que:

$$V(y_i) = V(f(g_i)), \quad \text{para todo } i = 1, \ldots, n. \tag{4.1}$$

Se trata de un sistema (en general, no lineal) de n ecuaciones con $t+1+k$ incógnitas. Como no disponemos de una estrategia directa para resolverlo, cambiaremos el enfoque del problema: encontrar un par de q-polinomios (V, N), tales que:

$$\begin{cases} V(y_i) = N(g_i), \quad \forall i = 1, \ldots, n, \\ \deg_q(V) \leq t, \\ \deg_q(N) \leq k + t - 1. \end{cases} \tag{4.2}$$

Este sistema es lineal, y sus incógnitas son los $k + 2t + 1$ coeficientes de N y V. Sin embargo, hemos de comprobar que efectivamente se puede establecer una relación entre los conjuntos de soluciones de los dos sistemas.

Proposición 4.1. *Cualquier solución (V, p) del sistema (4.1) proporciona una solución $(V, N = V \circ p)$ del sistema (4.2).*

Demostración. Sea (V_0, p_0) una solución del sistema (4.1). Entonces, el par $(V_0, N_0 = V_0 \circ p_0)$ es una solución del sistema (4.2). □

Además, en algunos casos, existe reciprocidad entre los dos sistemas, como se plantea a continuación.

Proposición 4.2. *Si $t \leq (n-k)/2$ y existe al menos una solución no nula del sistema (4.1), entonces el espacio vectorial de soluciones del sistema (4.2) tiene dimensión igual a 1, y cualquier solución no nula del sistema (4.2) proporciona una solución del sistema (4.1).*

Demostración. Analizamos en primer lugar el caso de que la dimensión del espacio de soluciones del sistema (4.2) sea 0. Esto implica que la única solución es $(0, 0)$, lo que resulta, por la Proposición 4.1, en que la única solución del sistema (4.1) también es $(0, 0)$.

Supongamos ahora que existe una solución no nula (V_0, p_0) del sistema (4.1), de modo que cumple $V_0(y_i) = V_0(p_0(g_i))$. Entonces cualquier solución (V, N) del sistema (4.2) satisface (teniendo en cuenta las propiedades de linealidad de estos particulares polinomios):

$$V_0[N(g_i)] = V_0(V(y_i)) = V_0(V(p_0(g_i)))$$

$$\Rightarrow V_0[N(g_i) - V \circ p_0(g_i)] = 0, \quad \forall i = 1, \ldots, n.$$

El q-polinomio $V_0[N - V \circ p_0](x)$ tiene q-grado $\leq k + 2t - 1$. Además, como $t \leq (n-k)/2$, se tiene que $\deg_q(V_0[N - V \circ p_0]) \leq n - 1$. Sin embargo, hemos visto que este polinomio se anula en al menos n puntos linealmente independientes sobre $\mathbb{F}_q$, luego necesariamente $V_0[N - V \circ p_0](x) = 0$ y, dado que los q-polinomios son un dominio de integridad para la composición, se obtiene que $N = V \circ p_0$. Es decir, cualquier solución (V, N) está completamente determinada por V y el espacio de soluciones del sistema (4.2) es de dimensión 1.

Por último, esto implica que existe algún $\alpha \in \mathbb{F}_{q^m}$ tal que $(V, N) = \alpha(V_0, V_0 \circ p_0)$. Por tanto, el conjunto de soluciones de (4.1) es de la forma $(\alpha V_0, p_0)$. □

4.3. Algoritmos de descodificación

Supongamos que hemos recibido un vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$ donde $\mathbf{c} \in \mathrm{Gab}_k(\mathbf{g})$ y el vector de error $\mathbf{e}$ tiene rango menor o igual a la capacidad de corrección de errores del código. Por la Proposición 4.2, sabemos que basta con encontrar una solución del sistema lineal (4.2) para obtener la solución única del problema de reconstrucción$(\mathbf{y}, \mathbf{g}, k, t)$. Una vez obtenida esta solución, se puede descodificar fácilmente mediante la división euclídea de q-polinomios.

De este modo, el algoritmo de descodificación puede describirse en dos pasos como sigue.

1. Encontrar un par de q-polinomios (V_0, N_0) que sean solución del sistema (4.2).
2. Calcular la división euclídea de N_0 por V_0 y definir $f := N_0/V_0$. En este caso se tendría

$$V_0(y_i) = N_0(g_i) = V_0(f(g_i)) \Rightarrow V_0(y_i - f(g_i)) = 0, \quad \text{para todo } i = 1, \ldots, n.$$

Luego $e_i := y_i - f(g_i) \in \ker V_0$, que tiene dimension $\leq t$ sobre $\mathbb{F}_q$, es decir, $\mathrm{rk}(\mathbf{e}) \leq t$ y, si definimos $\mathbf{c} := f(\mathbf{g})$, tendremos la descomposición

$$y_i = f(g_i) + e_i, \quad \text{para todo } i = 1, \ldots, n.$$

El resto de la sección está dedicado a describir dos algoritmos diferentes para resolver el sistema (4.2), dado que ya sabemos que la división euclídea de q-polinomios del segundo paso puede calcularse en tiempo polinomial (ver el algoritmo en [10]). De hecho, la complejidad computacional de calcular la división euclídea entre N_0 y V_0 es de $(k-1)t$ multiplicaciones en $\mathbb{F}_{q^m}$.

4.3.1. Algoritmo natural

En primer lugar describiremos un *algoritmo más natural*, más básico, aunque poco eficiente. Sean

$$\mathbf{v} := (v_0, \ldots, v_t)^t, \quad \mathbf{n} := (n_0, \ldots, n_{k+t-1})^t.$$

Consideramos las representaciones matriciales V, N sobre $\mathbb{F}_q$ de $\mathbf{v}, \mathbf{n}$, respectivamente, y definimos la matriz:

$$S := \left(\begin{array}{ccc|ccc} g_1 & \cdots & g_1^{[k+t-1]} & y_1 & \cdots & y_1^{[t]} \\ \vdots & & \vdots & \vdots & & \vdots \\ g_n & \cdots & g_n^{[k+t-1]} & y_n & \cdots & y_n^{[t]} \end{array} \right)$$

Entonces resolver el sistema (4.2) es equivalente a resolver el sistema lineal:

$$S \cdot \begin{pmatrix} \mathbf{n} \\ \mathbf{v} \end{pmatrix} = \mathbf{0}. \tag{4.3}$$

Las incógnitas del sistema son los vectores $\mathbf{n}$ y $\mathbf{v}$, es decir, tenemos $k+2t+1$ incógnitas. Por tanto, el coste de resolución del sistema lineal es del orden de $(k+2t)^3$ operaciones sobre $\mathbb{F}_q$. Este coste es demasiado alto para que el algoritmo se pueda implementar de forma eficiente, comparado con otros algoritmos de descodificación existentes.

Tratamos de mejorar este coste computacional. Al observar la ecuación 4.3, se puede ver que una parte de la matriz S es independiente de la palabra recibida, y depende únicamente de los parámetros del código Gabidulin, luego escribiremos

$$S = \left(\begin{array}{c|c} G_1 & Y_1 \\ G_2 & Y_2 \end{array} \right),$$

donde

$$G_1 = \left(g_i^{[j]} \right)_{\substack{i=1,\ldots,\, k+t \\ j=0,\ldots,\, k+t-1}}$$

es la submatriz superior izquierda $(k+t) \times (k+t)$ de S. Como, por definición, los g_i son linealmente independientes, G_1 es una matriz invertible, de modo que resolver la ecuación (4.3) es equivalente a resolver:

$$\left\{ \begin{array}{l} G_1 N + Y_1 V = 0, \\ G_2 N + Y_2 V = 0, \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} N = U \times (Y_1 V), \\ ((T \times Y_1) + Y_2) V = 0, \end{array} \right.$$

donde $U = -G_1^{-1}$ y $T = -G_2 G_1^{-1}$ pueden calcularse previamente. Así, la complejidad total de resolución de este sistema es de

$$\boxed{(k+t)(k+t^2+2t) + \frac{1}{2}t^3 \quad \text{operaciones sobre } \mathbb{F}_{q^m}}.$$

A pesar de que resulta más eficiente que resolver directamente el sistema original, la complejidad de este método sigue siendo demasiado alta (cúbica en t) en comparación con la de otros algoritmos de complejidad, a lo sumo, cuadrática, como es el presentado en el siguiente apartado.

4.3.2. Algoritmo elaborado

A continuación mostraremos un *algoritmo más elaborado* y eficiente para resolver el problema de reconstrucción de polinomios. Recordamos que nuestro objetivo es encontrar dos q-polinomios $V(y)$ de q-grado $\leq t$, y $N(x)$ de q-grado $< k+t$, que satisfagan el sistema (4.2), es decir, tales que

$$V(y_i) - N(g_i) = 0, \quad \forall i = 1, \ldots, n.$$

En este caso, construiremos dos secuencias de manera iterativa de polinomios

$$(V_0^{(i)}(y),\ N_0^{(i)}(x)) \quad \text{y} \quad (V_1^{(i)}(y),\ N_1^{(i)}(x))$$

que, para $i \leq n$, satisfagan la siguiente propiedad:

$$\forall k \leq i, \quad \begin{cases} V_0^{(i)}(y_k) - N_0^{(i)}(g_k) = 0, \\ V_1^{(i)}(y_k) - N_1^{(i)}(g_k) = 0. \end{cases}$$

Denotamos esta propiedad por $\mathcal{P}(i)$.

Si logramos acotar los grados de los polinomios de forma que:

$$\begin{cases} \deg_q(V_0^{(n)}) \leq t, \\ \deg_q(N_0^{(n)}) \leq k-1+t, \end{cases} \quad \text{o bien} \quad \begin{cases} \deg_q(V_1^{(n)}) \leq t, \\ \deg_q(N_1^{(n)}) \leq k-1+t, \end{cases}$$

entonces habremos encontrado los polinomios buscados y estará resuelto el problema.

Para ello, tendremos en cuenta la siguiente idea: como el índice i recorre n posiciones, si los grados de los polinomios se incrementan en cada paso, no se podrá satisfacer la condición de acotación final. Por tanto, debemos encontrar un modo de mantener los grados lo más bajos posible.

Supongamos que se ha construido una secuencia de polinomios que satisface $\mathcal{P}(j)$ para todo $j = 0, \ldots, i < n$. Veremos ahora cómo construir polinomios que satisfacen $\mathcal{P}(i+1)$. Primero definimos las siguientes diferencias de polinomios evaluados,

$$s_0^{(i)} := V_0^{(i)}(y_{i+1}) - N_0^{(i)}(g_{i+1}), \qquad s_1^{(i)} := V_1^{(i)}(y_{i+1}) - N_1^{(i)}(g_{i+1}),$$

que, en caso de valer 0, la propiedad $\mathcal{P}(i+1)$ se satisface inmediatamente.

Llevaremos a cabo un procedimiento en dos pasos, con el fin de construir polinomios que satisfagan $\mathcal{P}(i+1)$.

- El primer paso, más sencillo, consiste en evaluar

$$N_0^{(i+1)}(x) = N_0^{(i)}(x)^{[1]} - s_0^{(i)} N_0^{(i)}(x),$$
$$V_0^{(i+1)}(y) = V_0^{(i)}(y)^{[1]} - s_0^{(i)} V_0^{(i)}(y).$$

  Esto corresponde a la interpolación del polinomio multivariante $Q(x, y) := V(y) - N(x)$ en el punto $[(y_{i+1}, g_{i+1}), 0]$. Comprobamos que para todo $k = 1, \ldots, i+1$, se cumple $V_0^{(i+1)}(y_k) - N_0^{(i+1)}(g_k) = 0$.

  Sin embargo, es importante destacar que este paso incrementa en cada iteración en una unidad el q-grado de los polinomios no nulos (estamos realizando la operación $x \longrightarrow x^{[1]}$).

- El segundo paso consiste en realizar una evaluación cruzada. Se define:

$$N_1^{(i+1)}(x) = s_0^{(i)} N_1^{(i)}(x) - s_1^{(i)} N_0^{(i)}(x),$$
$$V_1^{(i+1)}(y) = s_0^{(i)} V_1^{(i)}(y) - s_1^{(i)} V_0^{(i)}(y).$$

  Esta transformación implica que:

$$\deg_q(N_1^{(i+1)}) \leq \text{máx}\{\deg_q(N_1^{(i)}), \deg_q(N_0^{(i)})\},$$

  con igualdad si los grados de $N_1^{(i)}$ y $N_0^{(i)}$ son distintos. Por tanto, este método no incrementa el grado y se puede verificar que para todo $k = 1, \ldots, i+1$, se tiene:

$$V_1^{(i+1)}(y_k) - N_1^{(i+1)}(g_k) = 0.$$

Esta es la base del algoritmo de descodificación que queremos diseñar. En resumen, habrá pasos donde se incrementan los grados de uno de los pares de polinomios (por ejemplo, $(V_0^{(i)}, N_0^{(i)})$) manteniendo constantes los grados del otro par (por ejemplo, $(V_1^{(i)}, N_1^{(i)})$). Así, se logra controlar el crecimiento del grado y podemos asegurar que uno de los pares satisface las condiciones de acotación en la última iteración.

Ahora procederemos a describir el algoritmo detalladamente (verlo en pseudocódigo al final del capítulo, **Algorithm 1**).

No construiremos las secuencias completas $(N_0^{(i)}, V_0^{(i)})$ y $(N_1^{(i)}, V_1^{(i)})$, sino que modificaremos los polinomios según convenga, por motivos de espacio. Esto implica que en cada paso i, ambos pares de polinomios (N_0, V_0) y (N_1, V_1) satisfacen la propiedad $\mathcal{P}(i)$.

El algoritmo consta de tres etapas, que explicaremos detenidamente.

1. Previa a la computación

- Calcular $\mu_{g_1,\ldots,g_k}(x)$, el único polinomio mónico de q-grado k tal que

$$\mu_{g_1,\ldots,g_k}(g_i) = 0, \quad \text{para todo } i = 1, \ldots, k.$$

- Calcular la lista de polinomios de interpolación de Lagrange de q-grado $k-1$, $\ell_1(x), \ldots, \ell_k(x)$, tales que

$$\forall i = 1, \ldots, k, \quad \begin{cases} \ell_i(g_j) = 0, & \text{si } j \neq i, \\ \ell_i(g_i) = 1, & \text{si } j = i \end{cases}$$

  Este conjunto de q-polinomios conforma una base del espacio vectorial de q-polinomios de q-grado $k-1$.

Para la computación, pueden usarse los algoritmos descritos en [10].

2. Inicialización

- Sean $V_0 = 0$, $N_0 = \mu_{g_1,\ldots,g_k}$.
- Sean $V_1(y) = y$, $N_1 = \sum_{i=1}^{k} y_i \ell_i$,

  Por las propiedades de los polinomios interpoladores ℓ_i, el polinomio N_1 tiene q-grado $k-1$ y cumple $\forall i = 1, \cdots, k, \quad N_1(g_i) = \sum_{j=1}^{k} y_j \ell_j(g_i) = y_i$. Dicho de otro modo, N_1 interpola los valores de la palabra recibida $\mathbf{y} = (y_1, \ldots, y_k)$ en los puntos g_i mediante los polinomios ℓ_i.

2. Aumento de grado alternado

Ahora comprobamos los grados de los pares de polinomios. Intercambiamos en cada paso los roles de N_0 y N_1 y de V_0 y V_1, de forma que siempre incrementamos el grado de N_0 y V_0. En primer lugar, definimos el índice auxiliar

$$s := \left\lfloor \frac{i-k}{2} \right\rfloor .$$

Después del i-ésimo paso tenemos:

- $\deg_q(N_0) = k + s$;
- $\deg_q(V_0) = s$ si $i - k$ es par y $\deg_q(V_0) = s + 1$ si $i - k$ es impar;
- $\deg_q(N_1) = k + s - 1$ si $i - k$ es par y $\deg_q(N_1) = k + s$ si $i - k$ es impar;
- $\deg_q(V_1) = s$.

Por lo tanto, después del paso final n, el par de polinomios (N_1, V_1) satisface la condición para ser una solución del sistema (4.2), ya que

$$\deg_q(N_1) = k + \left\lfloor \frac{n-k}{2} \right\rfloor - 1 \quad \text{y} \quad \deg_q(V_1) = \left\lfloor \frac{n-k}{2} \right\rfloor .$$

4.4. Análisis de complejidad del algoritmo elaborado

La operación más costosa es la multiplicación de elementos en cuerpos finitos, de modo que sera la más relevante, en comparación con las operaciones de potenciación y suma. Procedemos a analizar la complejidad de los procesos descritos en la subsección anterior.

1. Inicialización

De los 4 polinomios de partida (V_0, N_0, V_1, N_1), el único que no puede calcularse de manera previa a la computación del algoritmo es N_1, dado que consiste en una combinación lineal de polinomios de interpolación. Por lo tanto, la complejidad de computar N_1 es de k^2 multiplicaciones en $\mathbb{F}_{q^m}$.

2. Aumento alternado de grado

Analizamos la complejidad del algoritmo en el paso $i \geq k + 1$.

- Cálculo de $s_0^{(i)}$ y $s_1^{(i)}$. Recordamos que

$$s_0^{(i)} := V_0^{(i)}(y_{i+1}) - N_0^{(i)}(g_{i+1}), \qquad s_1^{(i)} := V_1^{(i)}(y_{i+1}) - N_1^{(i)}(g_{i+1}).$$

  Es sencillo verificar que, tanto si $i-k$ es par como si es impar, el coste del cálculo de estos valores es exactamente $2i-1$ multiplicaciones.

- Calcular $s_0N_1(x) - s_1N_0(x)$ y $s_0V_1(y) - s_1V_0(y)$ cuesta igualmente $2i-1$ multiplicaciones.

- Calcular $N_0(x)^q - s_0N_0(x)$ y $V_0(x)^q - s_0V_0(x)$ cuesta i multiplicaciones.

Por tanto, en cada paso $k+1 \leq i \leq n$, se deben realizar $5i-2$ multiplicaciones. Así, el número total de multiplicaciones en este paso es:

$$\sum_{i=k+1}^{n} (5i-2) = 5\sum_{i=k+1}^{n} i - \sum_{i=k+1}^{n} 2$$

Por un lado,

$$5\sum_{i=k+1}^{n} i = 5\sum_{i=1}^{n} i - 5\sum_{i=1}^{k} i = 5\frac{n(n+1)}{2} - 5\frac{k(k+1)}{2} = \frac{5}{2}(n(n+1) - k(k+1))$$

y por otro,

$$\sum_{i=k+1}^{n} 2 = 2(n-k)$$

Luego resulta

$$\sum_{i=k+1}^{n} (5i-2) = \frac{5}{2}(n(n+1) - k(k+1)) - 2(n-k)$$

$$= \frac{5}{2}(n^2+n-k^2-k) - 2(n-k) = \frac{5}{2}(n^2-k^2) + \frac{5}{2}(n-k) - 2(n-k).$$

$$= \frac{5}{2}(n^2-k^2) + \left(\frac{5}{2}-2\right)(n-k) = \frac{5}{2}(n^2-k^2) + \frac{1}{2}(n-k)$$

En conclusión, la complejidad total del algoritmo es de

$$\boxed{\sum_{i=k+1}^{n} (5i-2) + k^2 = \frac{5}{2}n^2 - \frac{3}{2}k^2 + \frac{n-k}{2}} \quad \text{multiplicaciones.}$$

En conclusión, la complejidad de este algoritmo crece de forma cuadrática en los parámetros del código, de modo que presenta una ventaja computacional relevante respecto del algoritmo más sencillo del apartado 4.3.1.

Algorithm 1: Algoritmo de descodificación para códigos de Gabidulin

Entrada: Un código de Gabidulin $Gab_k(\mathbf{g})$ de longitud n con distancia de rango menor o igual a $t = \lfloor (d-1)/2 \rfloor$, y un vector $\mathbf{y} = (y_1, \ldots, y_n)$.

Salida: Un par de polinomios (N_1, V_1) que satisfacen el sistema (4.2).

Paso de inicialización:

$V_0(y) \leftarrow 0$, $V_1(y) \leftarrow y$

$N_0(x) \leftarrow \mu_{g_1,\ldots,g_k}$, $N_1(x) \leftarrow \sum_{i=1}^{k} y_i \ell_i$

Paso de aumento alternado de grado:

for $i \in \{k+1, \ldots, n\}$ **do**

$s_0 \leftarrow V_0(y_i) - N_0(g_i)$

$s_1 \leftarrow V_1(y_i) - N_1(g_i)$

Intercambiar N_0 y N_1, V_0 y V_1, s_0 y s_1

Calcular:

(a) $N_1(x) \leftarrow s_0 N_1(x) - s_1 N_0(x)$

(b) $V_1(y) \leftarrow s_0 V_1(y) - s_1 V_0(y)$

(c) $N_0(x) \leftarrow N_0(x)^q - s_0 N_0(x)$

(d) $V_0(y) \leftarrow V_0(y)^q - s_0 V_0(y)$

return (N_1, V_1)

Conclusiones

Para comenzar este apartado, efectuamos una recapitulación de los principales temas abordados a lo largo del trabajo. Se han presentado los aspectos fundamentales de los cuerpos finitos y los códigos lineales, que han sido indispensables para desarrollar un estudio detallado de los polinomios linealizados. Así, hemos podido comprobar su aplicación a la hora de construir y descodificar códigos de Gabidulin en la métrica del rango, al tiempo que hemos comprendido el contenido algebraico subyacente que los hace apropiados para la resolución de determinados problemas, como los relacionados con la corrección de errores.

A modo de cierre, destacaremos algunas propiedades fundamentales de los polinomios linealizados que justifican su papel central en la teoría de los códigos de Gabidulin. Una de sus características esenciales es preservar la linealidad sobre $\mathbb{F}_q$, así como el hecho de que su conjunto de raíces forma un subespacio vectorial. Esto permite que la evaluación de polinomios linealizados en conjuntos de elementos linealmente independientes sobre $\mathbb{F}_q$ genere palabras del código con un rango controlado directamente por el q-grado del polinomio evaluado. Además, hemos visto que las palabras de un código Gabidulin, $\mathrm{Gab}[n, k]$, pueden verse como la q-transformada inversa de dichos polinomios evaluados, lo que establece una correspondencia algebraica explícita entre el mensaje original y el mensaje codificado. Adicionalmente, hemos comprobado que el empleo de bases normales permite reducir significativamente la complejidad computacional de esta transformación.

Otra de las propiedades principales de estos particulares polinomios es la relación entre la dimensión de su núcleo, su q-grado y el rango de la palabra de código generada por su evaluación. Esta relación nos ha permitido establecer que los códigos de Gabidulin, $\mathrm{Gab}[n, k]$, definidos sobre $\mathbb{F}_{q^m}$ con $n \leq m$, son análogos a los códigos de Reed–Solomon en la métrica del rango y son óptimos en el sentido de que su distancia mínima de rango alcanza la cota de Singleton, es decir, $d = n - k + 1$.

En lo que respecta a la descodificación, la estructura algebraica de los polinomios linealizados ha permitido el desarrollo de algoritmos eficientes, basados en técnicas de interpolación y en la división euclídea dentro del anillo de polinomios linealizados. En el último capítulo, hemos establecido una equivalencia entre la solución del problema de reconstrucción de polinomios linealizados y la del problema de descodificación de los códigos de Gabidulin. Esto nos ha conducido a proponer dos enfoques para la resolución del primero de los problemas. Un primer algoritmo, de implementación más sencilla, resuelve (con una leve optimización) un sistema lineal asociado y presenta una complejidad cúbica. El segundo algoritmo es más eficiente, dado que utiliza una construcción recursiva de pares de polinomios linealizados y alcanza una complejidad computacional cuadrática, ofreciendo así una estrategia práctica para la descodificación en la métrica del rango.

En conclusión, este estudio no sólo permite comprender en profundidad una clase importante de códigos en la métrica del rango, sino que también pone de manifiesto la sólida base algebraica que posibilita su construcción y análisis. Además, se ofrece un punto de partida para investigaciones futuras, tanto en el posible uso de los códigos de Gabidulin en otros ámbitos como en la optimización de algoritmos de descodificación.

Bibliografía

[1] P. Delsarte. Bilinear forms over a finite field with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[2] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–16, 1985.

[3] M. Gadouleau and Z. Yan. Properties of codes with the rank metric. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, San Francisco, CA, USA, 2006.

[4] E. Hernández Rodríguez. *Álgebra y Geometría*. Addisson-Wesley, 1994.

[5] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[6] P. Loidreau. A welch–berlekamp like algorithm for decoding gabidulin codes, 2005.

[7] P. Loidreau. Properties of codes in rank metric. In *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pages 192–198, Pamporovo, Bulgaria, 2008.

[8] T. Migler, K. E. Morrison, and M. Ogle. Weight and rank of matrices over finite fields. urlhttp://arxiv.org/abs/math/0403314, 2004.

[9] E. H. Moore. A two-fold generalization of fermat's theorem. *Bulletin of the American Mathematical Society*, 2:189–199, 1896.

[10] O. Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35 (3):559–584, 1933.

[11] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, 1991.

[12] J. Tena and C. Munuera. *Codificación de la Información*. Universidad de Valladolid, 1997.

[13] A. Wachter-Zeh. *Decoding of block and convolutional codes in rank metric (Doctoral dissertation)*. Université de Rennes; Universität Ulm, 2013.

[14] L. R. Welch and E. R. Berlekamp. Error correction for algebraic block codes, 1986.