Sección de Matemáticas
Universidad de La Laguna

Oswaldo José Pérez Luis

¿Qué familia de códigos es adecuada para la criptografía basada en códigos?

Which family of codes is suitable for code-based cryptography?

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Julio de 2019

Dirigido por
Irene Márquez Corbella

Irene Márquez Corbella

Departamento de Matemáticas,
Estadística e Investigación
Operativa
Universidad de La Laguna
38271 La Laguna, Tenerife

Agradecimientos

Quiero expresar mis más sinceros agradecimientos al grupo de investigación de álgebra por este maravilloso año juntos. Especialmente a mi tutora Irene Márquez Corbella, no solo por guiarme y aconsejarme durante este trabajo, sino también por permitirme descubrir cuánto me motiva este área de las matemáticas y darme una visión más amplia del mismo.

Oswaldo José Pérez Luis
La Laguna, 8 de julio de 2019

Resumen · Abstract

Resumen

Este trabajo comienza explicando la diferencia entre Teoría de códigos y Criptografía, y de cómo siendo dos áreas tan diferentes se pueden fusionar ambas en Criptografía basada en Códigos (CBC), una propuesta interesante para resistir ataques con un ordenador cuántico (Criptografía post-cuántica). Estos esquemas requieren de familias de códigos con algoritmos eficientes de decodificación y que tengan la propiedad de que sean indistinguibles de un código lineal aleatorio. En este trabajo vamos a centrarnos en estudiar las familias de códigos de evaluación de polinomios.

El trabajo continúa con el Capítulo 1, una introducción a la Teoría de códigos; en particular conceptos de códigos lineales, cíclicos y restricción de códigos lineales a otros subcuerpos. Luego, en el Capítulo 2 nos centramos en algunas familias de códigos de evaluación de polinomios. Introducimos estas familias y estudiamos algunas de sus propiedades fundamentales; en particular, los códigos Reed-Solomon y sus generalizaciones, para los que explicamos un algoritmo de decodificación eficiente, y los códigos Reed-Muller, que son códigos de evaluación en varias variables. Finalmente, en el Capítulo 3, trabajamos con la restricción de las familias antes nombradas a subcuerpos más pequeños, como los códigos Goppa, que pueden ser estudiados como la restricción de un código Reed-Solomon generalizado. Además, en este último capítulo explicamos porqué siguen siendo interesantes estos últimos códigos en criptografía.

Palabras clave: *Teoría de códigos – Criptografía basada en códigos – Códigos lineales – Restricción de códigos a otros subcuerpos – Códigos Reed-Solomon – Códigos Reed-Muller – Códigos Alternantes – Códigos Goppa.*

Abstract

This work begins by explaining the difference between Coding Theory and Cryptography, and even being two different areas how they can be merged into Code-based Cryptography (CBC), an interesting proposal to resist attacks from a quantum computer (Post-quantum cryptography). These schemes require a family of codes with an efficient decoding algorithm and which have the property that they are indistinguishable from a random linear code. In this work we will focus on studying the families of polynomial codes.

The work continues with Chapter 1, an introduction to Coding theory; in particular concepts of linear codes, cyclic codes and subfield-subcodes. Then, in Chapter 2, we focus on some families of polynomial codes. We introduce these families and we study some of their fundamental properties; in particular, Reed-Solomon codes and their generalizations, for which we explain an efficient decoding algorithm, as well as Reed-Muller codes, which are polynomial codes in several variables. Finally, in Chapter 3, we work with the subfield-subcodes of some of the previously named families, such as Goppa codes, which can be studied as the subfield-subcode of a generalized Reed-Solomon code. Furthermore, in this last chapter we explain why these last codes are still interesting in cryptography.

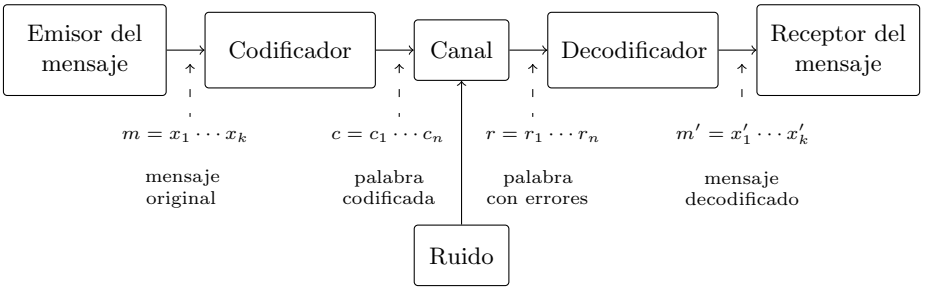
Keywords: *Coding Theory – Code-based Cryptography – Linear codes – Subfield-subcodes – Reed-Solomon codes – Reed-Muller codes – Alternant codes – Goppa codes.*

Índice general

Introducción

Las aplicaciones de los códigos correctores han sido muchas a lo largo de los últimos años: corregir errores en la lectura de CDs, comunicaciones exitosas con el espacio, almacenamiento de información en ordenadores... Los códigos correctores se basan en la idea de añadir información redundante de tal manera que sea posible detectar e incluso corregir errores tras recibir el mensaje; es decir, la Teoría de códigos busca proporcionar confidencialidad y fidelidad en las comunicaciones.

Partimos de que tenemos un mensaje m, con una longitud fijada, formada por letras de un alfabeto $\mathcal{A}$ y que lo codificamos hasta formar una palabra c de un código, aumentando la longitud del mensaje añadiendo información redundante. De esta forma, podemos definir la tasa de información R, un parámetro, que mide la ralentización de la transmisión de información; es decir, representa la proporción de datos que es útil frente a la redundante. El mensaje codificado c se envía a través de un canal (con ruido) que puede producir errores en el mensaje, de tal manera que los símbolos se modifican de acuerdo a ciertas probabilidades que son características del canal. Luego, viene el proceso más delicado en el que la palabra recibida r se decodifica en un mensaje m', obteniedo $m' = m$ cuando no hay errores en la decodificación.



Esquema de canal de comunicación

Dadas las características del canal se puede definir la capacidad C de este, que tiene la propiedad de que para todo $R < C$ (siendo R la tasa de información del código utilizado) es posible encontrar un esquema de codificación y decodificación tal que la probabilidad de que $m' \neq m$ sea relativamente pequeña. La noción de canal debe tomarse en un sentido amplio. No solo la transmisión de información via satélite o telefónica son canales, sino que también el almacenamiento de información en un disco duro de un ordenador se puede modelar como un canal.

No debemos confundir la **Teoría de Códigos**, que tiene como objetivo enviar un mensaje con la mayor eficiencia y confidencialidad posible, con la **Criptografía** que posee un objetivo distinto en el que se pretende hacer confusa la información de tal manera que si un mensaje es interceptado este sea incomprensible. Sin embargo, veremos que ambas áreas se funden para formar esquemas criptográficos muy potentes.

Entre las numerosas técnicas que se practican para el cifrado, una de las más utilizadas actualmente es la **Criptografía de Clave Pública** (o 'PKC' por sus siglas en inglés *Public-Key Cryptography*). Se trata de un criptosistema que emplea dos claves: una pública que se puede difundir a todos los usuarios de forma que cualquiera la puede usar para cifrar un mensaje, y una privada que solo el propietario conoce y le permite descifrar de manera eficiente. La generación de tales claves depende de algoritmos matemáticos basados en una *función unidireccional*, una función que es fácil de calcular pero difícil de invertir (donde "fácil" y "díficil" se deben ententer en el sentido teórico de complejidad computacional). Hacemos notar que la existencia de tales funciones unidireccionales es todavía una conjetura abierta.

A día de hoy, la criptografía es esencial para la seguridad de las comunicaciones. Algunas están protegidas por criptosistemas PKC como puede ser el *Rivest-Shamir-Adleman (RSA)*, en cuyo esquema se toma como parte de la clave pública el producto de dos números primos secretos. Sin embargo, conforme se avanza con el desarrollo de los ordenadores cuánticos, se confirma que muchos de los criptosistemas más comunes serán rotos. Nos referimos a **Criptografía Post-Cuántica** cuando se asume que el atacante puede poseer un ordenador cuántico, de forma que los criptosistemas post-cuánticos buscan mantenerse seguros tanto frente a una posible aparición del ordenador cuántico como a mantenerse seguros frente a los ordenadores actuales, cada vez con más agilidad de cálculo. El desafío principal de la criptografía post-cuántica es satisfacer las demandas de eficacia y flexibilidad de ser utilizada en diferentes dispositivos que aporta la criptografía actual sin sacrificar la confidencialidad del mensaje. Por ejemplo, la seguridad de los criptosistemas RSA está basada en la dificultad que existe de encontrar los factores primos en los que se descompone parte de la clave pública. No obstante, en 1994, Shor introduce un algoritmo cuántico eficiente (trabaja en tiempo polinomial) para encontrar la factorización en primos de un entero positivo aunque este sea grande. El *algoritmo de Shor* tiene un efecto devastador para

la criptografía actual, por lo que a continuación comentaremos qué propuestas actuales de criptosistemas (se cree) son capaces de resistir un ataque cuántico. El concurso NIST que comenzó en 2016 con el objetivo de proponer criptosistemas post-cuánticos eficientes y que puedan estandarizarse para ser utilizados en el día a día recoge estas propuestas que se reducen en tres problemas: criptografía basada en códigos, criptografía basada en retículos y criptografía basada en polinomios quadráticos en varias variables. En esta introducción solo describiremos en detalle el primer problema.

La **Criptografía basada en Códigos** [3, 19] es una de las pocas técnicas matemáticas que permite actualmente la construcción de criptosistemas PKC que son seguros contra atacantes con un ordenador cuántico. Robert McEliece propuso el primer esquema de criptografía basada en códigos en 1978 [11] y actualmente sigue siendo seguro. Veremos los principios básicos de este sistema y qué suposiciones de seguridad deben tomarse, mostrando que se trata de un sistema interesante para criptografía post-cuántica a pesar del gran tamaño que se usa para la clave.

Todos los criptosistemas de estilo McEliece utilizan como clave pública una matriz generatriz G de un código lineal $\mathcal{C}$ definido en $\mathbb{F}_q$ del que se conoce un algoritmo eficiente de decodificación $D_{\mathcal{C}}$. También forma parte de la clave pública el número de errores t que el agoritmo permite corregir. Para cifrar un mensaje $\mathbf{m} \in \mathbb{F}_q^k$ basta con codificar la palabra y añadir tantos errores como podamos corregir; es decir, nuestro mensaje cifrado es $\mathbf{c} = \mathbf{m}G + \mathbf{e}$, con $\mathbf{e} \in \mathbb{F}_q^k$ un vector de error de peso $\mathrm{w_H}(\mathbf{e}) \leq t$. Para descifrar el mensaje y recuperar $\mathbf{m}$ basta con aplicar el algoritmo $D_{\mathcal{C}}$, mientras que los atacantes se ven reducidos a un problema de *decodificación genérica* (es decir, la codificación de un código aleatorio), que se cree que es difícil en general incluso para atacantes con un ordenador cuántico.

Algoritmo 1: Cript. de McEliece

Parámetros: Una familia $\mathcal{F}$ de códigos $[n, k]_q$ que tienen un algoritmo de decodificación eficiente que corrige t errores.

Generación de Claves:

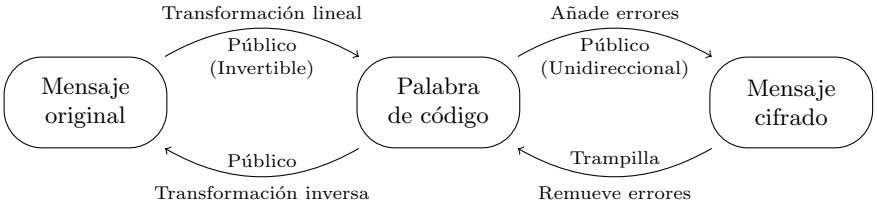
- **Clave pública:** $G \in \mathbb{F}_q^{k \times n}$ matriz generatriz de $\mathcal{C} \in \mathcal{F}$ y t el número de errores.
- **Clave privada:** $D_{\mathcal{C}}$ algoritmo de decodificación para $\mathcal{C}$ que corrige t errores.

Cifrado: Codificar un mensaje $\mathbf{m}$ y añadirle un vector error $\mathbf{e}$ aleatorio de peso $\mathrm{w_H}(\mathbf{e}) \leq t$. Entonces $\mathbf{c} = \mathbf{m}G + \mathbf{e}$.

Descifrado: Aplicar $D_{\mathcal{C}}$ a c y recuperar $\mathbf{m}$.

La seguridad del sistema se basa en dos suposiciones: la decodificación genérica es difícil (no se puede hacer de manera eficiente) y, además, la matriz generatriz del código elegido (que forma parte de la clave pública) es difícil de distinguir de una matriz de un código aleatorio. Esto último se mantiene cierto para la familia de *Códigos Goppa*, pero no ocurre para otras familias de códigos

como pueden ser los *Códigos Reed-Solomon*. La búsqueda de familias de códigos que no se distinguen de códigos aleatorios es uno de los problemas clave de la criptografía basada en códigos.



Esquema de criptosistemas de estilo McEliece

La propuesta original de McEliece [11] estaba basada en códigos Goppa binarios, esta propuesta sigue siendo válida ya que no se ha encontrado ningún ataque que permita recuperar la clave secreta en tiempo razonable; aunque debido a la velocidad de cálculo de los ordenadores actuales y a pequeñas mejoras en algoritmos genéricos de decodificación de códigos lineales, los parámetros que propuso McEliece (que eran utilizar un cógido Goppa binario de longitud $n = 1024$, dimensión $k = 524$ y distancia mínima $t = 101$) ya no son seguros y se han tenido que aumentar para utilizar códigos de parámetros $[n = 2048, k = 1608]$. Más tarde otras familias alternativas con mejor capacidad de corrección fueron propuesta intentando reducir el tamaño de las claves. Por ejemplo:

- Niederreiter en 1986 [14] propuso utilizar *códigos Reed-Solomon generalizados (GRS)*. Quizás esta sería la primera propuesta que todo especialista de códigos hubiese sugerido para criptografía ya que se trata de códigos con algoritmos de decodificación muy eficientes y con la mejor capacidad de corrección posible. Sin embargo su fuerte estructura lineal permitió describir a Sidelnikov y Shestakov en 1992 [20] un ataque. Además, tal y como veremos al final del trabajo, se ha descubierto que estos códigos se pueden distinguir de un código lineal aleatorio, véase [23].
- Un poco más tarde, Berger y Loidreau en 2005 [2] proponen utilizar un *subcódigo de un código GRS*, pero también esta propuesta fue atacada en 2010 por Wieschebrink, véase [23].
- Los *códigos Reed-Muller* binarios también fueron propuestos por Sidelnikov en 1994 en [21], pero esta familia tampoco es segura tal y como demostró Minder y Shokrollahi en 2007 [12].

Los ataques presentados en [12, 20, 23] son ataques que permiten recuperar la clave secreta en tiempo polinomial o sub-exponencial.

1

Introducción a la teoría de códigos

Existen muchos esquemas de codificación y decodificación que satisfacen las condiciones requeridas, pero la elección del mejor código en términos del máximo número de errores que se pueden corregir para cierta tasa de información y longitud dadas no es clara.

En general, los alfabetos del mensaje y de la palabra codificada pueden ser distintos. Nosotros nos restringiremos a estudiar códigos $(n, k)_{\mathcal{A}}$; esto es, el mensaje tiene una longitud fija de k símbolos y la palabra codificada tiene una longitud fija de n símbolos del mismo alfabeto $\mathcal{A}$.

Definición 1.1. *Sea $\mathcal{A}$ un conjunto de q símbolos denominado alfabeto. Sea $\mathcal{A}^n$ el conjunto de todas las n-tuplas $\mathbf{x} = (x_1, \ldots, x_n)$ con elementos $x_i \in \mathcal{A}$. Un código $\mathcal{C}$ de longitud n en $\mathcal{A}$ es un subconjunto no vacío de $\mathcal{A}^n$. Los elementos de $\mathcal{C}$ se dicen palabras de código o simplemente palabras. Si $\mathcal{C}$ contiene M palabras entonces M es el tamaño del código, con $k \coloneqq log_q(M)$. Para estos códigos, el valor $n - log_q(M)$ se denomina la redundancia; mientras que la tasa de información se define como $R \coloneqq {}^{log_q(M)}/_{n}$.*

Definición 1.2. *Sea $\mathcal{C}$ un código $(n, k)_{\mathcal{A}}$. Un codificador de $\mathcal{C}$ es una aplicación inyectiva $\mathcal{E}\colon\ \mathcal{A}^k \longrightarrow \mathcal{A}^n$ tal que $\mathcal{C} = \mathcal{E}(\mathcal{A}^k)$. Sea $\mathbf{c} \in \mathcal{C}$ una palabra de código; entonces existe un único mensaje $\mathbf{m} \in \mathcal{A}^k$ tal que $\mathbf{c} = \mathcal{E}(\mathbf{m})$. Esta $\mathbf{m}$ se denomina el mensaje original de la palabra codificada $\mathbf{c}$.*

Si queremos medir la diferencia entre dos palabras distintas y evaluar la capacidad correctora del código, necesitamos introducir una métrica adecuada en $\mathcal{A}^n$. Una métrica natural empleada en teoría de códigos es la distancia de Hamming, que verifica los axiomas propios de distancia.

Definición 1.3. *Para $\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{A}^n$, la distancia de Hamming $\mathrm{d_H}(x, y)$ se define como el número de coordenadas en los que los vectores $\mathbf{x}$ e $\mathbf{y}$ difieren; es decir, $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) \coloneqq |\{\, i \in \mathbb{N} \mid x_i \neq y_i \,\}|$.*

Proposición 1.4. *[16, Proposición 1.1.9] La distancia de Hamming es una métrica bien definida en $\mathcal{A}^n$. Esto significa que verifica las siguientes propiedades para cualesquiera que sean $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{A}^n$:*

(a) No negativa: $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) \geq 0$, con igualdad únicamente cuando $\mathbf{x} = \mathbf{y}$.
(b) Simétrica: $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = \mathrm{d_H}(\mathbf{y}, \mathbf{x})$.
(c) Desigualdad triangular: $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) \leq \mathrm{d_H}(\mathbf{x}, \mathbf{z}) + \mathrm{d_H}(\mathbf{z}, \mathbf{y})$.

Definición 1.5. *La distancia mínima de un código $\mathcal{C} \in \mathcal{A}^n$ se define como*

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

si $\mathcal{C}$ consiste en más de un elemento. Por definición $d(\mathcal{C}) = n + 1$ si $\mathcal{C}$ está formado únicamente por una palabra. Denotamos por $(n, M, d)_{\mathcal{A}}$ los parámetros de un código $\mathcal{C}$ de longitud n, número de palabras M y distancia mínima d.

Definición 1.6. *Para una palabra $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ su soporte, denotado por $\mathrm{supp}(\mathbf{x})$, se define como el conjunto de coordenadas no nulas de $\mathbf{x}$; esto es, $\mathrm{supp}(\mathbf{x}) \coloneqq \{\, i \in \mathbb{N} \mid x_i \neq 0, \; x_i \in \mathbb{F}_q \,\}$. Además, el peso de Hamming de $\mathbf{x}$ se define como el número de elementos de su soporte y se denota como $\mathrm{w_H}(\mathbf{x})$. El peso mínimo de un código $\mathcal{C}$, denotado por w, se define como el valor mínimo de los pesos de las palabras no nulas:*

$$w = w(\mathcal{C}) \coloneqq \min\{\, \mathrm{w_H}(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}, \;\; \mathbf{x} \neq 0 \,\},$$

de existir $0 \neq \mathbf{x} \in \mathcal{C}$. En caso contrario, por convenio diremos que $w(\mathcal{C}) = n + 1$.

Desde este punto de vista, el problema principal de los códigos correctores es contruir, para una longitud y número de palabras fijas, un código con la distancia mínima más grande posible; pues tal código permite corregir una mayor cantidad de errores (tal y como veremos en la siguiente sección). Asímismo, encontrar algorítmos de codificación y decodificación eficientes para tal código.

1.1. Códigos lineales

Los códigos lineales se introducen en el caso de que el alfabeto sea un cuerpo finito. Estos códigos tienen más estructura y son, por consiguiente, más tangibles que un código arbitrario. A partir de ahora vamos a trabajar con $\mathcal{A} = \mathbb{F}_q$, que denota un cuerpo finito con q elementos. Referimos al lector a la Sección 1.2 para más información sobre cuerpos finitos. Nótese que si el alfabeto $\mathcal{A}$ es un cuerpo finito entonces $\mathcal{A}^n$ tiene estructura de espacio vectoral.

Definición 1.7. *Un código lineal $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$. La dimensión de un código lineal es su dimensión como $\mathbb{F}_q$-espacio vectorial. Denotamos a un código $\mathcal{C}$ de $\mathbb{F}_q$ de longitud n y dimensión k como un código $[n, k]_q$. Además, si d es la distancia mínima del código, entonces llamamos $[n, k, d]_q$ a los parámetros de $\mathcal{C}$.*

Es claro que para un código lineal $[n,k]_q$ su tamaño es $M = q^k$. Además, su tasa de información viene dada por $R = {}^k/_n$ y la redundancia es $n-k$.

Definición 1.8. *Sean $\mathcal{C}$ y $\mathcal{D}$ dos códigos lineales de longitud n en $\mathbb{F}_q$. Si $\mathcal{D} \subseteq \mathcal{C}$ entonces $\mathcal{D}$ se dice un subcódigo de $\mathcal{C}$.*

Observación 1.9. Supongamos que $\mathcal{C}$ es un código $[n,k,d]_q$. Para cada $r \in (1,k)$ existen subcódigos de dimensión r, no necesariamente únicos. La distancia mínima de un subcódigo es siempre mayor o igual que d, siendo d la distancia mínima de $\mathcal{C}$. Por tanto, tomando un subcódigo apropiado, podemos conseguir un nuevo código con la misma longitud n pero con mayor distancia mínima.

Definición 1.10. *Una matriz G de dimensiones $k \times n$ con elementos en $\mathbb{F}_q$ se denomina una matriz generatriz de un código lineal $\mathcal{C}$ si las filas de G forman una base para $\mathcal{C}$.*

Sea $\mathcal{C}$ un código lineal $[n,k]_q$. Como $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k, existe una base que consiste de k palabras linealmente independientes. Supongamos que $\{\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_k}\}$ es dicha base donde $\mathbf{g_i} = (g_{i1}, g_{i2}, \ldots, g_{in})$, para $i = 1, 2, \ldots, k$, y denotemos por G la matriz generatriz de $\mathcal{C}$:

$$G = \begin{pmatrix} \mathbf{g_1} \\ \mathbf{g_2} \\ \vdots \\ \mathbf{g_k} \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} \in \mathbb{F}_q^{k \times n}.$$

Cada palabra $\mathbf{c}$ se puede escribir de manera única como una combinación lineal de elementos de la base; esto es, $\mathbf{c} = m_1\mathbf{g_1} + m_2\mathbf{g_2} + \cdots + m_k\mathbf{g_k}$, donde $m_1, m_2, \ldots, m_k \in \mathbb{F}_q$. Sea $\mathbf{m} = (m_1, m_2, \ldots, m_k) \in \mathbb{F}_q^k$, entonces, $\mathbf{c} = \mathbf{m}G$. La codificación $\mathcal{E}\colon\ \mathcal{A}^k \longrightarrow \mathcal{A}^n$ de un mensaje $\mathbf{m} \in \mathbb{F}_q^k$ a la correspondiente palabra $\mathbf{c} \in \mathbb{F}_q^n$ cuando trabajamos con códigos lineales se puede hacer de manera eficiente simplemente multiplicando vectores y matrices: $\mathbf{c} = \mathcal{E}(\mathbf{m}) \coloneqq \mathbf{m}G$. Hay dos formas de describir un subespacio de un espacio vectorial, de forma explícita dando una base, o de forma implícita mediante el espacio de soluciones de un conjunto de ecuaciones lineales homogéneas. Esto nos dice que existen dos maneras de describir un código lineal, siendo una de estas mediante la matriz generatriz (como ya hemos visto), y la otra implícitamente como un conjunto de ecuaciones lineales homogéneas; es decir, como el núcleo de una matriz. En particular, los códigos lineales están implícitamente definidos por ecuaciones de control (o de paridad) que definiremos más adelante.

Sea $\mathcal{C}$ un código lineal $[n,k]_q$. Supongamos que H es una matriz de dimensiones $m \times n$ con elementos en $\mathbb{F}_q$. Sea $\mathcal{C}$ el núcleo de H, esto es, $\mathcal{C}$ es el conjunto de todos los vectores $\mathbf{c} \in \mathbb{F}_q^n$ tales que $H\mathbf{c}^\top = 0$. Esto nos proporciona m ecuaciones lineales homogéneas que reciben el nombre de ecuaciones de paridad. Nótese que la dimensión k de $\mathcal{C}$ es al menos $n-m$. Luego, si existen filas

linealmente dependientes en la matriz H (esto es, $k > n-m$), se pueden eliminar filas mediante transformaciones elementales hasta obtener una nueva matriz H' de dimensiones $(n-k) \times n$ con todas sus filas independientes y mismo núcleo que H. Por tanto, $\operatorname{rank}(H') = n-k$.

Definición 1.11. *Sea $\mathcal{C}$ un código $[n,k]_q$. Una matriz de dimensiones $(n-k)\times n$ de rango $n-k$ se denomina una matriz de paridad de $\mathcal{C}$ si $\mathcal{C}$ es el núcleo de dicha matriz; esto es, $\mathcal{C} \coloneqq \{\, \mathbf{c} \in \mathbb{F}_q^n \mid H\mathbf{c}^\top = 0 \,\}$.*

Ejemplo 1.12. Sea $\mathcal{C}$ un código lineal con parámetros $[7,4]_7$ con matriz generatriz G y matriz de paridad H las que siguen:

$$G = \begin{pmatrix} 1&1&1&1&1&1&1 \\ 0&1&2&3&4&5&6 \\ 0&1&4&2&2&4&1 \\ 0&1&1&6&1&6&6 \end{pmatrix} \in \mathbb{F}_7^{4\times 7}, \quad H = \begin{pmatrix} 1&1&1&1&1&1&1 \\ 0&1&2&3&4&5&6 \\ 0&1&4&2&2&4&1 \end{pmatrix} \in \mathbb{F}_7^{3\times 7}.$$

En efecto, es fácil comprobar que: $GH^\top = 0$.

La matriz de paridad de un código es útil para detectar errores y como tal veremos que todo código lineal $\mathcal{C}$ tiene una matriz de paridad.

Proposición 1.13. *Sea $\mathcal{C}$ un código $[n,k]_q$. Sea G una matriz generatriz de $\mathcal{C}$ de dimensión $k \times n$ y H una matriz de dimensión $(n-k)\times n$ de rango $n-k$. Entonces H es una matriz de paridad de $\mathcal{C}$ si, y solo si, $GH^\top = 0$, la matriz nula de dimensión $k \times (n-k)$.*

Demostración. Supongamos que H es una matriz de paridad. Para cualquier $\mathbf{m} \in \mathbb{F}_q^k$, tenemos que $\mathbf{m}G$ es es una palabra en $\mathcal{C}$. Por tanto, $HG^\top \mathbf{m}^\top = H(\mathbf{m}G)^\top = 0$; lo que implica que $(H(\mathbf{m}G)^\top)^\top = \mathbf{m}GH^\top = 0$. Dada la arbitrariedad de $\mathbf{m} \in \mathbb{F}_q^k$, necesariamente $GH^\top = 0$.

Recíprocamente, supongamos que $GH^\top = 0$. Por hipótesis, G es una matriz de dimensiones $k\times n$ de rango k y H es una matriz de dimensiones $(n-k)\times n$ de rango $n-k$. Esto nos dice que H es una matriz de paridad de un código $\mathcal{C}'$ de parámetros $[n,k]_q$. Se tiene que $\mathbf{c} = \mathbf{m}G$, para cualquier $\mathbf{c} \in \mathcal{C}$ y para algún $\mathbf{m} \in \mathbb{F}_q^k$. Además, $H\mathbf{c}^\top = H(\mathbf{m}G)^\top = (\mathbf{m}GH^\top)^\top = 0$; es decir, $\mathbf{c} \in \mathcal{C}'$, $\forall \mathbf{c} \in \mathcal{C}$. Luego, como $\mathcal{C}$ y $\mathcal{C}'$ tienen la misma dimensión, $\mathcal{C} = \mathcal{C}'$. Se concluye así que H es una matriz de paridad de $\mathcal{C}$. ■

Proposición 1.14. *La distancia mínima de un código lineal $\mathcal{C}$ es igual a su peso mínimo.*

Demostración. Como $\mathcal{C}$ es un código lineal, tenemos que $0 \in \mathcal{C}$ y que para cualquier $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{C}$, $\mathbf{c_1} - \mathbf{c_2} \in \mathcal{C}$. De las definiciones de peso y distancia de Hamming sigue que $\mathrm{w_H}(\mathbf{x}) = \mathrm{d_H}(0, \mathbf{x})$ y que $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = \mathrm{w_H}(\mathbf{x} - \mathbf{y})$, para todo

$\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Sea $\mathbf{c} \in \mathcal{C}$ una palabra de código de peso mínimo; esto es, $w := \text{mín}(\mathrm{w_H}(\mathcal{C})) = \mathrm{w_H}(\mathbf{c})$. Entonces, $\mathrm{w_H}(\mathbf{c}) = \mathrm{d_H}(0, \mathbf{c})$ y como 0 es una palabra distinta de $\mathbf{c}$, se sigue que $d \leq w$, donde d denota la distancia mínima. Por otro lado, si $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{C}$ son palabras de distancia mínima, tenemos que $\mathrm{d_H}(\mathbf{c_1}, \mathbf{c_2}) = \mathrm{w_H}(\mathbf{c_1} - \mathbf{c_2})$; y como $\mathbf{c_1} - \mathbf{c_2} \in \mathcal{C} \setminus \{0\}$ se sigue que $w \leq d$. Hemos probado que $d \leq w$ y que $w \leq d$, por lo que se concluye que $d = w$. ■

La siguiente proposición da un método de obtener la distancia mínima de un código en términos del número de columnas dependientes de una matriz de paridad.

Proposición 1.15. *Sea H una matriz de paridad de un código $\mathcal{C}$. La distancia mínima $d(\mathcal{C})$ es el menor entero d tal que hay d columnas linealmente dependientes en H.*

Demostración. Sean $\mathbf{h_1}, \ldots, \mathbf{h_n}$ las columnas de la matriz H y sea $\mathbf{c}$ una palabra de código no nula con peso $\mathrm{w_H}(\mathbf{c}) = w$ y soporte $\mathrm{supp}(\mathbf{c}) = \{j_1, j_2, \ldots, j_w\}$, siendo $1 \leq j_1 < \cdots < j_w \leq n$. Entonces, $H\mathbf{c}^\top = 0$; esto es,

$$c_{j_1}\mathbf{h_{j_1}} + c_{j_2}\mathbf{h_{j_2}} + \cdots + c_{j_w}\mathbf{h_{j_w}} = 0, \quad \text{con } c_{j_i} \neq 0,\ \forall i = 1, 2, \ldots, w.$$

Esto nos dice que las columnas $\mathbf{h_{j_1}}, \ldots, \mathbf{h_{j_w}}$ son linealmente dependientes.

Recíprocamente, si $\mathbf{h_{j_1}}, \ldots, \mathbf{h_{j_w}}$ son linealmente dependientes, existen constantes $a_1, \ldots, a_w$ no todas nulas tal que $a_1 h_{j_1}, \ldots, a_w h_{j_w} = 0$. Sea $\mathbf{c}$ la palabra denifida como:

$$\mathbf{c} = \begin{cases} c_j = 0 & \text{si } j \neq j_i \\ c_j = a_i & \text{si } j = j_i \end{cases}, \quad \text{para algún } i \in \{1, 2, \ldots, w\}.$$

Entonces $H\mathbf{c}^\top = 0$, por lo que $\mathbf{c}$ es una palabra no nula con peso $\mathrm{w_H}(\mathbf{c}) \leq w$. ■

Observación 1.16. Si H es una matriz de paridad de un código $\mathcal{C}$, como consecuencia del resultado anterior se presentan los siguientes casos especiales: La distancia mínima de $\mathcal{C}$ es uno si, y solo si, H tiene una columna de ceros; si H no tiene ninguna columna de ceros entonces la distancia mínima de $\mathcal{C}$ es al menos dos, siendo $d = 2$ si, y solo si, H tiene dos columnas linealmente dependientes.

Vamos ahora a introducir el concepto de código dual. Para ello tenemos que definir un producto interno que, en el caso de código lineales, tomaremos el producto interno usual en $\mathbb{F}_q^n$ definido como:

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n, \quad \forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n.$$

Este producto interno es bilineal, simétrico y no degenerado. Sin embargo, la noción de "definido positivo" no tiene mucho sentido cuando trabajamos en un cuerpo finito como sí lo tiene en el conjunto de los números reales. Por ejemplo, si $\mathbb{F}_q^n = \mathbb{F}_2^n$ tenemos que $\mathbf{x} \cdot \mathbf{x} = 0$ si, y solo si, $\mathbf{x}$ tiene peso par, con $\mathbf{x} \in \mathbb{F}_2^n$.

Definición 1.17. *Sea $\mathcal{C}$ un código $[n,k]_q$. Definimos el código dual (u ortogonal) de $\mathcal{C}$ como $\mathcal{C}^\perp := \{\, \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{c}\cdot\mathbf{x} = 0,$ para todo $\mathbf{c} \in \mathcal{C}\,\}$.*

Proposición 1.18. *Sea $\mathcal{C}$ un código $[n,k]_q$ con matriz generatriz G. Entonces $\mathcal{C}^\perp$ es un código $[n,n-k]_q$ con matriz de paridad G.*

Demostración. Por la definición de código dual las siguientes afirmaciones son equivalentes: (a) $\mathbf{x} \in \mathcal{C}^\perp$, (b) $\mathbf{c}\cdot\mathbf{x} = 0$ para todo $\mathbf{c} \in \mathcal{C}$, (c) $\mathbf{m}G\mathbf{x}^\top = 0$ para todo $\mathbf{m} \in \mathbb{F}_q^k$ y (d) $G\mathbf{x}^\top = 0$.

Esto significa que $\mathcal{C}^\perp$ es el núcleo de la matriz G. Como G es una matriz de rango k, tenemos que el espacio vectorial $\mathcal{C}^\perp$ tiene dimensión $n-k$, siendo G una matriz de paridad para $\mathcal{C}^\perp$. ■

Proposición 1.19. *El dual del código dual de $\mathcal{C}$ es $\mathcal{C}$; es decir, $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.*

Demostración. Sea $\mathbf{c} \in \mathcal{C}$. Por definición de código dual, $\mathbf{c}\cdot\mathbf{x} = 0$, $\forall \mathbf{x} \in \mathcal{C}^\perp$; esto es, $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. Además, aplicando la proposición anterior dos veces, $\mathcal{C}$ y $(\mathcal{C}^\perp)^\perp$ tienen la misma dimensión finita; por lo que se da la igualdad. ■

Corolario 1.20. *Sea $\mathcal{C}$ un código lineal de parámetros $[n,k]_q$. Se tiene que:*

(a) G es matriz gen. de $\mathcal{C}$ si, y solo si, G es matriz de paridad de $\mathcal{C}^\perp$.
(b) H es matriz de paridad de $\mathcal{C}$ si, y solo si, H es matriz gen. de $\mathcal{C}^\perp$.

Demostración. La primera afirmación es la Proposición 1.18, mientras que la segunda es consecuencia de la primera aplicada al código dual $\mathcal{C}^\perp$ usando la Proposición 1.19. ■

Hasta ahora hemos introducido algunos parámetros de un código lineal. En teoría de códigos uno de los problemas más básicos es encontrar el mejor valor de un parámetro cuando son conocidos de antemano los demás. Por ello hablaremos a continuación de la siguiente cota, conocida como la Cota de Singleton, que nos dice la mayor distancia mínima de un código lineal cuando es conocida su longitud y su dimensión.

Teorema 1.21 (Cota de Singleton). *Sea $\mathcal{C}$ un código lineal de parámetros $[n,k,d]_q$. Entonces, la distancia mínima de $\mathcal{C}$ verifica $d \leq n-k+1$.*

Demostración. Sea H una matriz de paridad para $\mathcal{C}$ de dimensiones $(n-k)\times n$, con rango $n-k$. Por la Proposición 1.15 sabemos que la distancia mínima de $\mathcal{C}$ es el menor entero d tal que H tiene d columnas linealmente dependientes. Esto significa que todo conjunto de $d-1$ columnas de H son linealmente independientes; es decir, el rango por columnas de H es al menos $d-1$. Se sigue de esto que $n-k \geq d-1$, lo que nos otorga la Cota de Singleton: $d \leq n-k+1$. ■

Definición 1.22. *Sea $\mathcal{C}$ un código de parámetros $[n,k,d]_q$. Si $d = n-k+1$ entonces $\mathcal{C}$ se denomina un código separable de distancia máxima, o bien, un código* MDS *(Maximum Distance Separable).*

No existen códigos de longitud n y distancia mínima d que tengan más palabras que un código MDS con parámetros n y d; o equivalentemente, no existen códigos de longitud n y M palabras de código que tengan una distancia mínima mayor que la de un código MDS con parámetros n y M.

Proposición 1.23. *Sea $\mathcal{C}$ un código $[n,k,d]_q$. Sean G una matriz generatriz y H una matriz de paridad de $\mathcal{C}$. Las siguientes afirmaciones son equivalentes:*

(a) $\mathcal{C}$ es un código MDS.
(b) Cualquier $(n-k)$-tupla de columnas de H son linealmente independientes.
(c) Cualquier k-tupla de columnas de G son linealmente independientes.

Demostración. Como la distancia mínima de $\mathcal{C}$ es d, cualquiera $d-1$ columnas de H son linealmente independientes (Proposición 1.15), y por la Cota de Singleton (Teorema 1.21) tenemos que $d \leq n-k+1$. Por tanto, $d = n-k+1$ si, y solo si, cualquier conjunto de $n-k$ columnas de H son linealmente independientes. Hemos probado así que (a) y (b) son equivalentes.

Supongamos que se da (c). Sea $\mathbf{c}$ una palabra de $\mathcal{C}$ con k coordenadas nulas. Sean $\mathbf{c} = \mathbf{x}G$, para algún $\mathbf{x} \in \mathbb{F}_q^k$, y G' una submatriz cuadrada de k columnas de G correspondientes a las k coordenadas nulas de $\mathbf{c}$. Entonces $\mathbf{x}G' = 0$, siendo necesariamente $\mathbf{x} = 0$ al ser las k columnas de G' linealmente independientes por hipótesis. De esto se sigue que $\mathbf{c} = \mathbf{x}G = 0$, lo que implica que la distancia mínima de $\mathcal{C}$ es al menos $n-(k-1) = n-k+1$. Por tanto, teniendo en cuenta la Cota de Singleton (Teorema 1.21), $\mathcal{C}$ es un código MDS de parámetros $[n,k,n-k+1]_q$.

Recíprocamente, supongamos que $\mathcal{C}$ es un código MDS. Sean G una matriz generatriz de $\mathcal{C}$ y G' una submatriz cuadrada compuesta por k columnas de G. Sea $\mathbf{x} \in \mathbb{F}_q^k$ tal que $\mathbf{x}G' = 0$; entonces $\mathbf{c} = \mathbf{x}G$ es una palabra de código con peso $\mathrm{w_H}(\mathbf{c}) \leq n-k$. Como la distancia mínima de $\mathcal{C}$ es $n-k+1$, se sigue que $\mathbf{c} = 0$. Luego, como el rango de G es k, también $\mathbf{x} = 0$. Por tanto, las k columnas de G' son linealmente independientes. ■

Decimos que un código $\mathcal{C}$ es trivial MDS en $\mathbb{F}_q$ si, y solo si, $\mathcal{C} = \mathbb{F}_q^n$; es decir, $\mathcal{C}$ es equivalente a un código generado por el $\mathbf{1}$ o su dual. Ejemplos de códigos MDS no triviales son los códigos Reed-Solomon en $\mathbb{F}_q$ de longitud $n = q-1$. Los códigos Reed-Solomon y sus generalizaciones serán estudiados más adelante en el siguiente capítulo.

Ejemplo 1.24. El código definido en el Ejemplo 1.12 es un código MDS. En efecto, se puede comprobar que cualesquiera cuatro columnas de G son linealmente independientes y que, igualmente, cualesquiera tres columnas de H son también linealmente independientes.

Proposición 1.25. *El dual de un código* MDS *vuelve a ser un código* MDS.

Demostración. Sea $\mathcal{C}$ un código MDS de parámetros $[n, k, n-k+1]_q$ con matriz de paridad H. Por (b) de la Proposición 1.23, cualquier conjunto de $n-k$ columnas de H son linealmente independientes. Por otro lado, H es una matriz generatriz del código dual $\mathcal{C}^\perp$, y por (c) de la Proposición 1.23, $\mathcal{C}^\perp$ es un código MDS de parámetros $[n, n-k, k+1]_q$. ■

1.2. Cuerpos Finitos

Para la construcción de los códigos lineales necesitamos hacer uso de la teoría básica de cuerpos finitos, conceptos que se tratarán a continuación aunque omitiendo varias de las demostraciones.

Un cuerpo $\mathbb{F}$ es finito si posee un número finito de elementos, donde el número de elementos del cuerpo se dice el orden de $\mathbb{F}$. En general, denotaremos por $\mathbb{F}_q$ al cuerpo finito de q elementos. Aunque no sea obvio, todos los cuerpos finitos con el mismo número de elementos son isomorfos entre sí. Por tanto, $\mathbb{F}_q$ representará al cuerpo finito con q elementos. Si p es un número primo, el conjunto de los enteros $\mathbb{Z}$ módulo p forman un cuerpo, denotado como $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Nótese que esto no es cierto si p no es primo (por ejemplo, $\mathbb{Z}_4$ no es un cuerpo). Estos son los ejemplos más simples de cuerpos finitos y, además, todo cuerpo finito contiene algún $\mathbb{Z}_p$ como subcuerpo.

El anillo cociente del dominio de polinomios en una variable con coeficientes en $\mathbb{F}_p$ módulo un polinomio irreducible de grado r nos permite construir el cuerpo finito $\mathbb{F}_p^r$. Es decir, si $f(x) \in \mathbb{F}_p[x]$ es un polinomio irreducible de grado r entonces el anillo cociente $\mathbb{F}_q \cong \frac{\mathbb{F}_p[x]}{(f(x))}$, donde $(f(x))$ denota el ideal generado por $f(x)$, es un cuerpo con $q = p^r$ elementos. Por abuso de notación, la clase de x módulo $f(x)$ se denota por x; así, los monomios $1, x, \ldots, x^{r-1}$ forman una base de $\mathbb{F}_q$ como $\mathbb{F}_p$-espacio vectorial. Por tanto, cualquier elemento en este cuerpo se representa de manera única por un polinomio $g(x) \in \mathbb{F}_p[x]$ de grado a lo sumo $r-1$. Esto se denomina la representación principal del cuerpo finito $\mathbb{F}_q$, que no es única.

Ejemplo 1.26. Empezamos con un ejemplo de cómo se construye un cuerpo de cuatro elementos, siendo $4 = 2^2$. La base 2 indica que vamos a trabajar en el conjunto de polinomios $\mathbb{F}_2[x]$, mientras que el exponente 2 nos indica el grado del polinomio irreducible en $\mathbb{F}_2[x]$ que vamos a emplear; por ejemplo, tomaremos el polinomio $f(x) = x^2 + x + 1$. (En realidad no existen más polinomios de grado dos irreducibles en $\mathbb{F}_2[x]$.) Se sigue que:

$$\mathbb{F}_4 \cong \frac{\mathbb{F}_2[x]}{(x^2+x+1)} = \{\, f(x) \in \mathbb{F}_2[x] \mid \deg(f(x)) < 2 \,\} = \{0, 1, x, x+1\}.$$

Análogamente, si queremos construir un cuerpo de ocho elementos, nótese que $8 = 2^3$ y se sigue que:

$$\mathbb{F}_8 \cong \frac{\mathbb{F}_2[x]}{(x^3+x^2+1)} = \{\, f(x) \in \mathbb{F}_2[x] \mid \deg(f(x)) < 3 \,\}$$
$$= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

En este caso, podríamos haber tomado también $x^3 + x + 1$ como polinomio irreducible en $\mathbb{F}_2[x]$ para la construcción del cuerpo finito.

Para cualquier cuerpo $\mathbb{F}_p$ y polinomio $f(x)$ en una variable existe un cuerpo $\mathbb{F}_q$ que contiene a $\mathbb{F}_p$ como subcuerpo tal que $f(x)$ se descompone en factores lineales en $\mathbb{F}_q[x]$. El menor cuerpo que cumple estas propiedades es único salvo isomorfismo de cuerpos y recibe el nombre de *cuerpo de descomposición* de $f(x)$ sobre $\mathbb{F}_p$. Nótese que si $\mathbb{F}_q$ es un cuerpo finito entonces $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ es un grupo multiplicativo de orden $q-1$. Luego, $x^{q-1} = 1$, para todo $x \in \mathbb{F}_q^*$; es decir, $x^q = x$, para todo $x \in \mathbb{F}_q$. Por tanto, los ceros del polinomio $x^q - x$ son precisamente los elementos de $\mathbb{F}_q$; esto es, $x^q - x$ se descompone en factores lineales en $\mathbb{F}_q$.

Teorema 1.27. *[16, Teorema 4.2.11] Sea p un primo y $q = p^r$. Existe un cuerpo finito de q elementos isomorfo al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$ y se denota por $\mathbb{F}_q$.*

Que $\mathbb{F}_q$ sea finito implica que existe un entero positivo p tal que: $p \cdot 1 = 1 + \overset{(p)}{\ldots} + 1 = 0$, siendo p el menor entero para el que ocurre esto. Se prueba que el entero p es primo y se denomina la *característica* de $\mathbb{F}_q$. Nótese que $p\alpha = 0$, $\forall \alpha \in \mathbb{F}_q$. El conjunto de p elementos distintos $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ de $\mathbb{F}_q$ es isomorfo al cuerpo $\mathbb{F}_p$ que está contenido en $\mathbb{F}_q$. Simplificando, decimos que $\mathbb{F}_p$ es un subcuerpo de $\mathbb{F}_q$ que recibe el nombre de subcuerpo primo de $\mathbb{F}_q$, siendo este el menor subcuerpo de $\mathbb{F}_q$; o dicho de otra forma, $\mathbb{F}_p$ se trata de la intersección de todos los subcuerpos de $\mathbb{F}_q$. Además, $\mathbb{F}_p$ es único y define la característica de $\mathbb{F}_q$.

Ejemplo 1.28. Tanto el cuerpo $\mathbb{F}_4$ como el cuerpo $\mathbb{F}_8$ contienen al subcuerpo finito $\mathbb{F}_2$, siendo este el menor subcuerpo de ambos. Esto nos dice que la característica de $\mathbb{F}_4$ y de $\mathbb{F}_8$ coincide y es dos.

Como $\mathbb{F}_p$ es un subcuerpo de $\mathbb{F}_q$, con $q = p^r$, tenemos que el cuerpo $\mathbb{F}_q$ es un $\mathbb{F}_p$-espacio vectorial de dimensión finita r. Además, si $\mathbb{F}_q$ es un cuerpo finito con q elementos, entonces $q = p^r$ con p primo.

Teorema 1.29. *[8, Teorema 3.1.1] Sea $\mathbb{F}_q$ un cuerpo finito. Se satisfacen los siguientes enunciados:*

(a) $q = p^r$, para algún p primo.
(b) $\mathbb{F}_q$ contiene al subcuerpo $\mathbb{F}_p$.
(c) $\mathbb{F}_q$ es un $\mathbb{F}_p$-espacio vectorial de dimensión r.

(d) $p\alpha = 0$, *para todo* $\alpha \in \mathbb{F}_q$.
(e) $\mathbb{F}_q$ *es único salvo isomorfismos.*
(f) Todos los subcuerpos de $\mathbb{F}_{p^r}$ *son* $\mathbb{F}_{p^s}$ *con* s *divisor de* r.

Observación 1.30. Sea $\mathbb{F}_q$ un cuerpo finito. Entonces:

$$(x+y)^q = x^q + y^q, \quad \forall x, y \in \mathbb{F}_q.$$

En efecto, si $q = p$, con p primo basta darse cuenta que al desarrollar $(x+y)^p$ con la fórmula del binomio de Newton, $\binom{p}{i}$ es divisible por p, para todo $i = 1, 2, \ldots, p-1$, por lo que los términos que acompañan a $\binom{p}{i}$ se anulan. Si $q = p^r$ con $r > 1$ se procede por inducción.

Proposición 1.31. *[8, Teorema 3.3.1] El grupo multiplicativo* $\mathbb{F}_q^*$ *de orden* $q-1$ *es cíclico. Si* γ *es un generador de este grupo cíclico entonces* $\mathbb{F}_q = \{0, 1 = \gamma^0, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$, *y* $\gamma^i = 1$ *si, y solo si,* $(q-1) \mid i$.

Definición 1.32. *Un generador del grupo* $\mathbb{F}_q^*$ *se denomina elemento primitivo.*

Ejemplo 1.33. Fijémonos en el grupo multiplicativo $\mathbb{F}_8^* = \mathbb{F}_8 \setminus \{0\}$. Se trata de un grupo conmutativo de siete elementos, donde todos sus elementos, salvo el 1, tienen orden siete (pues el orden de un elemento tiene que ser un divisor del orden gel grupo); es decir, el grupo es cíclico. En particular, el polinomio x tiene orden siete y es, por tanto, generador: $\mathbb{F}_8^* = \langle x \rangle$. En efecto, x es un elemento primitivo de $\mathbb{F}_8^*$:

$$\mathbb{F}_8^* = \{x, x^2, x^3 = x^2 + 1, x^4 = x^2 + x + 1, x^5 = x + 1, x^6 = x^2 + x, x^7 = 1\}.$$

Observación 1.34. Si x es un elemento primitivo de $\mathbb{F}_q^*$ entonces x^i con $\mathrm{mcd}(i, q-1) = 1$ también es un generador de $\mathbb{F}_q^*$. Por lo tanto, hay $\phi(q-1)$ elementos primitivos, donde ϕ representa la función phi de Euler.

Sea $\mathbb{E}$ una extensión de cuerpos finita de $\mathbb{F}_q$. Entonces $\mathbb{E}$ es un $\mathbb{F}_q$-espacio vectorial; es decir, necesariamente $\mathbb{E} = \mathbb{F}_{q^t}$, para algún entero positivo t. Cada elemento $\alpha \in \mathbb{E}$ es una raíz del polinomio $x^{q^t} - x$. Por tanto, existe un polinomio mónico $m_\alpha(x)$ en $\mathbb{F}_q[x]$ que tiene a α como raíz con el menor grado posible. A tal polinomio $m_\alpha(x)$ se le denomina el *polinomio mínimo* de α en $\mathbb{F}_q$. En el siguiente teorema se recogen varios hechos elementales sobre los polinomios mínimos:

Teorema 1.35. *[8, Teorema 3.7.1] Sean* $\mathbb{F}_{q^t}$ *una extensión de cuerpos finita de* $\mathbb{F}_q$ *y* α *un elemento de* $\mathbb{F}_{q^t}$ *con polinomio mínimo* $m_\alpha(x) \in \mathbb{F}_q[x]$. *Se verifican:*

(a) $m_\alpha(x)$ *es polinomio mónico irreducible en* $\mathbb{F}_q$.
(b) Si $g(x) \in \mathbb{F}_q[x]$ *es tal que* $g(\alpha) = 0$, *entonces* $m_\alpha(x) \mid g(x)$.
(c) $m_\alpha(x)$ *es único; esto es, solo hay un polinomio mónico en* $\mathbb{F}_q[x]$ *que tiene a* α *como raíz con el menor grado posible.*

Si partimos de un polinomio irreducible $f(x)$ en $\mathbb{F}_q$ de grado r, podemos añadir una raíz α de $f(x)$ a $\mathbb{F}_q$ y obtener el cuerpo $\mathbb{F}_{q^r} \cong \mathbb{F}_q[\alpha]$ de tal manera que todas las raíces de $f(x)$ se encuentren en $\mathbb{F}_{q^r}$.

Teorema 1.36. *[8, Teorema 3.7.2] Sea $f(x)$ un polinomio mónico irreducible en $\mathbb{F}_q$ de grado r. Entonces:*

(a) Todas las raíces de $f(x)$ se encuentran en $\mathbb{F}_{q^r}$ y en cualquier cuerpo que contenga a $\mathbb{F}_q$ y alguna raíz de $f(x)$.
(b) $f(x) = \prod_{i=1}^{r}(x - \alpha_i)$, donde $\alpha_i \in \mathbb{F}_{q^r}$ para $1 \leq i \leq r$.
(c) $f(x) \mid x^{q^r} - x$.

Observación 1.37. En particular, este teorema se verifica para los polinomios mínimos $m_\alpha(x)$ en $\mathbb{F}_q$ ya que estos son polinomios mónicos irreducibles.

Dos elementos de $\mathbb{F}_{q^t}$ que tienen el mismo polinomio mínimo en $\mathbb{F}_q[x]$ se dicen *conjugados* en $\mathbb{F}_q$. En la siguiente sección será importante encontrar todos los elementos conjugados de $\alpha \in \mathbb{F}_q$; esto es, todas las raíces de $m_\alpha(x)$ (y ya sabemos que todas son distintas y se encuentran en $\mathbb{F}_{q^t}$). Para hallar estas raíces podemos hacer uso del siguiente teorema:

Teorema 1.38. *[8, Teorema 3.7.4] Sean $f(x)$ un polinomio en $\mathbb{F}_q[x]$ y α una raíz de $f(x)$ en alguna extensión de cuerpo finita $\mathbb{F}_{q^t}$. Entonces:*

(a) $f(x^q) = f(x)^q$.
(b) α^q es también una raíz de $f(x)$ en $\mathbb{F}_q$.

Aplicando este teorema las veces que haga falta podemos ver que α, α^q, $\alpha^{q^2} \ldots$ son las raíces de $m_\alpha(x)$. Nótese que esta sucesión es finita y terminará en r términos, siendo $\alpha^{q^r} = \alpha$. Supongamos ahora que γ es un elemento primitivo de $\mathbb{F}_{q^t}$. Entonces $\alpha = \gamma^s$ para algún entero positivo s. Esto nos dice que $\alpha^{q^r} = \alpha$ si, y solo si, $\gamma^{sq^r - s} = 1$. Por la Proposición 1.31 tenemos que: $sq^r \equiv s \mod q^t - 1$. Basándonos en este hecho, podemos definir la clase ciclotómica de s módulo $q^t - 1$:

Definición 1.39. *Sea s un entero tal que: $0 \leq s < q^t - 1$. La clase ciclotómica de s módulo $q^t - 1$ (respecto de q) se define como el conjunto:*

$$C_s := \{\, sq^j \mod q^t - 1 \mid j \geq 0 \,\} = \{s, sq, sq^2, \ldots, sq^{j-1}\},$$

donde j es el menor entero positivo tal que $sq^j \equiv s \mod q^t - 1$ y s es el menor elemento que pertenece a C_s. A este s se le denomina el representante de la clase ciclotómica.

Observación 1.40. El conjunto de clases ciclotómicas C_s particiona el conjunto $\{0, 1, 2, \ldots, q^t - 2\}$ de enteros en conjuntos disjuntos. En efecto, cada $0 \leq k <$

q^t-1 pertenece a una clase ciclotómica C_s. Supongamos que las clases C_s y $C_{s'}$ no son disjuntas; es decir, $C_s \cap C_{s'} \neq \emptyset$. Esto nos dice que existen $0 < i \leq j$ enteros positivos tales que $sq^i = s'q^j$, si y solo si, $s = s'q^{j-i}$. Ahora, si multiplicamos a ambos miembros de la igualad por q^m, con $m \in \mathbb{N}$, se sigue que $sq^m = s'q^{j-i+m}$. Esto implica que $C_s \subseteq C_{s'}$. Por otro lado, nótese que q es un elemento invertible en $\mathbb{Z}_{q^t-1}$; esto es, existe $e \in \mathbb{N}$ tal que $q^e \equiv 1 \mod q^t - 1$. Entonces, de la igualdad $s'q^{j-i+m} = sq^m$ y teniendo en cuenta que $q^e = q^{j-i}q^{e-j+i}$, se sigue que $s'q^m = sq^mq^{e-j+i} = sq^{e-j+i+m}$, con $m \in \mathbb{N}$. Esto nos dice que $C_{s'} \subseteq C_s$; luego, hemos probado que si dos clases ciclotómicas C_s y $C_{s'}$ tienen algún elemento en común, necesariamente son iguales. Se concluye así que el conjunto de clases ciclotómicas particiona el conjunto $\{0, 1, 2, \ldots, q^t - 2\}$ en conjuntos disjuntos.

Las raíces de $m_\alpha(x) = m_{\gamma^s}(x)$ incluye al conjunto de elementos $\{\, \gamma^i \mid i \in C_s \,\}$. De hecho, estas son todas las raíces del polinomio mínimo. Por tanto, si conocemos el tamaño de C_s también conocemos el grado de $m_{\gamma^s}(x)$. Esto se ve reflejado en el siguiente resultado:

Teorema 1.41. *Sean $n \in \mathbb{Z}$ un entero positivo y $m \in \mathbb{Z}$ el menor entero positivo tal que $q^m \equiv 1 \mod n$. Sea $\alpha^n = 1$ con $\alpha \in \mathbb{F}_{q^m}$. Entonces, para cada entero s, con $0 \leq s < n$, el polinomio mínimo de α^s en $\mathbb{F}_q$ es $m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i)$, siendo C_s la clase ciclotómica de s módulo n. Además, $(x^n - 1) = \prod_s m_{\alpha^s}(x)$, es la factorización de $(x^n - 1)$ en factores irreducibles en $\mathbb{F}_q$, donde s recorre un conjunto de representantes de las clases ciclotómicas módulo n.*

Demostración. Sea $m \in \mathbb{Z}$ tal que $q^m \equiv 1 \mod n$ con m el menor entero positivo que verifica la ecuación: $\alpha^n = \alpha^{q^m-1} = 1$ (pues $\mathbb{F}^*_{q^m}$ es cíclico). Esto nos dice que $\mathbb{F}_{q^m}$ contiene una raíz n-ésima de la unidad α; esto es, $\alpha^n = 1$. Como α^i, $0 \leq i < n$, son distintos dos a dos y $(\alpha^i)^n = 1$, podemos asegurar que $\mathbb{F}_{q^m}$ contiene todas las raíces del polinomio $x^n - 1$; esto es, $\mathbb{F}_{q^m}$ es el cuerpo de descomposición de $x^n - 1$ en $\mathbb{F}_q$. Por tanto, los factores irreducibles de $x^n - 1$ en $\mathbb{F}_q$ deben ser el producto de polinomios mínimos de las n-ésimas raíces de la unidad en $\mathbb{F}_{q^m}$.

Supongamos que γ es un elemento primitivo de $\mathbb{F}_{q^m}$. Entonces $\alpha = \gamma^d$ es una n-ésima raíz primitiva de la unidad (es decir, $\alpha^s \neq 1$, para todo $0 < s < n$), donde $d = {}^{(q^m-1)}/_n$. Luego, las raíces del polinomio mínimo de α^s sobre $\mathbb{F}_q$ son $\{\alpha^s, \alpha^{sq}, \alpha^{sq^2}, \ldots, \alpha^{sq^{j-1}}\}$, siendo j el menor entero positivo tal que:

$$dsq^j \equiv ds \mod q^t - 1, \text{ si y solo si, } sq^j \equiv s \mod q^t - 1.$$

Teniendo en cuenta que hemos definido el conjunto $C_s \coloneqq \{\, sq^j \mod n \mid j \geq 0 \,\}$, hemos probado que, para cada $0 \leq s < n$, el polinomio mínimo de α^s en $\mathbb{F}_q$ es:

$$m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i).$$

■

Ejemplo 1.42. Sean $n = 7$ y $q = 2$. Las clases ciclotómicas módulo 7 son:

$$\begin{aligned} C_0 &= \{\, 0 \cdot 2^j \mod 7 \mid j \geq 0 \,\}\{0\}. \\ C_1 &= \{\, 1 \cdot 2^j \mod 7 \mid j \geq 0 \,\} = \{1, 2, 4\}. \\ C_3 &= \{\, 3 \cdot 2^j \mod 7 \mid j \geq 0 \,\} = \{3, 5, 6\}. \end{aligned}$$

Obsérvese que: $C_0 \cup C_1 \cup C_3$=$\{0,1,2,3,4,5,6\}$, siendo las clases C_s disjuntas. Por otra parte, un elemento primitivo α se encuentra en el cuerpo $\mathbb{F}_{2^3} = \mathbb{F}_8$, y no en ninguna otra extensión finita de cuerpos de $\mathbb{F}_2$ más pequeña que esta. Además, por el Teorema 1.41 los factores irreducibles del polinomio $x^n - 1$ en $\mathbb{F}_2$ tienen grado 1, 3 y 3, siendo estos los polinomios mínimos de α^s, $s = 0, 1, 3$, donde s es el representante de las clases ciclotómicas C_s:

$$\begin{aligned} m_{\alpha^0}(x) &= \prod_{i \in C_0} (x - \alpha^i) = x - \alpha^0 = x + 1. \\ m_{\alpha^1}(x) &= \prod_{i \in C_1} (x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^4). \\ m_{\alpha^3}(x) &= \prod_{i \in C_3} (x - \alpha^i) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6). \end{aligned}$$

Nótese que hay dos polinomio irreducibles de grado tres en $\mathbb{F}_2$, siendo estos: $x^3 + x + 1$ y $x^3 + x^2 + 1$. El resto de polinomios de grado tres en $\mathbb{F}_2[x]$ son reducibles pues tienen raíces en $\mathbb{F}_2$. Por tanto, la factorización del polinomio es $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Corolario 1.43. *El cardinal de cada clase ciclotómica módulo n es un divisor de $m \in \mathbb{Z}$, siendo m el menor entero positivo que verifica $q^m \equiv 1 \mod n$. En particular, $|C_1| = m$.*

Demostración. Sean $m \in \mathbb{Z}$ el menor entero positivo tal que $q^m \equiv 1 \mod n$ y $t = |C_s|$. Entonces el polinomio mínimo $m_{\alpha^s}(x)$ tiene grado t, siendo α un elemento primitivo. Esto nos dice que t divide a m. ■

1.3. Códigos Cíclicos

Cuando estudiemos un código cíclico $\mathcal{C}$ de longitud n será conveniente pensar en las coordenadas de una palabra $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. En esta sección veremos la equivalencia que existe entre los ideales de un anillo cociente y los códigos cíclicos. Trabajaremos con clase ciclotómicas para poder representar un código cíclico de manera que quede unívocamente determinado. En esta sección también dejaremos resultados sin demostrar (por falta de espacio).

Definición 1.44. *Un código lineal $\mathcal{C}$ en $\mathbb{F}_q$ de longitud n se dice cíclico si contiene las distintas permutaciones cíclicas de cada palabra $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$; esto es, si $(c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$ entonces $(c_1, c_2, \ldots, c_{n-1}, c_0) \in \mathcal{C}$.*

Por conveniencia, representaremos las palabras de código en forma polinómica. De esta manera, podemos identificar el cuerpo $\mathbb{F}_q^n$ con el espacio vectorial de polinomios de grado menor que n utilizando la relación:

$$\mathbf{c} = (c_0, c_1, \ldots, c_n) \longleftrightarrow c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x].$$

Nótese que un código cíclico $\mathcal{C}$ es invariante bajo permutaciones cíclicas; esto es, si $c(x) \in \mathcal{C}$ entonces también $xc(x) \in \mathcal{C}$ cuando multiplicamos módulo $x^n - 1$. Teniendo en cuenta esta correspondencia podemos estudiar los códigos cíclicos como los ideales del anillo cociente

$$\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{(x^n - 1)},$$

que se reduce al estudio de ideales generados por polinomios que dividen al polinomio $x^n - 1$.

Supondremos a lo largo del capítulo que $\mathrm{mcd}(q, n) = 1$. Si esto ocurre entonces el polinomio $x^n - 1$ tiene $n-1$ raíces distintas entre sí. Esto nos permitirá describir los códigos cíclicos a partir de clases ciclotómicas módulo n, donde recordemos que $C_s \coloneqq \{\, sq^j \mod n \mid j \geq 0 \,\}$, siendo j el menor entero positivo tal que $sq^j \equiv s \mod n$, representa la clase ciclotómica de s módulo n.

Teorema 1.45 (Teorema Fundamental de códigos cíclicos).
Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$ de longitud n definitido en $\mathbb{F}_q$. Existe un polinomio $g(x) \in \mathcal{C}$ que verifica las propiedades siguientes:

(a) $g(x)$ es el único polinomio mónico de grado mínimo en $\mathcal{C}$.
(b) $\mathcal{C} = \langle g(x) \rangle$.
(c) $g(x) \mid (x^n - 1)$.

Demostración. Sean $\mathcal{C}$ un código cíclico y $g(x) \in \mathcal{C}$:
"(a)" Supongamos por reducción al absurdo que existen $g_1(x)$ y $g_2(x)$ polinomios mónicos diferentes de grado mínimo en $\mathcal{C}$. Se tiene que $0 \neq g_1(x) - g_2(x) \in \mathcal{C}$ y que: $\deg(g_1(x) - g_2(x)) < \deg(g_1(x)) \wedge \deg(g_1(x) - g_2(x)) < deg(g_2(x))$. Pero esto contradice la hipótesis de minimalidad de $g_1(x)$ y $g_2(x)$.
"(b)" Para todo $\mathbf{c} \in \mathcal{C}$ existen polinomios $h(x)$ y $r(x)$ tales que;

$$c(x) = g(x)h(x) + r(x), \quad \text{con } \deg(r(x)) < \deg(g(x)) \vee r(x) = 0.$$

En particular, $r(x) = c(x) - g(x)h(x) \in \mathcal{C}$, pero esto no es posible pues $g(x)$ es el polinomio mínimo en $\mathcal{C}$.
"(c)" Tenemos que $\mathcal{C}$ es un ideal del anillo cociente $F_q[x]/(x^n - 1)$ y que $0 \in \mathcal{C}$; es decir, también $x^n - 1 \in \mathcal{C}$. Como $\mathcal{C} = \langle g(x) \rangle$, podemos escribir $x^n - 1 = g(x)h(x)$, para algún polinomio $h(x) \in \mathcal{C}$; esto es, g(x) es un divisidor de $x^n - 1$. ■

Proposición 1.46. *[8, Teorema 4.2.1] En las condiciones del teorema anterior, sean* $k = n - \deg(g(x))$ *y* $g(x) = \sum_{i=0}^{n-k} g_i x^i$*, donde* g_{n-k}*=1. Entonces,*

(d) la dimensión del código $\mathcal{C}$ *es* k *y* $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ *es una base.*
(e) todo elemento de $\mathcal{C}$ *se expresa de manera única como producto de polinomios* $g(x)f(x)$*, donde: o bien* $f(x) = 0$*, o bien* $\deg(f(x)) < k$*.*
(f) la matriz

$$\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix} \leftrightarrow \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} \in \mathbb{F}_q^{k\times n}$$

es la matriz generatriz del código $\mathcal{C}$*.*
(g) si α *es un elemento primitivo para alguna extensión de cuerpo finita de* $\mathbb{F}_q$ *entonces* $g(x) = \prod_s m_{\alpha^s}(x)$*, donde el producto se encuentra en un subconjunto de representantes de clases ciclotómicas módulo* n*.*

Ejemplo 1.47. Supongamos que queremos construir un código definido en $\mathbb{F}_2$ de longitud $n = 15$; para ello sabemos que hay tantos códigos cíclicos sobre $\mathbb{F}_2$ de longitud 15 como divisores mónicos del polinomio $x^{15} - 1$ en $\mathbb{F}_2[x]$.

Las clases ciclotómicas módulo 15 son:

$$\begin{aligned} C_0 &= \{\, 0 \cdot 2^j \mod 15 \mid j \geq 0 \,\} = \{0\}. \\ C_1 &= \{\, 1 \cdot 2^j \mod 15 \mid j \geq 0 \,\} = \{1, 2, 4, 8\}. \\ C_3 &= \{\, 3 \cdot 2^j \mod 15 \mid j \geq 0 \,\} = \{3, 6, 9, 12\}. \\ C_5 &= \{\, 5 \cdot 2^j \mod 15 \mid j \geq 0 \,\} = \{5, 10\}. \\ C_7 &= \{\, 7 \cdot 2^j \mod 15 \mid j \geq 0 \,\} = \{7, 11, 13, 14\}. \end{aligned}$$

Sea α un el elemento primitivo de $\mathbb{F}_{2^4} = \mathbb{F}_{16}$. Los polinomios mínimos de α^s, $s = 0, 1, 3, 5, 7$, se escriben:

$$\begin{aligned} m_0(x) &= \prod_{i\in C_0} (x - \alpha^i) = x + 1. \\ m_1(x) &= \prod_{i\in C_1} (x - \alpha^i) = x^4 + x + 1. \\ m_3(x) &= \prod_{i\in C_3} (x - \alpha^i) = x^4 + x^3 + x^2 + x + 1. \\ m_5(x) &= \prod_{i\in C_5} (x - \alpha^i) = x^2 + x + 1. \\ m_7(x) &= \prod_{i\in C_7} (x - \alpha^i) = x^4 + x^3 + 1. \end{aligned}$$

Luego, se sigue que:

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

En particular, el código generado por $g(x)=x^4+x^3+1$ es un código cíclico de longitud 15 y dimensión $11=n-\deg(g(x))$ en $\mathbb{F}_2$. Además, su matriz generatriz se escribe:

$$G=\begin{pmatrix} 1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\ 0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1 \end{pmatrix}\in\mathbb{F}_q^{11\times 15}.$$

Proposición 1.48. *[16, Teorema 4.1.37] El código dual $\mathcal{C}^\perp$ de un código cíclico $\mathcal{C}$ es también un código cíclico. Sea $\mathcal{C}$ un código cíclico con parámetros $[n,k]_q$ y polinomio generador $g(x)$. Consideramos el polinomio:*

$$h(x)=\frac{x^n-1}{g(x)}=\sum_{i=0}^{k}h_ix^i,$$

que recibe el nombre de polinomio de control de $\mathcal{C}=\langle g(x)\rangle$. Entonces, el polinomio generador del código dual $\mathcal{C}^\perp$ es:

$$g^\perp(x)=\frac{x^kh(x^{-1})}{h(0)}.$$

En particular, una matriz de paridad de $\mathcal{C}$ se expresa como:

$$H=\begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0\\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}\in\mathbb{F}_q^{(n-k)\times n}.$$

1.4. Ceros de un código cíclico

Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$ con polinomio generador:

$$g(x)=\prod_s m_{\alpha^s}(x)=\prod_s\prod_{i\in\mathcal{C}_s}(x-\alpha^i),$$

donde s recorre algún subconjunto de representantes de las clases ciclotómicas C_s módulo n. Denotamos $T=\cup_sC_s$ al conjunto representativo que define $g(x)$. El conjunto $\mathrm{Z}(\mathcal{C})=\{\,\alpha^i\mid i\in T\,\}$ se denomina el *conjunto de ceros* del código cíclico $\mathcal{C}$, mientras que $\{\,\alpha^i\mid i\notin T\,\}$ es el conjunto de no ceros de $\mathcal{C}$.

Ejemplo 1.49. Sea $\mathcal{C}$ el código definido en $\mathbb{F}_2$ de longitud 15 generado por:

$$g(x) = m_1(x)m_3(x) = (1+x+x^4)(1+x+x^2+x^3+x^4) = (1+x^4+x^6+x^7+x^8)$$

donde $m_1(x)$ y $m_3(x)$ son los polinomios mínimos que ya calculamos en el Ejemplo 1.47. Nótese que $\mathcal{C} = \langle g(x) \rangle$ es un código de parámetros $[15, 7]_2$. Además, su conjunto de ceros se escribe $\mathrm{Z}(\mathcal{C}) = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}\}$. Obsérvese que la dimensión de $\mathcal{C}$ es $n - |\mathrm{Z}(\mathcal{C})| = 15 - 8 = 7$.

Observación 1.50. El conjunto representativo T depende del elemento primitivo α que se tome y, por consiguiente, también el conjunto de ceros $\mathrm{Z}(\mathcal{C})$ del código.

Teorema 1.51. *Sean α un elemento primitivo en alguna extensión de cuerpo finita de $\mathbb{F}_q$ y $\mathcal{C}$ un código cíclico de longitud n en $\mathbb{F}_q$ con conjunto representativo $T = \cup_s C_s$ y polinomio generador $g(x)$. Entonces,*

(a) $g(x) = \prod_{i \in T}(x - \alpha^i)$.
(b) $c(x) \in \mathcal{R}_n$ está en $\mathcal{C}$ si, y solo si, $c(\alpha^i) = 0$ para todo $i \in T$.
(c) la dimensión de $\mathcal{C}$ es $n - |\mathrm{Z}(\mathcal{C})|$.

Demostración. Sea $m \in \mathbb{Z}$ el menor entero positivo tal que $q^m \equiv 1 \mod n$. Esto nos dice que $\mathbb{F}_{q^m}$ es el cuerpo de descomposición del polinomio $x^n - 1$; es decir, $\mathbb{F}_{q^m}^*$ está generado por el elemento primitivo $\alpha \in \mathbb{F}_{q^m}$. Además, sabemos que $x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$, es la factorización de $x^n - 1$ en factores lineales en $\mathbb{F}_{q^m}$ (recordemos que estamos suponiedo que: $\mathrm{mcd}(q, n) = 1$). Más aún, sabemos que $x^n - 1 = \prod_s m_{\alpha^s}(x)$, es la factorización de $x^n - 1$ en factores irreducibles en $\mathbb{F}_q$, donde s recorre un conjunto de representantes de las clases ciclotómicas módulo n. Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$ con polinomio generador:

$$g(x) = \prod_s m_{\alpha^s(x)} = \prod_s \prod_{i \in C_s} (x - \alpha^i),$$

y sea $T = \cup_s C_s$ la unión de estas clases cliclotómicas módulo n. Por el apartado (g) de la Proposición 1.46, se sigue que una palabra de código $c(x) \in \mathcal{C}$ si, y solo si, $c(\alpha^i) = 0$ para cada $i \in T$.

Nótese que T, y por tanto el conjunto de ceros de $\mathcal{C}$, determinan unívocamente el polinomio generador $g(x)$; esto es, $g(x) = \prod_{i \in T}(x - \alpha^i)$. Como el polinomio $g(x)$ tiene grado $\deg(g(x)) = |T| = |\mathrm{Z}(\mathcal{C})|$, la Proposición 1.46 nos asegura que la dimensión del código es: $\dim(\mathcal{C}) = n - |\mathrm{Z}(\mathcal{C})|$. ■

Teorema 1.52 (Cota de BCH). ***[16, Teorema 4.5.3]*** *Sea $\mathcal{C}$ un código cíclico de longitud n en $\mathbb{F}_q$ con conjunto representativo T. Supongamos que $\mathcal{C}$ tiene peso mínimo d y que T contiene $\delta - 1$ elementos consecutivos para algún entero δ. Entonces $d \geq \delta$.*

Definición 1.53. *Sea δ un entero tal que $2 \leq \delta \leq n$. Un código* BCH *en $\mathbb{F}_q$ de longitud n y distancia asignada δ se define como un código cíclico con conjunto representativo $T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$, siendo C_i la clase ciclotómica módulo n que contiene a i. Además, la cota de* BCH *nos dice que este código tiene distancia mínima δ.*

Ejemplo 1.54. Si queremos construirnos un código definido en $\mathbb{F}_2$ con distancia $d(\mathcal{C}) \geq 7$, por la Cota de BCH (Teorema 1.52) buscamos que $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ esté contenido en $\mathrm{Z}(\mathcal{C})$. Definimos el polinomio $g(x) = m_1(x)m_3(x)m_5(x)$, siendo $m_1(x)$, $m_3(x)$ y $m_5(x)$ los polinomios mínimos que aparecen en el Ejemplo 1.47, de tal manera que $\mathcal{C} = \langle g(x) \rangle$ verifica que $d(\mathcal{C}) \geq 7$.

1.5. Restricción de códigos a otro subcuerpo

En esta sección nos concentraremos en una técnica que resulta de escribir el cuerpo finito $\mathbb{F}_{q^m}$ como espacio vectorial de su subcuerpo $\mathbb{F}_q$. Esto nos permite conseguir un código con la misma longitud n que el inicial pero con mayor distancia mínima. La técnica comienza con códigos lineales en $\mathbb{F}_{q^m}$ y terminaremos con códigos lineales en $\mathbb{F}_q$.

Definición 1.55. *Sean $\mathcal{D}$ un código definido en $\mathbb{F}_q$ y $\mathcal{C}$ un código definido en $\mathbb{F}_{q^m}$, ambos lineales y de longitud n. Si $\mathcal{D} = \mathcal{C} \cap \mathbb{F}_q^n$, entonces $\mathcal{D}$ se denomina la restricción (por escalares) de $\mathcal{C}$ y se denota por $\mathcal{C}|_{\mathbb{F}_q}$.*

Lema 1.56. *Sean $\mathbf{h_1}, \mathbf{h_2}, \ldots, \mathbf{h_n} \in \mathbb{F}_{q^m}$ y $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial. Existen elementos únicos h_{ij} de $\mathbb{F}_q$ tales que:*

$$\mathbf{h_j} = \sum_{i=1}^{m} h_{ij}\alpha_i \in \mathbb{F}_{q^m}.$$

Además, para todo $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$,

$$\sum_{j=1}^{n} \mathbf{h_j} x_j = 0 \in \mathbb{F}_{q^m} \Leftrightarrow \sum_{j=1}^{n} h_{ij} x_j = 0 \in \mathbb{F}_q, \quad \forall i = 1, 2, \ldots, m.$$

Demostración. Supongamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ es una base de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial. De esto se deduce la existencia y unicidad de los $h_{ij} \in \mathbb{F}_q$.

Sea $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. Se sigue que:

$$\sum_{j=1}^{n} \mathbf{h_j} x_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} h_{ij}\alpha_i \right) x_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} h_{ij} x_j \right) \alpha_i.$$

Recordemos que los α_i forman una base de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial y que los x_j son elementos de $\mathbb{F}_q$. Esto nos dice que $\sum_{i=1}^{m} h_{ij}\alpha_i \in \mathbb{F}_q$, de donde se deduce el resultado. ■

Proposición 1.57. *Sea $E = (\mathbf{h_1}, \mathbf{h_2}, \ldots, \mathbf{h_n}) \in \mathbb{F}_{q^m}^{1\times n}$ una matriz de paridad de un código lineal $\mathcal{C}$ con parámetros $[n, n-1]_{q^m}$. Supongamos que el rango de la matriz $H = (h_{ij}) \in \mathbb{F}_q^{m\times n}$, cuyos elementos h_{ij} vienen definidos por el Lema 1.56 es l. Entonces la dimensión del código restringido $\mathcal{C}|_{\mathbb{F}_q}$ es igual a $n-l$.*

Demostración. Sea $H = (h_{ij}) \in \mathbb{F}_q^{m\times n}$ una matriz de rango l tal que sus columnas $(h_{1j}, h_{2j}, \ldots, h_{mj})$ son las coordenadas de $\mathbf{h_j}$ con respecto de una base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial. Por el Lema 1.56, el código $\mathcal{C}|_{\mathbb{F}_q}$ verifica que $H\mathbf{c}^\top = 0$, para todo $\mathbf{c} \in \mathcal{C}|_{\mathbb{F}_q}$, por lo que se concluye que $\dim(\mathcal{C}) = n - l$. ■

Ejemplo 1.58. Sea $\mathbb{F}_9 \cong {}^{\mathbb{F}_3[x]}\!/_{(x^2+x+2)}$ un cuerpo finito y sea $\alpha \in \mathbb{F}_9$ cualquier elemento primitivo tal que α es una raíz de x^2+x+2. Esto nos dice que $\langle\alpha\rangle = \mathbb{F}_9^*$, donde $\mathbb{F}_9^*$ denota el cuerpo de las unidades de $\mathbb{F}_9$. Es fácil comprobar que $\{1, \alpha\}$ es una base de $\mathbb{F}_9$ como $\mathbb{F}_3$-espacio vectorial. Consideremos la matriz de paridad

$$E = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{pmatrix} \in \mathbb{F}_9^{1\times 8}$$

del código lineal $\mathcal{C}$ en $\mathbb{F}_9$. Entonces, de acuerdo al Lema 1.56, el código $\mathcal{C}|_{\mathbb{F}_3}$ es el núcleo de la siguiente matriz:

$$H = \begin{pmatrix} 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \end{pmatrix} \in \mathbb{F}_3^{2\times 8}.$$

Para obtener las columnas de H hay que calcular las coordenadas de cada elemento de E respeco de la base $\{1, \alpha\}$. Por ejemplo, $\alpha^3 = 2 + 2\alpha$, por lo que α^3 tiene coordenadas $(2, 2)$ con respecto de la base elegida y su vector transpuesto corresponde con la cuarta columna de H. Además, obsérvese que el rango de H es dos, por lo que la dimensión de $\mathcal{C}|_{\mathbb{F}_3}$ es $6 = n - \operatorname{rank}(H)$.

Proposición 1.59. *Sea $\mathcal{D}$ un código lineal en $\mathbb{F}_q$ de longitud n y dimensión k. Sea $m = n-k$; si $k < n$ entonces $\mathcal{D}$ es la restricción de un código $\mathcal{C}$ en $\mathbb{F}_{q^m}$ con dimensión $\dim(\mathcal{C}) = \dim(\mathcal{D}) - 1$.*

Demostración. Sea $H = (h_{ij}) \in \mathbb{F}_q^{m\times n}$, con $m = n-k$, una matriz de paridad del código $\mathcal{D}$ en $\mathbb{F}_q$ (nótese que $m > 0$ al ser $k < n$). Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base de $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espacio vectorial. Definimos:

$$\mathbf{h_j} = \sum_{i=1}^{m} h_{ij}\alpha_i \in \mathbb{F}_{q^m}, \quad \text{para cada } j = 1, 2, \ldots, n.$$

Así, podemos construir la matriz de paridad $E = (\mathbf{h_1}, \mathbf{h_2}, \ldots, \mathbf{h_n}) \in \mathbb{F}_{q^m}^{1\times n}$ del código lineal $\mathcal{C}$ en $\mathbb{F}_{q^m}$. Ahora, como hemos supuesto $k < n$, E no puede corresponder al vector nulo. Por tanto, $\mathcal{C}$ tiene $\dim(\mathcal{D}) - 1$ y, por la Proposición 1.57, se concluye que $\mathcal{D}$ es la restricción de $\mathcal{C}$. ■

Proposición 1.60. *Sea $\mathcal{C}$ un código con parámetros $[n, k, d]_{q^m}$. Entonces, la dimensión de $\mathcal{C}|_{\mathbb{F}_q}$ es $k(\mathcal{C}|_{\mathbb{F}_q}) \geq n - m(n-k)$ y su distancia mínima es $d(\mathcal{C}|_{\mathbb{F}_q}) \geq d$.*

Demostración. Ya que $\mathcal{C}|_{\mathbb{F}_q}$ es un subconjunto de $\mathcal{C}$, es claro que la distancia mínima de este tiene que ser, al menos, d.

Si E es una matriz de paridad de $\mathcal{C}$, esta consiste de $n - k$ filas (pues la dimensión del código es k). Por el Lema 1.56, cada una de estas filas nos da m ecuaciones lineales sobre $\mathbb{F}_q$. Luego, la restricción $\mathcal{C}|_{\mathbb{F}_q}$ es el espacio de soluciones de $m(n-k)$ ecuaciones lineales homogéneas sobre $\mathbb{F}_q$. Se concluye que la dimensión de $\mathcal{C}|_{\mathbb{F}_q}$ es, al menos, $n - m(n-k)$. ■

Ejemplo 1.61. Sea $\mathcal{C}$ un código $[7, 5]_8$ con matriz de paridad:

$$H = \begin{pmatrix} 1 & 0 & \beta^2 & 0 & \beta^2+\beta+1 & \beta+1 & \beta^2+\beta \\ 0 & 1 & \beta^2+\beta+1 & 1 & \beta^2+1 & \beta+1 & \beta+1 \end{pmatrix} \in \mathbb{F}_8^{2\times 7},$$

siendo $\beta \in \mathbb{F}_8$ cualquier elemento primitivo tal que β es una raíz de $x^3 + x + 1$. Esto nos dice que podemos ver el cuerpo finito $\mathbb{F}_8$ como la extensión:

$$\mathbb{F}_8 \cong \frac{\mathbb{F}_2[x]}{(x^3 + x + 1)} \cong \mathbb{F}_2[\beta],$$

con $\{1, \beta, \beta^2\}$ una base de $\mathbb{F}_2[\beta]$. Se tiene entonces la siguiente matriz de paridad $\hat{H}$ para el código $\mathcal{C}|_{\mathbb{F}_2}$:

$$\hat{H} = \begin{pmatrix} 1&0&0&0&1&1&0 \\ 0&0&0&0&1&1&1 \\ 0&0&1&0&1&0&1 \\ 0&1&1&1&1&1&1 \\ 0&0&1&0&0&1&1 \\ 0&0&1&0&1&0&0 \end{pmatrix} \in \mathbb{F}_2^{6\times 7}.$$

Obsérve que tanto $\mathcal{C}$ como $\mathcal{C}|_{\mathbb{F}_2}$ son códigos de distancia mínima 2 al estar sus matrices de paridad H y $\hat{H}$ compuestas por columnas no nulas con dos de ellas linealmente dependientes (Observación 1.16). Pero $\dim(\mathcal{C}) = 2$, mientras que $\dim(\mathcal{C}|_{\mathbb{F}_2}) = n - \operatorname{rank}(H) = 7 - 5 = 2 \geq n - m(n-k) = 7 - 3 \cdot (7-5) = 1$.

Definición 1.62. *La aplicación traza $\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ viene definida por*

$$\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x) = x + x^q + \cdots + x^{q^{m-1}}, \quad x \in \mathbb{F}_{q^m}.$$

En caso de que no haya dudas, la aplicación se escribirá simplemente como Tr.

Observación 1.63. La *aplicación traza* se extiende de manera natural (coordenada a coordenada) a la aplicación $\mathrm{Tr}\colon \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^n$. Además, las aplicaciones $\mathrm{Tr}\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ y $\mathrm{Tr}\colon \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^n$ son sobreyectivas y lineales en $\mathbb{F}_q$.

En efecto, probemos que $\mathrm{Tr}\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ es una aplicación lineal en $\mathbb{F}_q$; esto es,

$$\mathrm{Tr}(\alpha x + y) = \alpha \mathrm{Tr}(x) + \mathrm{Tr}(y), \quad x, y \in \mathbb{F}_{q^m},\ \alpha \in \mathbb{F}_q.$$

Sean $x, y \in \mathbb{F}_{q^m}$ y $\alpha \in \mathbb{F}_q$. Se tiene que:

$$\mathrm{Tr}(\alpha x + y) = (\alpha x + y) + (\alpha x + y)^q + \cdots + (\alpha x + y)^{q^{m-1}} \in \mathbb{F}_q.$$

Recordemos que, según la Observación 1.30, si $a, b \in \mathbb{F}_q$ entonces $a^q = a$ y $(a+b)^q = a^q + b^q$. Se sigue que:

$$\begin{aligned}
\mathrm{Tr}(\alpha x + y) &= \alpha x + y + (\alpha x)^q + y^q + \cdots + (\alpha x)^{q^{m-1}} + y^{q^{m-1}} \\
&= \alpha x + \alpha^q x^q + \cdots + \alpha^{q^{m-1}} x^{q^{m-1}} + y + y^q + \cdots + y^{q^{m-1}} \\
&= \alpha x + \alpha x^q + \cdots + \alpha x^{q^{m-1}} + y + y^q + y^{q^{m-1}} \\
&= \alpha(x + x^q + \cdots + x^{q^{m-1}}) + (y + y^q + \cdots + y^{q^{m-1}}) \\
&= \alpha \mathrm{Tr}(x) + \mathrm{Tr}(y) \in \mathbb{F}_q.
\end{aligned}$$

Hemos probado que:

$$\mathrm{Tr}(\alpha x + y) = \alpha \mathrm{Tr}(x) + \mathrm{Tr}(y), \quad x, y \in \mathbb{F}_{q^m},\ \alpha \in \mathbb{F}_q.$$

Veamos ahora que la aplicación $\mathrm{Tr}\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ es sobreyectiva. Esto significa que: $\forall y \in \mathbb{F}_q\ \exists x \in \mathbb{F}_{q^m}\colon \mathrm{Tr}(x) = y$. En efecto, nótese que Tr es una aplicación lineal en $\mathbb{F}_q$ y que $\mathbb{F}_{q^m}$ es una extensión de cuerpo finita de $\mathbb{F}_q$. Esto nos dice que es suficiente probar que existe al menos un elemento x en $\mathbb{F}_{q^m}$ tal que $\mathrm{Tr}(x) \neq 0$ para que la aplicación sea sobreyectiva (ya que $\mathrm{Tr}(\alpha x) = \alpha \mathrm{Tr}(x)$, $\alpha \in \mathbb{F}_q$). Sea $x \in \mathbb{F}_{q^m}$. Como $\mathrm{Tr}(x)$ es un polinomio de grado q^{m-1} sabemos que no puede tener más de q^{m-1} raíces en $\mathbb{F}_{q^m}$. Pero $|\mathbb{F}_{q^m}| = q^m$, es decir, la aplicación Tr es no nula. Se concluye así la sobreyectividad de la aplicación $\mathrm{Tr}\colon \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^n$.

Definición 1.64. *Sea $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ un código lineal en $\mathbb{F}_{q^m}$. Se denomina código traza de $\mathcal{C}$ al conjunto* $\mathrm{Tr}(\mathcal{C}) \coloneqq \{\, \mathrm{Tr}(c) \in \mathbb{F}_q \mid c \in \mathcal{C} \,\} \subseteq \mathbb{F}_q^n$.

Observación 1.65. Nótese que las restricciones de códigos a su subcuerpo $\mathbb{F}_q$ y los códigos traza de un código $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ son códigos en $\mathbb{F}_q$ de longitud n.

Ejemplo 1.66. Sean $\mathbb{F}_8 \cong \mathbb{F}_2[\alpha]$, con $\alpha \in \mathbb{F}_8$ una raíz del polinomio $x^3 + x + 1 \in \mathbb{F}_2[x]$, y $\mathcal{C}$ el código con matriz generatriz $G = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}$. La aplicación Traza $\mathrm{Tr}\colon \mathbb{F}_8 \longrightarrow \mathbb{F}_2$ se define como $\mathrm{Tr}(\beta) = \beta + \beta^2 + \beta^4$, con $\beta \in \mathbb{F}_8$. Se comprueba que: $\mathrm{Tr}(\alpha^i) = 1$, para $i \in \{0, 3, 5, 6\}$ y $\mathrm{Tr}(\alpha^i) = 0$ con $i \in \{1, 2, 4\}$.

El código $\mathcal{C}$ está compuesto por siete vectores que corresponden a todas las permutaciones cíclicas del vector $(1, \alpha, \alpha^2, \ldots, \alpha^6)$, además del elemento neutro $\mathbf{0}$. Por lo tanto, el código $\mathrm{Tr}(\mathcal{C}) \coloneqq \{\, \mathrm{Tr}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \,\}$ definido en $\mathbb{F}_2$, está formado por $\mathrm{Tr}(\mathbf{0}) = 0$ y por las permutaciones cíclicas de $\mathrm{Tr}(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6) = (1, 0, 0, 1, 0, 1, 1)$.

Teorema 1.67 (Dualidad de Delsarte). *Sea $\mathcal{C}$ un código lineal en $\mathbb{F}_{q^m}$. Entonces, $\mathcal{C} \cap \mathbb{F}_q^n = (\mathrm{Tr}(\mathcal{C}^\perp))^\perp$.*

Demostración. Sean $\mathbf{x} \in \mathcal{C} \cap \mathbb{F}_q^n$ e $\mathbf{y} \in \mathrm{Tr}(\mathcal{C}^\perp)$. Existe $\mathbf{z} \in \mathcal{C}^\perp$ tal que $\mathbf{y} = \mathrm{Tr}(\mathbf{z})$. Como $\mathbf{x} \in \mathcal{C}$ es claro que $\mathbf{x} \cdot \mathbf{z} = 0$. También, por ser $\mathbf{x} \in \mathbb{F}_q^n$ y Tr una aplicación lineal, se tiene que $\mathbf{x} \cdot \mathrm{Tr}(\mathbf{z}) = \mathrm{Tr}(\mathbf{x} \cdot \mathbf{z}) = 0$. De esta forma, obtenemos que $\mathbf{x} \cdot \mathbf{y} = 0$, es decir, que $\mathcal{C} \cap \mathbb{F}_q^n$ es un subespacio de $(\mathrm{Tr}(\mathcal{C}^\perp))^\perp$.

Supongamos ahora que no se verifica la igualdad. Entonces existirá $\mathbf{x} \in (\mathrm{Tr}(\mathcal{C}^\perp))^\perp$ tal que $\mathbf{x} \notin \mathcal{C}$ (basta tener en cuenta que $(\mathrm{Tr}(\mathcal{C}^\perp))^\perp \subseteq \mathbb{F}_q^n$). Luego, existirá $\mathbf{y} \in \mathcal{C}^\perp$ tal que $\mathbf{x} \cdot \mathbf{y} \neq 0$. Recordemos que la aplicación traza es sobreyectiva, lo que nos dice que hay un $\alpha \in \mathbb{F}_{q^m}$ tal que $\mathrm{Tr}(\alpha(\mathbf{x} \cdot \mathbf{y})) \neq 0$ y, por tanto, $\mathbf{x} \cdot \mathrm{Tr}(\alpha \mathbf{y}) = \mathrm{Tr}(\mathbf{x} \cdot \alpha \mathbf{y}) = \mathrm{Tr}(\alpha(\mathbf{x} \cdot \mathbf{y})) \neq 0$. Esto contradice que $\mathbf{x} \cdot \mathrm{Tr}(\alpha \mathbf{y}) = 0$, ya que $\mathbf{x} \in (\mathrm{Tr}(\mathcal{C}^\perp))^\perp$. Probamos así que $\mathcal{C} \cap \mathbb{F}_q^n = (\mathrm{Tr}(\mathcal{C}^\perp))^\perp$. ■

Lema 1.68. *Sea $\mathcal{C}$ un código de longitud n en $\mathbb{F}_{q^m}$. Se tiene que:*

$$n - m(n - \dim(\mathcal{C})) \leq \dim(\mathcal{C}|_{F_q}) \leq \dim(\mathcal{C}),$$

$$\dim(\mathcal{C}) \leq \dim(\mathrm{Tr}(\mathcal{C})) \leq m \cdot \dim(\mathcal{C}),$$

son cotas inferiores para la dimensión de una restricción de un código a su subcuerpo $\mathbb{F}_q$ y de un código traza, respectivamente.

Demostración. Sea $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ un código lineal en $\mathbb{F}_{q^m}$. Es claro que:

$$\dim(\mathcal{C}|_{\mathbb{F}_q}) \leq \dim(\mathcal{C}) \quad \text{y} \quad \dim(\mathrm{Tr}(\mathcal{C})) \leq m \cdot \dim(\mathcal{C})$$

son cotas superiores para la dimensión de una restricción de un código a su subcuerpo $\mathbb{F}_q$ y de un código traza, respectivamente. En efecto, para ver la primera de las cotas basta tener en cuenta que una base de $\mathcal{C}|_{\mathbb{F}_q}$ en $\mathbb{F}_q$ es también linealmente independiente en $\mathbb{F}_{q^m}$. La segunda cota se sigue del hecho de que la aplicación $\mathrm{Tr}\colon\ \mathcal{C} \longrightarrow \mathrm{Tr}(\mathcal{C})$ es sobreyectiva y lineal en $\mathbb{F}_q$, y de que podemos ver $\mathcal{C}$ como un $\mathbb{F}_q$-espacio vectorial.

Por otro lado, de la Prop. 1.60 tenemos que $\dim(\mathcal{C}|_{F_q}) \geq n - m(n - \dim(\mathcal{C}))$, mientras que de la Dualidad de Delsarte (Teorema 1.67) se sigue que:

$$\dim(\mathrm{Tr}(\mathcal{C})) = \dim((\mathcal{C}^\perp\big|_{\mathbb{F}_q})^\perp) = n - \dim(\mathcal{C}^\perp\big|_{\mathbb{F}_q}) \geq n - \dim(\mathcal{C}^\perp) = \dim(\mathcal{C}).$$

2

Códigos de evaluación de polinomios

Los códigos de evaluación son una familia de códigos definidos a partir de la evaluación de polinomios. En este capítulo vamos a trabajar con códigos de evaluación, en particular los conocidos como códigos Reed-Solomon y sus generalizaciones y los códigos Reed-Muller. Estos códigos tienen interesantes propiedades y aplicaciones en diferentes áreas como la criptografía tal y como se comenta en la introducción del trabajo.

2.1. Códigos de Reed-Solomon

S. Reed y G. Solomon introdujeron la familia de códigos Reed-Solomon en 1960 [18]. Son muy utilizados en dispositivos como CDs, DVDs, Blu-Ray, DSL, WiMAX o RAID. Aunque la estructura de los códigos Reed-Solomon es bien conocida, el problema de diseñar algoritmos de decodificación eficientes para esta familia de códigos sigue siendo un área activa en investigación.

Tras el descubrimiento de los códigos *Reed-Solomon (RS)* empezó un nuevo campo de investigación para intentar encontrar algoritmos de decodificación eficientes. Tal y como veremos en este capítulo, los códigos Reed-Solomon en el sentido estricto pueden verse como códigos cíclicos, por lo tanto algoritmos de decodificación específicos para códigos cíclicos y códigos BCH pueden ser utilizados para esta familia. Ejemplos de estos algoritmos específicos para códigos cíclicos son el algoritmo de Peterson [15] presentado en 1960, luego mejorado por Gorenstein y Zierler [5], y el algoritmo de Berlekamp [1] presentado en 1968 y simplificado más tarde por Massey [10]. Ambos algoritmos: Peterson-Gorenstein-Zierler y Berlekamp-Massey son algoritmos de decodificación eficientes (tienen una complejidad polinomial en ambos casos). En 1997 Sudan [22] desarrolló un algoritmo específico para códigos Reed-Solomon, que mejora la capacidad de corrección de los algoritmos anteriores y su eficacia. Una versión mejorada fue

presentada en 1999 por Sudan y Guruswami [6] y más tarde en 2003 por Koetter y Vardy [9].

Estudiamos los códigos Reed-Solomon como un caso especial de códigos cíclicos definidos en el cuerpo finito $\mathbb{F}_q$ y más tarde los estudiaremos, utilizando una definición equivalente, como códigos de evaluación de polinomios en una variable. Además, veremos que los códigos RS en $\mathbb{F}_q$ son códigos MDS; aunque también se dará una prueba alternativa en la siguiente sección al estudiar sus generalizaciones.

Definición 2.1. *Sea α un elemento primitivo de $\mathbb{F}_q$. Sean b y k dos enteros no negativos tales que $0 \leq b, k \leq n = q-1$. Se define el código Reed-Solomon de dimensión k, denotado por $\mathrm{RS}_k(n,b)$, como el código cíclico con polinomio generador $g_{b,k}(x)$, donde: $g_{b,k}(x) = (x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+n-k-1})$.*

Proposición 2.2. *El código $\mathrm{RS}_k(n,b)$ en $\mathbb{F}_q$ es un código* MDS *y tiene por conjunto de ceros $\mathrm{Z}(\mathcal{C}) = \{\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+n-k-1}\}$, con $b \in \mathbb{Z}$ no negativo.*

Demostración. Sea $\mathcal{C} = \mathrm{RS}_k(n,b)$ un código de dimensión k y de longitud $n = q-1$, con polinomio generador:

$$g_{b,k}(x) = (x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+n-k-1}),$$

siendo $\alpha \in \mathbb{F}_q$ un elemento primitivo. Como n es el menor entero positivo tal que $q^n \equiv 1 \mod n$, el polinomio $x^n - 1$ se descompone en factores lineales en $\mathbb{F}_q$ y todas las clases ciclotómicas módulo n tienen un único elemento; por lo que el conjunto representativo es de tamaño $|T| = n-k$, con $n-k$ elementos consecutivos, siendo $T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+n-k-1}$, para algún $b \in \mathbb{Z}$. Por la cota de BCH (Teorema 1.52) se tiene que la distancia mínima es al menos $n-k+1$ y por la cota de Singleton (Teorema 1.21) se sigue que la distancia mínima es a lo sumo $n-k+1$; esto es, $\mathrm{RS}_k(n,b)$ es un código MDS de distancia mínima $d = n-k+1$. Además, el conjunto de ceros de $\mathcal{C}$ se escribe:

$$\mathrm{Z}(\mathcal{C}) = \{\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+n-k-1}\}.$$

■

Definición 2.3. *Sean α un elemento primitivo de $\mathbb{F}_q$ y k un entero no negativo con $0 \leq k \leq n = q-1$. Sea $\mathrm{ev}(f(x)) \coloneqq (f(1), f(\alpha), \ldots, f(\alpha^{n-1}))$ la evaluación de $f(x) \in \mathbb{F}_q[x]$ en α. Entonces,*

$$\mathrm{RS}_k(n,b) \coloneqq \{\, \mathrm{ev}(x^{n-b+1} f(x)) \mid f(x) \in \mathbb{F}_q[x],\ \deg(f(x)) < k \,\}.$$

Observación 2.4. En [16, Proposición 5.1.5] se demuestra que ambas definiciones son equivalentes.

2.2. Códigos de Reed-Solomon Generalizados

Pasamos ahora al estudio de una familia más general: los códigos *Reed-Solomon generalizados (GRS)*. Estudiaremos en detalle sus propiedades básicas y su estructura.

Definición 2.5. *Denotamos el conjunto de polinomios en* $\mathbb{F}_q[x]$ *con grado menor que* k *como:* $\mathrm{L}_k \coloneqq \{\, f(x) \in \mathbb{F}_q[x] \mid deg(f(x)) < k \,\}$. *Sea* $a \in \mathbb{F}_q$. *Definimos la aplicación evaluación de* f *en* a*:* $\mathrm{ev}_{k,a}\colon \mathrm{L}_k \longrightarrow \mathbb{F}_q$, *que viene dada por* $\mathrm{ev}_{k,a}(f(x)) = f(a)$. *Además, si* $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ *es una n-tupla, la aplicación evaluación* $\mathrm{ev}_{k,\mathbf{a}}\colon \mathrm{L}_k \longrightarrow \mathbb{F}_q^n$ *se extiende de manera natural como*

$$\mathrm{ev}_{k,\mathbf{a}}(f(x)) = (\mathrm{ev}_{k,a_1}(f(x)), \mathrm{ev}_{k,a_2}(f(x)), \ldots, \mathrm{ev}_{k,a_n}(f(x))).$$

Observación 2.6. La aplicación evaluación es lineal. En efecto, si α es una constante de $\mathbb{F}_q$ y $f(x), g(x) \in \mathrm{L}_k$, entonces $\alpha f(x) + g(x)$ también está en L_k, y

$$\begin{aligned}\mathrm{ev}_{k,a}(\alpha f(x) + g(x)) &= \mathrm{ev}(\alpha f + g) = (\alpha f + g)(a) = \alpha f(a) + g(a) \\ &= \alpha \mathrm{ev}_{k,a}(f(x)) + \mathrm{ev}_{k,a}(g(x)).\end{aligned}$$

Nótese que la aplicación $\mathrm{ev}_{k,a}$ no depende de k pero sí depende de si $a \in \mathbb{F}_q$.

Definición 2.7. *Sea* n *un entero arbitrario tal que* $1 \leq n \leq q$. *Sean* $\mathbf{a} \in \mathbb{F}_q^n$ *un vector de* n *elementos de* $\mathbb{F}_q$ *distintos dos a dos y* $\mathbf{b} \in \mathbb{F}_q^n$ *un vector de* n *elementos no nulos de* $\mathbb{F}_q$. *Sea* k *un entero arbitrario tal que* $0 \leq k \leq n$. *Se define el código Reed-Solomon generalizado de dimensión* k *asociado a los vectores* $\mathbf{a}$ *y* $\mathbf{b}$ *de* $\mathbb{F}_q^n$ *como:*

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) \coloneqq \{\, \mathrm{ev}_{k,\mathbf{a}}(f(x)) * \mathbf{b} \mid f(x) \in \mathrm{L}_k \,\},$$

donde el producto estrella $*$ *de dos vectores* $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ *se define como la multiplicación coordenada a coordenada; es decir,*

$$\mathbf{a} * \mathbf{b} \coloneqq (a_1 b_1, a_2 b_2, \ldots, a_n b_n), \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

Observación 2.8. En particular, un código $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ definido en $\mathbb{F}_q$ es un código RS en sentido estricto si la longitud del código es $n = q - 1$ y se toma por vectores $\mathbf{a} = \{1, \alpha, \ldots, \alpha^{q-2}\} \in \mathbb{F}_q^*$, con $\alpha \in \mathbb{F}_q^*$ un elemento primitivo, y $\mathbf{b} = (1, 1, \ldots, 1) \in \mathbb{F}_q^n$.

Sea $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$. Como el conjunto $\mathcal{B} = \{1, x, \ldots, x^{k-1}\} \subseteq \mathrm{L}_k$ forma una base de L_k, podemos construir una matriz generatriz de un código $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ evaluando los monomios de la base $\mathcal{B}$ en $\mathbf{a}$ y escalando por $\mathbf{b}$; esto es, los elementos de G se escriben de la forma $(g_{ij}) = (a_j^{i-1} b_j)$, para $i = 1, 2, \ldots, k$, j= $1, 2, \ldots, n$.

$$G = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ b_1 a_1 & b_2 a_2 & \cdots & b_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \cdots & b_n a_n^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n}.$$

Ejemplo 2.9. Sean $\mathbf{a} = \{0, 1, 2, 3, 4, 5, 6\} \in \mathbb{F}_7^7$ y $\mathbf{b} \in \mathbb{F}_7^7$ el vector cuyas coordenadas valen todas uno. Entonces, una matriz generatriz para el código $\mathrm{GRS}_4(\mathbf{a}, \mathbf{b})$ se escribe como:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 0 & 1 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \\ 0 & 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix} \in \mathbb{F}_7^{4 \times 7}.$$

Nótese que esta es la matriz generatriz de un código lineal $[7, 4, 4]_7$ que ya habíamos visto en el Ejemplo 1.12 y se trataba de un código MDS. Con el siguiente resultado veremos que un código GRS es siempre MDS.

Proposición 2.10. *Sea* $0 \leq k \leq n \leq q$. *El código* $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ *es un código* MDS *lineal con parámetros* $[n, k, n-k+1]_q$.

Demostración. Un código lineal $\mathcal{C}$ mantiene la linealidad a través de la aplicación $\mathbf{c} \mapsto \mathbf{b} * \mathbf{c} = (b_1 c_1, b_2 c_2, \ldots, b_n c_n) \in \mathbb{F}_q^n$, con $\mathbf{b} \in \mathbb{F}_q^n$, y se conservan también los parámetros si $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ tiene todas sus componentes no nulas. Supongamos, sin pérdida de generalidad, que $\mathbf{b} = \mathbf{1} = (1, 1, \overset{(n)}{\ldots}, 1)$ y consideremos la aplicación evaluación

$$\mathrm{ev}_{k,a} \colon \mathrm{L}_k \longrightarrow \mathbb{F}_q^n$$

definida como $\mathrm{ev}_{k,\mathbf{a}}(f(x)) = (f(a_1), f(a_2), \ldots, f(a_n))$. Es claro que esta aplicación es lineal (2.6) y que L_k es un subespacio vectorial de dimensión k. Más aún, $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ es la imagen de L_k a través de esta aplicación: $\mathrm{ev}_{k,\mathbf{a}}(\mathrm{L}_k) = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$.

Supongamos que $\mathbf{a} \in \mathbb{F}_q^n$ es una n-tupla con todos sus elementos distintos dos a dos. Sea $f(x) \in \mathrm{L}_k$ y $\mathrm{ev}_{k,\mathbf{a}}(f(x)) = 0$. De esta manera tenemos que $\deg(f) < k$ y que f tiene n ceros con $k < n$, por lo que f es, necesariamente, el polinomio nulo. Esto nos dice que la aplicación anterior es inyectiva y que $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ tiene la misma dimensión que L_k.

Probamos ahora que la distancia mínima del código es $d = n - k + 1$. Sea $\mathbf{c} \in \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ una palabra de código no nula con peso $\mathrm{w_H}(\mathbf{c}) = d$. Entonces, existe un polinomio no nulo $f(x) \in \mathrm{L}_k$ tal que $\mathrm{ev}_{k,\mathbf{a}}(f(x)) = \mathbf{c}$. Sabemos que los ceros de $f(x)$ se corresponden con las coordenadas nulas de $\mathbf{c}$, es decir, el número de ceros de $f(x)$ entre las componentes de $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ es igual al número de ceros en las coordenadas de $\mathbf{c}$; esto es, $n - d$. Se sigue que,

$$n - d \leq deg(f(x)) < k, \text{ es decir, } \; d \geq n - k + 1,$$

y se alcanza la igualdad gracias a la cota de Singleton (Teorema 1.21) para códigos lineales. Así, por definición, el código $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ se dice que es un código MDS. ■

Observación 2.11. Otra manera de realizar la demostración es considerar el polinomio $h(x) = \prod_{i=1}^{k-1}(x - a_i) \in \mathrm{L}_k$, que produce una palabra $\mathbf{c} = \mathrm{ev}_{k,\mathbf{a}}(h)$ con peso $\mathrm{w_H}(\mathbf{c}) = n - k + 1$.

Proposición 2.12. *Sean k y l dos enteros positivos tales que $k+l \leq n$. Entonces*

$$\langle \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) * \mathrm{GRS}_l(\mathbf{a}, \mathbf{c}) \rangle = \mathrm{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c}) \rangle.$$

Demostración. Si $f(x) \in \mathrm{L}_k$ y $g(x) \in \mathrm{L}_l$, entonces $h(x) = f(x)g(x) \in \mathrm{L}_{k+l-1}$, siendo $h(a) = f(a)g(a)$, para todo $a \in \mathbb{F}_q$. Por lo tanto, se tiene que:

$$\mathrm{ev}_{k+l-1,a}(f(x)g(x)) = \mathrm{ev}_{k,a}(f(x)) * \mathrm{ev}_{l,a}(g(x)).$$

Esto nos dice que:

$$(\mathrm{ev}_{k,\mathbf{a}}(f(x)) * \mathbf{b}) * (\mathrm{ev}_{l,\mathbf{a}}(g(x)) * \mathbf{c}) = \mathrm{ev}_{k+l-1,\mathbf{a}}(f(x)g(x)) * \mathbf{b} * \mathbf{c},$$

con $\deg(f(x)g(x)) < k+l-1$ siempre que $\deg(f(x)) < k$ y $\deg(g(x)) < l$. Luego, hemos probado que: $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) * \mathrm{GRS}_l(\mathbf{a}, \mathbf{c}) \subseteq \mathrm{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$. En general, la igualdad no se mantiene, pero tenemos que:

$$\langle \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) * \mathrm{GRS}_l(\mathbf{a}, \mathbf{c}) \rangle = \mathrm{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c}),$$

ya que los espacios vectoriales en ambos lados de la igualdad están generados por los elementos

$$(\mathrm{ev}_{k,\mathbf{a}}(x^i) * \mathbf{b}) * (\mathrm{ev}_{l,\mathbf{a}}(x^j) * \mathbf{c}) = \mathrm{ev}_{k+l-1,\mathbf{a}}(x^{i+j}) * \mathbf{b} * \mathbf{c},$$

donde $0 \leq i < k$ y $0 \leq j < l$. ■

Por interpolación polinómica sabemos que cualquier polinomio de grado menor que k se determina únicamente por sus valores en k (o más) puntos distintos. Observamos que para cualquier palabra de código $\mathbf{c} \in \mathcal{C}$ con k coordenadas nulas esta se corresponde con un polinomio $f \in \mathbb{F}_q[x]$ con $\deg(f) < k$ tal que $f(a_i) = 0$, con $i \in I$ y $\mathrm{card}(I) = k$, por lo que este debe ser el polinomio nulo.

Dada cualquier n-tupla $\mathbf{c} \in \mathbb{F}_q^n$, podemos reconstruir el polinomio único $f(x) \in \mathbb{F}_q[x]$ de grado menor que n como $\mathbf{c} = \mathrm{ev}_{n,\mathbf{a}}(f(x))$, donde el vector $\mathbf{c}$ tiene por i-ésima coordenada $b_i f(a_i)$. Definimos los siguientes polinomios:

$$L(x) = \prod_{i=j}^{n}(x - a_i) \quad \text{y} \quad L_i(x) = \frac{L(x)}{(x - a_i)} = \prod_{i \neq j}(x - a_j),$$

siendo $L(x), L_i(x) \in \mathbb{F}_q[x]$ polinomios mónicos de grados n y $n-1$, respectivamente. Por tanto, tenemos suficiente información para calcular $f(x)$ usando la fórmula de interpolación de Lagrange:

$$f(x) = \sum_{i=1}^{n} \frac{L_i(x)}{L_i(a_i)} f(a_i) \in \mathbb{F}_q[x],$$

donde los coeficientes $L_i(a_i)$ son siempre no nulos.

Proposición 2.13. *Sea* $\mathbf{b}^\perp$ *el vector con componentes*

$$b_j^\perp = \frac{1}{b_j \prod_{i \neq j}(a_i - a_j)}, \quad \textit{para } j = 1, 2, \ldots, n.$$

Entonces $\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{b}^\perp)$ *es el código dual de* $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$.

Demostración. Tenemos que ver que $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}^\perp) = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})^\perp$. Para ello probamos que, para cada $\mathbf{c}$ de $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, $\mathbf{c} \cdot \mathbf{d} = 0$, $\forall \mathbf{d} \in \mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{b}^\perp)$, de donde el resultado es inmediato. Sean $\mathbf{c} = \mathrm{ev}_{k,\mathbf{a}}(f(x))$ y $\mathbf{d} = \mathrm{ev}_{n-k,\mathbf{a}}$. Sabemos que $f \in \mathrm{L}_k$ y que $g \in \mathrm{L}_{n-k}$. Esto nos dice que $\deg(fg) < n-1$, es decir, $fg \in \mathrm{L}_{n-1}$. Mediante interpolación de Lagrange, tenemos que:

$$f(x)g(x) = \sum_{i=1}^{n} \frac{L_i(x)}{L_i(a_i)} f(a_i)g(a_i) \in \mathbb{F}_q[x].$$

Igualando los coeficientes de x^{n-1} en la expresión anterior se obtiene:

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \frac{1}{L_i(a_i)} f(a_i)g(a_i) = \sum_{i=1}^{n} (b_i f(a_i)) \left(\frac{b_i^{-1}}{L_i(a_i)} g(a_i) \right) = \\ &= \sum_{i=1}^{n} (b_i(f(a_i))(b_i^\perp g(a_i)) = \mathbf{c}, \mathbf{d}. \end{aligned}$$

Hemos probado que $\mathbf{c} \cdot \mathbf{d} = 0$. ■

2.3. Decodificación para códigos GRS

Sea $\mathbf{y} = \mathbf{c} + \mathbf{e}$ un vector recibido con $\mathbf{c} \in \mathcal{C} = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ y $\mathbf{e}$ el error generado durante la transmisión de la palabra. Como $\mathbf{c} \in \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, sabemos que existe un polinomio $f \in \mathrm{L}_k$ tal que: $\mathbf{c} = \mathbf{b} * \mathrm{ev}_{k,\mathbf{a}}(f) = \mathbf{b} * f(\mathbf{a})$, para algún $\mathbf{b} \in \mathbb{F}_q^n$. Definimos el conjunto de índices de error (que a priori es desconocido):

$$I \coloneqq \{\, i \in \{1, 2, \ldots, n\} \mid b_i f(a_i) \neq y_i \,\} = \{i_1, i_2, \ldots, i_t\},$$

con $t < n$, y definimos también el polinomio $E(x) \coloneqq \prod_{i \in I}(x - a_i)$. Se tiene entonces que la ecuación:

$$E(x)b_i f(a_i) = E(x)y_i, \quad \forall i \in \{1, 2, \ldots, n\}$$

cumple lo siguiente: si $i \in I$ entonces $E(a_i) = 0$; si $i \notin I$ entonces $b_i f(a_i) = y_i$. Por lo tanto, la ecuación es cierta para todo $i \in \{1, 2, \ldots, n\}$.

Además, como $E(x)$ es un polinomio de grado $t = |I|$, el segundo miembro de la igualdad anterior se puede expresar como el polinomio mónico:

$$E(x)y_i = x^t + \sum_{i=0}^{t-1} A_i x^i,$$

donde se desconocen los coeficientes $A_i \in \mathbb{F}_q$, con $i = 0, 1, \ldots, t-1$. Por otra parte, en el primer miembro, tenemos un polinomio con grado $\deg(Ef) \leq \deg(E) + \deg(f) = t + k - 1$; es decir, se puede escribir como:

$$E(x)f(x) = \sum_{i=0}^{t+k-1} B_i x^i,$$

siendo otra vez desconocidos los coeficientes $B_i \in \mathbb{F}_q$. Nótese que esta igualdad de polinomios:

$$\sum_{i=0}^{t+k-1} B_i x^i = x^t + \sum_{i=0}^{t-1} A_i x^i,$$

nos proporciona un sistema de n ecuaciones lineales con $2t + k$ incógnitas, que tendrá solución no trivial si $2t + k < n$. Por tanto, como $\mathcal{C}$ es un código MDS (esto es, $d = n - k + 1$), podemos corregir t errores, siendo:

$$t \leq \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Obsérvese que este algoritmo también nos sirve para decodificar subcódigos de un código GRS; es decir, si $\mathcal{D} \subseteq \mathcal{C}$, con $\mathcal{C}$ un código GRS definido en $\mathbb{F}_q$, entonces el algoritmo antes explicado también funciona para decodificar en $\mathcal{D}$. Sin embargo, en este caso se podrá decodificar t errores siendo:

$$t \leq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \leq \left\lfloor \frac{d(\mathcal{D})-1}{2} \right\rfloor.$$

Por tanto, podrá corregir menos errores que un agoritmo específico para $\mathcal{D}$. En particular, el mismo razonamiento se aplica para cualquier restricción del código $\mathcal{C}$ a un subcuerpo de $\mathbb{F}_{q^m}$.

Nos referimos por tiempo de complejidad de un algoritmo al número de operaciones elementales que se deben realizar para obtener el resultado final.

Nótese que este algoritmo, aunque no sea el más eficiente, trabaja en tiempo polinomial, pues el proceso de decodificación se reduce a resolver un sistema de ecuaciones lineales en $\mathbb{F}_q$ por el método de Gauss, siendo el orden de complejidad de este método del orden de $\mathcal{O}(n^3)$.

2.4. Códigos Reed-Muller

Los códigos *Reed-Muller (RM)* se encuentran entre los códigos más antiguos que existen y fueron introducidos como generalización de códigos Reed-Solomon. Fueron descubiertos por E. Muller en 1954 y S. Reed [13], quienes propusieron el primer algoritmo de decodificación eficiente en [17] para estos códigos. Nos restringimos al estudio de estos códigos desde el punto de vista de códigos de evaluación de polinomios en varias variables.

Elegimos una enumeración $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ de n puntos distintos de $\mathbb{F}_q^m$, esto es, $P_i = (p_1^{(i)}, p_2^{(i)}, \ldots, p_m^{(i)}) \in \mathbb{F}_q^m$. Se define la *aplicación evaluación*

$$\mathrm{ev}_{\mathcal{P}} \colon \mathbb{F}_q[x_1, x_2, \ldots, x_m] \to \mathbb{F}_q^n$$

como $\mathrm{ev}_{\mathcal{P}}(f(x)) = (f(P_1), f(P_2), \ldots, f(P_n))$, donde $f(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

Proposición 2.14. *La aplicación evaluación* $\mathrm{ev}_{\mathcal{P}}$ *es lineal y sobreyectiva.*

Demostración. Si $m = 1$ ya hemos demostrado su linealidad en la Observación 2.6 y la sobreyectividad en la prueba de la Proposición 2.10.

Supongamos que $m > 1$. Por como se ha construido la aplicación $ev_{\mathcal{P}}$ es claro que se trata de una aplicación lineal. Consideramos, para todo $j \in \{1, 2, \ldots, n\}$, los puntos $P_i = (p_1^{(i)}, p_2^{(i)}, \ldots, p_m^{(i)}) \in \mathbb{F}_q^m$. Se define el polinomio $g_{P_j}(x)$ como

$$g_{P_j}(x) = \prod_{i=1}^{m} \prod_{\substack{b \in \mathbb{F}_q \\ b \neq p_i^j}} (x_j - b).$$

Entonces $g_{P_j}(P_i) = 0$, para todo $P_i \in \mathbb{F}_q^m$, $i \neq j$; y $g_{P_j}(P_j) \neq 0$. Definimos:

$$f_{P_j}(x) = \frac{g_{P_j}(x)}{g_{P_j}(P_j)}, \quad P_j = (p_1^{(j)}, p_2^{(j)}, \ldots, p_m^{(j)}) \in \mathbb{F}_q^m.$$

De esta manera, $f_{P_j}(P_i) = 0$, para todo $P_i \in \mathbb{F}_q^m$, $i \neq j$; pero $f_{P_j}(P_j) = 1$.

Por tanto, cualquier vector de $\mathbb{F}_q^m$ es la imagen de una combinación lineal de polinomios $f_{P_j}(x)$ bajo la aplicación $\mathrm{ev}_{\mathcal{P}}$. En efecto, para todo $b \in \mathbb{F}_q^n$, tenemos que encontrar $h \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ tal que $h(P_j) = b_j$, $j \in \{1, 2, \ldots, n\}$. Sea $x = (x_1, x_2, \ldots, x_n)$. De la construcción anterior para f_{P_j} se sigue que:

$$h(x) = b_1 f_{P_1}(x) + b_2 f_{P_2}(x) + \cdots + b_n f_{P_n}(x).$$

Esto nos dice que $h(P_j) = b_j$, para cada $P_j \in \mathbb{F}_q^m$. ∎

Observación 2.15. Nótese que $\mathrm{ev}_{\mathcal{P}}(x_i^q) = \mathrm{ev}_{\mathcal{P}}(x_i)^q = \mathrm{ev}_{\mathcal{P}}(x_i)$, para todo i. La primera igualdad viene del hecho de que la aplicación es lineal y la segunda de que estamos trabajando con elementos de $\mathbb{F}_q$.

Definición 2.16. *El núcleo de la aplicación $ev_{\mathcal{P}}$ es el ideal generado por los elementos $x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m$ en $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Denotaremos a este ideal por $\mathrm{I}_q(m)$, siendo $\mathrm{I}_q(m) \coloneqq \mathrm{Ker}(\mathrm{ev}_{\mathcal{P}}) = \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m \rangle$.*

Definición 2.17. *Sea $x^e = \prod_{i=1}^m x^{e_i}$ para $e \in \mathbb{N}^m$. Un polinomio $f(x)$ en m variables de $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ se denomina q-reducido cuando se escribe de la forma*

$$f(x) = \sum_{e \in \{0,1,\ldots,q-1\}^m} f_e x^e,$$

donde $f_e \in \mathbb{F}_q$ para todo e.

Proposición 2.18. *Sean $n = q^m$ y $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ una enumeración de todos los $n = q^m$ elementos de $\mathbb{F}_q^m$. Entonces la aplicación evaluación $\mathrm{ev}_{\mathcal{P}}$ induce un isomorfismo de espacios vectoriales:*

$$\frac{\mathbb{F}_q[x_1, x_2, \ldots, x_m]}{\mathrm{I}_q(m)} \cong \mathbb{F}_q^m.$$

Demostración. Sabemos que $ev_{\mathcal{P}}(x_i^q) = ev_{\mathcal{P}}(x_i)$, para todo i. Luego, para todo $f(x)$ de $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, existe un polinomio q-reducido que denotaremos por $\bar{f}$ de $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ tal que:

$$\mathrm{ev}_{\mathcal{P}}(f(x)) = \mathrm{ev}_{\mathcal{P}}(\bar{f}(x)) \quad \wedge \quad f(x) \equiv \bar{f}(x) \mod \mathrm{I}_q(m).$$

De esto se obtiene que la aplicación lineal $\mathrm{ev}_{\mathcal{P}}$ induce sobre $\frac{\mathbb{F}_q[x_1, x_2, \ldots, x_m]}{\mathrm{I}_q(m)}$ una aplicación bien definida. Además, esta aplicación es sobreyectiva (Proposición 2.4). Nótese que los polinomios q-reducidos en m variables se encuentran en un subespacio vectorial de $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ y dimensión $n = q^m$. Esto significa que: $\dim(\mathrm{Im}(\mathrm{ev}_{\mathcal{P}})) = n$. Se concluye que la aplicación inducida por $\mathrm{ev}_{\mathcal{P}}$ es biyectiva y, por tanto, un isomorfismo entre espacios vectoriales. ■

Definición 2.19. *Sean r, m dos enteros tales que $0 \leq r < m(q-1)$ y $n = q^m$. El código Reed-Muller $\mathrm{RM}_q(r, m)$ de orden (o grado) r en m variables se define como $\mathrm{RM}_q(r, m) \coloneqq \{\, \mathrm{ev}_{\mathcal{P}}(f) \mid f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m],\ \deg(f) \leq r \,\}$.*

Proposición 2.20. *La dimensión del código $\mathrm{RM}_q(r, m)$ es igual al cardinal de $\mathrm{E}_q(r, m) \coloneqq \{\, e \in \mathbb{N}^m \mid 0 \leq e_i \leq q-1,\ \forall i,\ \text{siendo } e_1 + e_2 + \cdots + e_m \leq r \,\}$.*

Demostración. Obsérvese que los monomios x^e, con $e \in \mathrm{E}_q(r, m)$ son q-reducidos y que sus evaluaciones $\mathrm{ev}_{\mathcal{P}}(x^e)$ forman una base del código $\mathrm{RM}_q(r, m)$. Esto es claro por la propia definición del código Reed-Muller y la proposición 2.18. ■

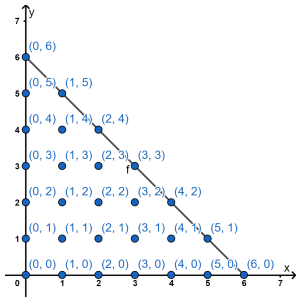
Ejemplo 2.21. Supongamos que queremos construir un código Reed-Muller definido en $\mathbb{F}_7$ de orden $r = 6$ en $m = 2$ variables. Dicho código se define como:

$$\mathrm{RM}_7(6,2) = \{\, \mathrm{ev}_{\mathcal{P}}(f) \mid f \in \mathbb{F}_7[x_1, x_2],\ \deg(f) \leq 6 \,\},$$

donde $\mathcal{P} = \{P_{ij}\}$ es una enumeración de puntos distintos de $\mathbb{F}_7^2$; esto es, $P_{ij} = (x_i, y_j)$ con $x_i, y_j \in \mathbb{F}_7$. El conjunto de monomios

$$\{\, x^i y^j \mid 0 \leq i, j \leq 6,\ i + j \leq 6 \,\}$$

conforma una base para el código $\mathrm{RM}_7(6,2)$, donde los puntos (i, j), con $0 \leq i, j \leq 6$, $i+j \leq 6$, se representan en la gráfica.



Proposición 2.22. *Sean r y s dos enteros no negativos tales que $r + s \leq m(q-1)$. Se tiene que $\langle \mathrm{RM}_q(r,m) * \mathrm{RM}_q(s,m) \rangle = \mathrm{RM}_q(r+s, m)$.*

Demostración. La demostración es muy similar a la vista en el caso de códigos GRS en la Proposición 2.12. ■

Proposición 2.23. *Sean r y m dos enteros no negativos tales que $0 \leq r < m(q-1)$ y $n = q^m$. Entonces el código $\mathrm{RM}_q(r^\perp, m)$ es el código dual de $\mathrm{RM}_q(r,m)$, siendo $r^\perp = m(q-1) - r - 1$.*

Demostración. Por la Proposición 2.22 sabemos que $\mathrm{RM}_q(r,m) * \mathrm{RM}_q(r^\perp, m) \subseteq \mathrm{RM}_q((q-1)m - 1, m)$. En particular, $\mathrm{RM}_q(r^\perp, m) \subseteq \mathrm{RM}_q((q-1)m - 1, m)$. Además, supongamos que $e \neq 0$ (en caso contrario $\mathbf{1} \cdot \mathbf{1} = q^m = 0$). Se sigue que:

$$\mathrm{ev}_{\mathcal{P}}(x^e) \cdot \mathbf{1} = \left(\sum_{Q \in \mathbb{F}_q} \mathrm{ev}_Q(x_1^{e_1}) \right) \underbrace{\left(\sum_{\mathcal{P} \in \mathbb{F}_q^{m-1}} \mathrm{ev}_{\mathcal{P}}(x_2^{e_2} \cdots x_m^{e_m}) \right)}_{H} = \left(\sum_{i=1}^{q-1} (\alpha^{e_1})^i \right) H = 0,$$

aplicando [16, Lema 4.6.2], con α es un generador de $\mathbb{F}_q^*$ y $\mathbf{1} \in \mathrm{RM}_q(r,m)$. Esto nos dice que $\mathrm{RM}_q((q-1)m-1, m) \subseteq (\mathrm{RM}_q(r,m))^\perp$. Además, $|\mathrm{E}_q((q-1)m, m)| = q^m = n$ y es fácil comprobar que el conjunto $\mathrm{E}_q(r^\perp, m)$ es igual a

$$\{\, ((q-1) - e_1, \ldots, (q-1) - e_m) \mid e \in \mathrm{E}_q((q-1)m, m) \setminus \mathrm{E}_q(r,m) \,\},$$

de donde se sigue que $\mathrm{RM}_q(r^\perp, m)$ y $(\mathrm{RM}_q(r,m))^\perp$ tienen la misma dimensión y, por tanto, son iguales. ■

3

Restricción de códigos a un subcuerpo

En este capítulo vamos a comenzar trabajando con la restricción de códigos Reed-Solomon a su subcuerpo primo. Es decir, partimos de un código $\mathcal{C}$ definido en $\mathbb{F}_q$, con $q = p^r$, perteneciente a la familia de códigos RS y estudiamos su restricción a $\mathbb{F}_p$ definida como $\mathcal{C}|_{\mathbb{F}_p} \coloneqq \mathcal{C} \cap \mathbb{F}_p^n$.

Nótese que la primera parte del trabajo se puede generalizar para estudiar $\mathcal{C}|_{\mathbb{F}_{p^s}} = \mathcal{C} \cap \mathbb{F}_{p^s}^n$, con s divisor de r; es decir, a cualquier subcuerpo de $\mathbb{F}_q$. Pero por simplificación del lenguaje trabajaremos con el subcuerpo primo, esto es, con el subcuerpo más pequeño de $\mathbb{F}_q$.

En las siguientes secciones trabajaremos con la restricción de códigos Reed-Solomon generalizados definidos en $\mathbb{F}_{q^m}$ al subcuerpo $\mathbb{F}_q$ (que, de nuevo, se podría generalizar para cualquier subucuerpo de $\mathbb{F}_{q^m}$).

3.1. Restricción de códigos Reed-Solomon a su subcuerpo primo

Esta sección está basada en el artículo [7]. Sea $\mathcal{C} \in \mathbb{F}_q^n$ un código Reed-Solomon. A lo largo de la sección supondremos siempre que $n = q-1$, con $q = p^r$ potencia de un primo p. Buscamos una base de $\mathcal{C}|_{\mathbb{F}_p}$ formada por polinomios $f \in \mathcal{R}$ con $\mathrm{ev}(f) \in \mathbb{F}_p^n$, siendo $\mathcal{R}$ el anillo cociente:

$$\mathcal{R} = \frac{\mathbb{F}_q[x]}{(x^{(q-1)} - 1)}.$$

Definimos la aplicación evaluación:

$$\mathrm{ev}\colon\ \mathcal{R} \longrightarrow \mathbb{F}_q^n,$$

que viene dada por $\mathrm{ev}(f(x)) = (f(P_1), f(P_2), \ldots, f(P_n))$, con $\{P_1, P_2, \ldots, P_n\} \subseteq (\mathbb{F}_q^*)^n$. Es claro que esta aplicación está bien definida, que es lineal en $\mathbb{F}_q$ y que,

además, define un isomorfismo. En efecto, se tiene que:

$$\begin{aligned}\ker(\mathrm{ev}) &= \{\, f(x) \in \mathcal{R} \mid \mathrm{ev}(f(x)) = 0 \,\} \\ &= \{\, f(x) \in \mathcal{R} \mid f(P_j) = 0,\ \forall j = 1, 2, \ldots, n \,\} = \{0\}.\end{aligned}$$

Proposición 3.1. *Sea f un polinomio en $\mathbb{F}_q[x]$ y sea $\mathcal{R} = \frac{\mathbb{F}_q[x]}{(x^{(q-1)}-1)}$ un anillo cociente. Entonces,*

$$\mathrm{ev}(f) \in \mathbb{F}_p^n \Leftrightarrow f(P_i) = (f(P_i))^p,\ \forall P_i \in \mathbb{F}_q^* \Leftrightarrow f^p = f \text{ en } \mathcal{R}.$$

Demostración. Recordemos que hemos definido la aplicación ev para que sea un isomorfimo. Se sigue que:

$$\begin{aligned}\mathrm{ev}(f) \in \mathbb{F}_p^n &\Leftrightarrow \mathrm{ev}(f) = (\mathrm{ev}(f))^p \Leftrightarrow \mathrm{ev}(f) = \mathrm{ev}(f^p) \\ &\Leftrightarrow \mathrm{ev}(f - f^p) = 0 \Leftrightarrow f - f^p \in \ker(\mathrm{ev}) \\ &\Leftrightarrow f^p(x) = f(x) \text{ en } \mathcal{R}.\end{aligned}$$

■

Para todo entero s con $0 \leq s \leq q-1$ se define la clase ciclotómica C_s módulo $q-1$ (respecto de q) como el conjunto

$$C_s = \{s, ps, p^2 s, \ldots, p^{n_s - 1} s\},$$

donde n_s es el menor entero positivo tal que $s \equiv sp^{n_s} \mod q-1$. Además, como se discute en la Sección 1.2, este conjunto cumple las siguientes propiedades:

(a) C_s es cerrado con la multiplicación por p.
(b) El cardinal de C_s es un divisor de r, donde $q = p^r$.
(c) Las clases C_s y $C_{s'}$ son iguales o son disjuntas, es decir, C_s particiona $\mathbb{F}_q$.

Observación 3.2. Si $\theta\colon \mathcal{R} \longrightarrow \mathcal{R}$ es un isomorfismo y $f \in \mathcal{R}$ es un polinomio tal que $\mathrm{ev}(f) \in \mathbb{F}_p^n$, entonces $\mathrm{ev}(\theta(f)) \in \mathbb{F}_p^n$ (ya que $\theta(f)^p = \theta(f^p) = \theta(f)$).

Definición 3.3. *Para todo polinomio $f(x) = \sum a_i x^i \in \mathcal{R}$ denotamos por $\mathrm{supp}(f) := \{\, i \in \mathbb{N} \mid a_i \neq 0 \,\}$ al soporte de f; es decir, $\mathrm{supp}(f)$ es el conjunto de índices i tal que el monomio x^i aparece en la descripción de f con coeficiente no nulo.*

Sea C_s la clase ciclotómica de s módulo $q-1$. Definimos $f_{C_s}(x) := \sum_{i \in C_s} x^i$ el polinomio con $\mathrm{supp}(f) = C_s$ y con todos sus coeficientes iguales a uno. Definimos $f_{C_s,\beta}$ al polinomio $f_{C_s}(\beta x)$; esto es,

$$f_{C_s,\beta} = \beta x^s + \beta^p x^{sp} + \beta^{p^2} x^{sp^2} + \cdots + \beta^{p^{n_s-1}} x^{sp^{n_s-1}}, \quad \text{donde } n_s = |C_s|.$$

Observación 3.4. Como $f_{C_s} = (f_{C_s})^p$ en $\mathcal{R}$ (pues C_s es cerrado con la multiplicación por p), por la Proposición 3.1 se tiene que $\mathrm{ev}(f_{C_s}) \in \mathbb{F}_p^n$. Sin embargo, $\mathrm{ev}(f_{C_s,\beta}) \in \mathbb{F}_p^n$ si, y solo si, β es un elemento primitivo de $\mathbb{F}_{p^{n_s}}$, con $n_s = |C_s|$.

Proposición 3.5. *Sea $f \in \mathcal{R}$ un polinomio con soporte* $\operatorname{supp}(f) = C_s$ *y* $n_s = |C_s|$ *tal que* $\operatorname{ev}(f) \in \mathbb{F}_p$. *Entonces f es una combinación lineal de los polinomios $f_{C_s}, f_{C_s,\beta}, \ldots, f_{C_s,\beta^{n_s-1}}$, con β un elemento primitivo de $\mathbb{F}_{p^{n_s}}$.*

Demostración. Por hipótesis sabemos que $\operatorname{supp}(f) = C_s$; luego,

$$f = a_1 x^s + a_2^p x^{sp} + \cdots + a_{n_s}^{p^{n_s-1}} x^{sp^{n_s-1}},$$

con $a_1, a_2, \ldots, a_{n_s} \in \mathbb{F}_q$. Además, se tiene que (por la Observación 1.30):

$$f^p = a_1^p x^{sp} + a_2^{p^2} x^{sp^2} + \cdots + a_{n_s}^{p^{n_s}} x^{sp^{n_s}}.$$

Por hipótesis, $\operatorname{ev}(f) \in \mathbb{F}_p^n$; luego, utilizando la Proposición 3.1 que nos dice que $f = f^p$ en $\mathcal{R}$, se sigue que $a_{i+1} = a_i^p$ $(i = 1, \ldots, n_s - 1)$ y $a_{n_s} = a_1$. Luego, podemos escribir f como:

$$f = \alpha x^s + \alpha^p x^{sp} + \cdots + \alpha^{p^{n_s-1}} x^{sp^{n_s-1}}.$$

Además, $\alpha^{p^{n_s}} = \alpha$, por lo que $\alpha \in \mathbb{F}_{p^{n_s}}$. (Recordemos que $n_s = |C_s|$ es un divisor de r con $q = p^r$ y, por lo tanto, $\mathbb{F}_{p^{n_s}} \subseteq \mathbb{F}_q$.)

Sea $\beta \in \mathbb{F}_{p^{n_s}}$ un elemento primitivo de $\mathbb{F}_{p^{n_s}}$; es decir, el conjunto $\{1, \beta, \ldots, \beta^{n_s-1}\}$ es una base de $\mathbb{F}_{p^{n_s}}$ como espacio vectorial de $\mathbb{F}_p$. Por tanto, podemos escribir α como una combinación lineal de estos elementos:

$$\alpha = a_0 + a_1\beta + \cdots + a_{n_s-1}\beta^{n_s-1},$$

con $a_i \in \mathbb{F}_p$ para todo $i = 0, 1, \ldots, n_s - 1$. Se sigue que:

$$\begin{aligned} f &= \sum_{i=0}^{n_s-1} \alpha^{p^i} x^{sp^i} = \sum_{i=0}^{n_s-1} x^{sp^i} \left(\sum_{j=0}^{n_s-1} a_j \beta^j \right)^{p^i} \\ &= \sum_{j=0}^{n_s-1} a_j^{p^i} \sum_{i=0}^{n_s-1} \beta^{jp^i} x^{sp^i} = \sum_{j=0}^{n_s-1} a_j \sum_{i=0}^{n_s-1} \beta^{jp^i} x^{sp^i} \\ &= \sum_{j=0}^{n_s-1} a_j f_{C_s,\beta^j}. \end{aligned}$$

Nótese que $a_j^p = a_j$ si $a_j \in \mathbb{F}_p$ y que $f_{C_s,\beta^j} = \sum_{i=0}^{n_s-1} \beta^{jp^i} x^{sp^i}$ por definición. ■

Proposición 3.6. *Los polinomios $f_{C_s}, f_{C_s,\beta}, \ldots, f_{C_s,\beta^{n_s-1}}$ son linealmente independientes en $\mathbb{F}_p$*

Demostración. Supongamos por reducción al absurdo que son linealmente dependientes en $\mathbb{F}_p$; esto es, existe una combinación lineal tal que:

$$a_0 f_{C_s} + a_1 f_{C_s,\beta} + \cdots + a_{n_s-1} f_{C_s,\beta^{n_s-1}} = 0,$$

con $a_i \in \mathbb{F}_p$ para todo $i = 0, 1, \ldots, n_s$. Nótese que el menor monomio en esta combinación es:

$$(a_0 + a_1\beta + \cdots + a_{n_s-1}\beta^{n_s-1})x^s.$$

Por la igualdad anterior, el coeficiente de este monomio tiene que ser cero; es decir, β es una raíz del polinomio

$$p(x) = a_0 + a_1 x + \cdots + a_{n_s-1}x^{n_s-1}.$$

Pero esto no es posible pues, por el Teorema 1.41, el polinomio mínimo de β tiene grado n_s; ya que $|C_s| = n_s$. ■

Teorema 3.7. *Una base del conjunto de polinomios $f \in \mathcal{R}$ tales que* $\mathrm{ev}(f) \in \mathbb{F}_p^n$ *es:*

$$\mathcal{L} = \bigcup_{C_s \in \mathcal{B}} \{\, f_{C_s,\beta^j} \mid j \in \{0, 1, \ldots, n_s - 1\},\ \textit{con } \beta \textit{ primitivo en } \mathbb{F}_{p^{n_s}} \,\},$$

siendo $\mathcal{B}$ el conjunto de todas las clases ciclotómicas módulo $q-1$.

Demostración. Veamos que $\mathcal{L}$ es un conjunto linealmente independiente. Observamos que si C_s y $C_{s'}$ son dos clases distintas entonces, por construcción, los polinomios $f_{C_s,\beta}$ y $f_{C_{s'},\beta}$ tienen soporte distintos; por lo que no se puede escribir $f_{C_{s'},\beta}$ como combinación lineal del conjunto $\{f_{C_s}, f_{C_s,\beta}, \ldots, f_{C_s,\beta^{n_s-1}}\}$. Además, la Proposición 3.6 nos indica que cada conjunto $\{f_{C_s}, f_{C_s,\beta}, \ldots, f_{C_s,\beta^{n_s-1}}\}$ es linealmente independiente. Por lo tanto, $\mathcal{L}$ es linealmente independiente.

Queda comprobar que el conjunto $\mathcal{L}$ es un sistema generador. Sea $J = \{s_1, s_2, \ldots, s_l\}$ el conjunto de representantes de las clases ciclotómicas de $\mathcal{B}$. Consideramos cualquier polinomio $f \in \mathcal{R}$ y sea $a_s x^s$ el menor monomio que aparece en f. Por la Proposición 3.5, tenemos que a_s es una combinación lineal de $\{1, \beta, \ldots, \beta^{n_s-1}\}$ con β elemento primitivo de $\mathbb{F}_{p^{n_s}}$. Además, s es uno de los elementos de J y podemos suponer, sin pérdida de generalidad, que $s = s_1$, con $s_1 < s_2 \cdots < s_l$. Definimos $f_1 = f - \sum_{j=0}^{n_{s_1}-1} \lambda_j f_{C_{s_1},\beta^j}$, con $\lambda_j \in \mathbb{F}_q$. Sea $a_{s'}x^{s'}$ el menor monomio que aparece en f_1; podemos repetir el proceso anterior y definir $f_2 = f_1 - \sum_{j=0}^{n_{s_2}-1} \lambda_j f_{C_{s_2},\beta^j}$, con $s_2 = s'$. Reiterando este proceso en como mucho l pasos deducimos que f es una combinación lineal de elementos de $\mathcal{L}$. Por consiguiente, se concluye el resultado. ■

Para el siguiente resultado introducimos una aplicación lineal en $\mathbb{F}_p$ generalizando la aplicación traza definida en la Definición 1.62:

$$\begin{aligned} \mathrm{Tr}\colon\ \mathcal{R} &\longrightarrow \mathcal{R} \\ g &\longmapsto \mathrm{Tr}(g) = g + g^p + \cdots + g^{p^{r-1}}, \quad \forall g \in \mathbb{R}. \end{aligned}$$

Proposición 3.8. *La imagen de la aplicación Traza antes definida es exactamente el conjunto de todos los polinomios $f \in \mathcal{R}$ que evalúan en $\mathbb{F}_p$:*

$$\mathrm{Im}(\mathrm{Tr}) = \{\, f \in \mathcal{R} \mid \mathrm{ev}(f) \in \mathbb{F}_p^n \,\}.$$

Demostración. Sea $f = \mathrm{Tr}(g) = g + g^p + \cdots + g^{p^{r-1}}$. Como $g^{p^r} = g$ en $\mathcal{R}$ tenemos que $f^p = f$. Esto nos dice que para todo $f \in \mathrm{Im}(\mathrm{Tr})$ se tiene que $\mathrm{ev}(f) \in \mathbb{F}_p$. Por tanto, por la Proposición 3.1, $\mathrm{ev}(f) \in \mathbb{F}_p^n$ para todo $f \in \mathrm{Im}(Tr)$.

Ahora veamos que para todo $f \in \mathcal{R}$ tal que $\mathrm{ev}(f) \in \mathbb{F}_p$ se tiene que $f \in \mathrm{Im}(\mathrm{Tr})$. Para ello vamos a utilizar el Teorema 3.7 que nos dice que si $\mathrm{ev}(f) \in \mathbb{F}_p$ entonces f es una combinación lineal de elementos del conjunto $\mathcal{L} = \cup_{C_s \in \mathcal{B}} \{\, f_{C_s,\beta^j} \mid j \in \{0, 1, \ldots, n_s - 1\},$ con β primitivo en $\mathbb{F}_{p^{n_s}} \,\}$. Luego, basta con demostrar que los elementos de $\mathcal{L}$ pertenecen a $\mathrm{Im}(\mathrm{Tr})$; es decir, veamos que $f_{C_s,\beta} = \mathrm{Tr}(\gamma x^s)$, con $\beta \in \mathbb{F}_{p^{n_s}}$. Sea $\gamma \in \mathbb{F}_{p^r}$ tal que $\hat{\mathrm{Tr}}(\gamma) = \beta$, siendo:

$$\begin{aligned} \hat{\mathrm{Tr}}\colon\ \mathbb{F}_{p^r} &\longrightarrow \mathbb{F}_{p^r} \\ g &\longmapsto \hat{\mathrm{Tr}}(g) = g + g^{p^{n_s}} + \cdots + g^{p^{r-1}}, \quad \forall g \in \mathbb{F}_{p^r}. \end{aligned}$$

Se tiene que:

$$\mathrm{Tr}(\gamma x^s) = \sum_{i=0}^{r-1} \gamma^{p^i} x^{sp^i} = \sum_{j=0}^{\frac{r}{n_s}-1} \sum_{i=0}^{n_s-1} \gamma^{p^{i+jn_s}} x^{sp^{i+jn_s}}$$

Como $sp^{n_s} = s$, se tiene que: $sp^{i+jn_s} = sp^i p^{n_s^j} = sp^i$ y $p^{i+jn_s} = p^i$. Luego,

$$\mathrm{Tr}(\gamma x^s) = \sum_{i=0}^{n_s-1} x^{sp^i} \left(\sum_{j=0}^{\frac{r}{n_s}-1} \gamma^{(p^{n_s})^j} \right)^{p^i} = f_{C_s,\beta}.$$

■

Observación 3.9. Esta prueba nos proporciona una forma constructiva de cómo obtener todos los polinomios $f \in \mathcal{R}$ tales que $\mathrm{ev}(f) \in \mathbb{F}_p^n$. En particular, tenemos una fórmula para la dimensión de un código RS restringuido al subcuerpo primo.

Teorema 3.10. *Sea $\mathcal{C}$ un código Reed-Solomon de parámetros $[n, k]_q$ con $n = q - 1$ y $q = p^r$, y sea $\mathcal{C}|_{\mathbb{F}_p} := \mathcal{C} \cap \mathbb{F}_p^n$ su restricción al cuerpo $\mathbb{F}_p$. Entonces $\mathcal{C}|_{\mathbb{F}_p} = \{\, \mathrm{ev}(\mathrm{Tr}(f)) \mid f \in \mathcal{R} \,\}$ y una base de polinomios que genera $\mathcal{C}|_{\mathbb{F}_p}$ es:*

$$\bigcup_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,k-1\}}} \left\{ f_{C_s,\beta^j} \;\middle|\; \begin{array}{r} j \in \{0, 1, \ldots, n_s - 1\},\ \textit{con } \beta \textit{ elemento} \\ \textit{primitivo en } \mathbb{F}_{p^{n_s}} \textit{ y } n_s = |C_s| \end{array} \right\},$$

siendo $\mathcal{B}$ el conjunto de todas las clases ciclotómicas módulo $q-1$. Además, $\mathcal{C}|_{\mathbb{F}_p}$ tiene dimensión:

$$\dim(\mathcal{C}|_{\mathbb{F}_p}) = \sum_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,k-1\}}} n_s.$$

Demostración. Sea $\mathcal{C} = \{\, \mathrm{ev}(f) \mid f \in \mathcal{R} \,\}$. Por la Proposición 3.8 se tiene que $\mathcal{C}|_{\mathbb{F}_p} = \{\, \mathrm{ev}(\mathrm{Tr}(f)) \mid f \in \mathcal{R} \,\}$, y por la Proposición 3.7 se sigue que $\mathcal{C}|_{\mathbb{F}_p} = \{\, \mathrm{ev}(f) \mid f \in \langle \mathcal{L} \rangle \,\}$. ■

Teorema 3.11. *El dual de $\mathcal{C}|_{\mathbb{F}_p} \coloneqq \mathcal{C} \cap \mathbb{F}_p^n$ está definido por:*

$$\left(\mathcal{C}|_{\mathbb{F}_p}\right)^{\perp} \coloneqq \left(\mathcal{C} \cap \mathbb{F}_p^n\right)^{\perp} \coloneqq \{\, \mathrm{ev}(\mathrm{Tr}(f)) \mid f \in \mathrm{L}_{n-k} \,\},$$

donde L_{n-k} denota al conjunto de polinomios de grado menor que $n-k$. Una base de polinomios es:

$$\bigcup_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,n-k-1\}}} \left\{ f_{C_s,\beta^j} \;\middle|\; \begin{array}{r} j \in \{0,1,\ldots,n_s-1\},\ \textit{con } \beta \textit{ elemento} \\ \textit{primitivo en } \mathbb{F}_{p^{n_s}} \textit{ y } n_s = |C_s| \end{array} \right\},$$

con $\mathcal{B}$ el conjunto de todas las clases ciclotómicas módulo $q-1$. Además, su dimensión es:

$$\dim\left(\left(\mathcal{C}|_{\mathbb{F}_p}\right)^{\perp}\right) = \sum_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,n-k-1\}}} n_s.$$

Demostración. La demostración es análoga a la del teorema anterior teniendo en cuenta la Dualidad de Delsarte (Teorema 1.67): $\left(\mathcal{C} \cap \mathbb{F}_p^n\right)^{\perp} = \left(\mathrm{Tr}(\mathcal{C}^{\perp})\right)$. ■

Ejemplo 3.12. Sea $\mathcal{C}$ un código RS en el sentido estricto definido en $\mathbb{F}_{16}$ con parámetros $[n,k,d]_{16}$; es decir, evaluamos todos los polinomios de grado menor que k en todos los puntos de $\mathbb{F}_{16}^*$, por lo que $n = 15$. Sea $\mathcal{C}|_{\mathbb{F}_2} = \mathcal{C} \cap \mathbb{F}_2^{15}$ la restricción de $\mathcal{C}$ al subcuerpo $\mathbb{F}_2$. Vamos a hallar todos los polinomios $f \in {}^{\mathbb{F}_{16}}\!/_{(x^{15}-1)}$ que tenemos que evaluar para obtener el código $\mathcal{C}|_{\mathbb{F}_2}$.

Las distintas clases ciclotómicas módulo 15 respecto de 2^4 son: $C_0 = \{0\}$, $C_1 = \{1,2,4,8\}$, $C_3 = \{3,6,12,9\}$, $C_5 = \{5,10\}$ y $C_7 = \{7,14,13,11\}$. Recordemos que $\mathcal{C}$ es un código MDS (Proposicion 2.2), por lo que $d = n-k+1$; y que $\mathcal{C}|_{\mathbb{F}_2}$ es su restricción a $\mathbb{F}_2$, por lo que $d(\mathcal{C}|_{\mathbb{F}_2}) \geq d(C)$.

Por el Teorema 3.10 sabemos que una base para $\mathcal{C}|_{\mathbb{F}_2}$ es el conjunto de polinomios:

$$\bigcup_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,k-1\}}} \{\, f_{C_s,\beta^j} \mid j \in \{0,1,\ldots,n_s-1\},\ \text{con } \beta \text{ primitivo en } \mathbb{F}_{p^{n_s}} \,\},$$

siendo $\mathcal{B} = \{C_1, C_3, C_5, C_7\}$, y que su dimensión se obtiene como:

$$\dim(\mathcal{C}|_{\mathbb{F}_2}) = \sum_{\substack{C_s \in \mathcal{B} \\ C_s \subseteq \{0,1,\ldots,k-1\}}} n_s.$$

Luego, dependiendo del valor que tome k se tiene que:

- Si $k \in [1, 8]$, la única clase ciclotómica C_s que verifica que $C_s \subseteq \{0, 1, \ldots, k-1\}$ es la correspondiente a la clase ciclotómica C_0. Por tanto,

$$\{ f_{C_0,\beta} \mid \beta \text{ primitivo de } \mathbb{F}_2 \} = \{1\},$$

  es una base de polinomios que generan $\mathcal{C}|_{\mathbb{F}_2}$. Esto nos dice que $\dim\left(\mathcal{C}|_{\mathbb{F}_2}\right) = 1$, por lo que $\mathcal{C}|_{\mathbb{F}_2}$ es un código de parámetros $[15, 1, 15]_2$.
- Si $k = 9$, $\mathcal{C} = [15, 9, 7]_{16}$ y tenemos que considerar los polinomios con soporte $\text{supp}(f) = \{C_0, C_1\}$, donde $\{ f_{C_1,\beta^j} \mid \beta \text{ primitivo de } \mathbb{F}_{2^4} \}$ es una base de los polinomios que generan $\mathcal{C}|_{\mathbb{F}_2}$. Estos polinomios son:

$$\begin{aligned} f_{C_1} &= x + x^2 + x^4 + x^8. \\ f_{C_1,\beta} &= \beta x + \beta^2 x^2 + \beta^4 x^4 + \beta^8 x^8. \\ f_{C_1,\beta^2} &= \beta^2 x + \beta^4 x^2 + \beta^8 x^4 + \beta x^8. \\ f_{C_1,\beta^3} &= \beta^3 x + \beta^6 x^2 + \beta^{12} x^4 + \beta^8 x^8. \end{aligned}$$

  Por tanto, $\mathcal{C}|_{\mathbb{F}_2}$ es un código de parámetros $[15, 5, \geq 7]_2$.
- Si $k = 10$ no aparecen nuevos polinomios ya que $k - 1 = 9 \in C_3$, pero la clase ciclotómica $C_3 \nsubseteq \{0, 1, \ldots, 9\}$.
- Si $k = 11$, tenemos $\mathcal{C} = [15, 11, 5]_{16}$. Ahora se tienen que considerar los polinomios anteriores además de los asociados a la clase ciclotómica C_5, siendo estos:

$$\begin{aligned} f_{C_5} &= x^5 + x^{10}. \\ f_{C_5,\beta} &= \beta^5 x^5 + \beta^{10} x^{10}. \end{aligned}$$

  Se concluye que: $\mathcal{C}|_{\mathbb{F}_2} = [15, 7, \geq 5]_2$.
- Si $k = 12$, vuelve a ocurrir que no aparecen polinomios nuevos pues $k-1 = 11 \in C_7$, pero $C_7 \nsubseteq \{0, 1, \ldots, 11\}$.
- Si $k = 13$, $C = [15, 13, 3]_{16}$ y se consideran los polinomios con soporte $\text{supp}(f) = C_3$ además de los ya obtenidos previamente. Se tiene que:

$$\begin{aligned} f_{C_3} &= x^3 + x^6 + x^9 + x^{12}. \\ f_{C_3,\beta} &= \beta^3 x^3 + \beta^6 x^6 + \beta^9 x^9 + \beta^{12} x^{12}. \\ f_{C_3,\beta^2} &= \beta^6 x^3 + \beta^{12} x^6 + \beta^2 x^9 + \beta^8 x^{12}. \\ f_{C_3,\beta^3} &= \beta^9 x^3 + \beta^2 x^6 + \beta^1 1 x^9 + \beta^4 x^{12}. \end{aligned}$$

  Luego, $\mathcal{C}|_{\mathbb{F}_2} = [15, 11, \geq 3]_2$.

- Si $k = 14$, no tenemos ningún polinomio que añadir. ($k - 1 = 13 \in C_7$, pero $C_7 \nsubseteq \{0, 1, \ldots, 13\}$.)
- Si $k = 15$ entonces $\mathcal{C} = [15, 15, 1]_{16}$ y $\mathcal{C}|_{\mathbb{F}_2} = [15, 15, 1]_2$, siendo los nuevo cuatro polinomios con soporte $\operatorname{supp}(f) = C_7$:

$$f_{C_7,\beta^j} = \beta^{7j}x^7 + \beta^{11j}x^{11} + \beta^{13j}x^{13} + \beta^{14j}x^{14}, \quad \forall j \in [0, 3].$$

3.2. Códigos Alternantes

Hasta el momento solo hemos hablado de la restricción de códigos Reed-Solomon a su subcuerpo primo. En esta sección introduciremos los *códigos alternantes*, que es la familia de restricciones de códigos GRS al subcuerpo $\mathbb{F}_q$, y veremos que todo código lineal de distancia mínima $d \geq 2$ es, en realidad, un código alternante.

Definición 3.13. *Sean* $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ *una* n*-tupla de* n *elementos distintos de* $\mathbb{F}_{q^m}$ *y* $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ *una* n*-tupla de elementos no nulos de* $\mathbb{F}_{q^m}$*. Sea* $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})$ *el código RS generalizado definido en* $\mathbb{F}_{q^m}$ *de dimensión* r*. Se define el código alternante* $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ *como la restricción lineal en* $\mathbb{F}_q$ *del código dual* $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp$*, es decir,*

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) \coloneqq \mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp \cap \mathbb{F}_q.$$

Corolario 3.14. *El código alternante* $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ *tiene parámetros* $[n, k, d]_q$*, siendo* $k \geq n - mr$ *y* $d \geq r + 1$*.*

Demostración. Sabemos que el dual de $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})$ es

$$\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp = \mathrm{GRS}_{n-r}(\mathbf{a}, \mathbf{c}),$$

con $c_j^{-1} = b_j \prod_{i \neq j}(a_j - a_i)$. Por la Proposition 2.10, se tiene que $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp$ tiene parámetros $[n, n - r, r + 1]_{q^m}$.

Como el código alternante $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ se define como la restricción lineal en $\mathbb{F}_q$ del código dual $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp$, aplicando la Proposición 1.60 se concluye que $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ es un código con parámetros $[n, k, d]_q$, siendo $k \geq n - mr$ y $d \geq r + 1$. ■

Proposición 3.15. *Todo código lineal de distancia mínima 2 (o superior) es un código alternante.*

Demostración. Sean $\mathcal{C}$ un código lineal con parámetros $[n, k, d]_q$ con $d \geq 2$ y $H = (h_{ij}) \in \mathbb{F}_q^{(n-k)\times n}$ una matriz de paridad de $\mathcal{C}$. Nótese que, al ser $d \geq 2$, la cota de Singleton (Teorema 1.21) permite afirmar que $n < k$ ($2 \leq d \leq n - k + 1$).

Consideremos m un entero positivo tal que $n-k$ divide a m y $q^m \geq n$. De esta manera sabemos que el cuerpo $\mathbb{F}_{q^m}$ es una extensión finita de $\mathbb{F}_{q^{n-k}}$ (Proposición 1.29). Tomemos $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ una n-tupla de n elementos distintos de $\mathbb{F}_{q^m}$ y sea $\{\alpha_1, \alpha_2, \ldots, \alpha_{n-k}\}$ una base de $\mathbb{F}_{q^{n-k}}$ como espacio vectorial de $\mathbb{F}_q$. Definimos $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^m}^n$, siendo:

$$b_j = \sum_{i=1}^{m} h_{ij}\alpha_i \in \mathbb{F}_{q^m}, \qquad \text{para cada } j = 1, 2, \ldots, n.$$

Recordemos que la distancia mínima de $\mathcal{C}$ es igual al número mínimo de columnas linealmente dependientes de H. Como $d \geq 2$, esto significa que H no tiene ninguna columna igual al vector nulo y, por tanto, $b_j \neq 0$, para todo $j = 1, 2, \ldots, n$. De esta forma, $\mathcal{C}$ es la restricción del código $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b})^{\perp}$, es decir, hemos probado que:

$$\mathcal{C} = \mathrm{Alt}_1(\mathbf{a}, \mathbf{b}).$$

■

3.3. Códigos Goppa

Siguiendo la introducción de los códigos alternantes estudiaremos ahora los *códigos Goppa*. Veremos la definición formal de estos códigos como un código lineal en $\mathbb{F}_q$ y probaremos que son una familia específica de códigos alternantes, lo que nos será de ayuda para estudiar sus propiedades.

Definición 3.16. *Sean $L = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ una n-tupla de n elementos distintos de $\mathbb{F}_{q^m}$ y $g \in \mathbb{F}_{q^m}[x]$ un polinomio tal que $g(a_j) \neq 0$ para todo j (un polinomio con estas características se denomina polinomio de Goppa respecto de L). Se define el código Goppa respecto de L y g como:*

$$\Gamma(L, g) \coloneqq \left\{ c \in \mathbb{F}_{q^n} \;\middle|\; \sum_{j=1}^{n} \frac{c_j}{x - a_j} \equiv 0 \mod g(x) \right\},$$

que se trata de un código lineal definido en $\mathbb{F}_q$ de longitud n.

Observación 3.17. Al suponer que $g(a_j) \neq 0$, los polinomios $g(x)$ y $(x - a_j)$ son primos relativos y, por tanto, su máximo común divisor es 1. El algoritmo de Euclides nos proporciona dos polinomios P_j y Q_j tales que $P_j(x)g(x) + Q_j(x)(x - a_j) = 1$. Así, $Q_j(x)$ es el inverso de $(x - a_j)$ módulo $g(x)$. Afirmamos que:

$$Q_j(x) = -\frac{g(x) - g(a_j)}{x - a_j} g(a_j)^{-1}.$$

En efecto, nótese que $g(x) - g(a_j)$ tiene a a_j como cero, por lo que $g(x) - g(a_j)$ es divisible por $(x - a_j)$ y su fracción es un polinomio de grado menor que el grado de $g(x)$. Con la definición anterior de Q_j se sigue que:

$$\begin{aligned} Q_j(x)(x - a_j) &= -(g(x) - g(a_j))g(a_j)^{-1} = 1 - g(x)g(a_j)^{-1} \\ &\equiv 1 \mod g(x). \end{aligned}$$

Observación 3.18. Sean g_1 y g_2 dos polinomios de Goppa respecto de L. Si g_2 divide a g_1, entonces el código Goppa $\Gamma(L, g_1)$ es un subcódigo de $\Gamma(L, g_2)$.

En efecto, sea $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ una palabra del código $\Gamma(L, g_1)$, esto es,

$$\sum_{j=1}^{n} \frac{c_j}{x - a_j} \equiv 0 \mod g_1(x).$$

Llamamos $f = \sum_{j=1}^{n} \frac{c_j}{x - a_j}$. La relación de congruencia nos dice que g_1 divide a f. Ya que g_2 divide a g_1, también g_2 divide a f. Esto significa que $f \equiv 0$ mód $g_2(x)$ y, por tanto, $\mathbf{c}$ es una palabra en $\Gamma(L, g_2)$.

Proposición 3.19. *Sean $L = \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ una n-tupla de n elementos distintos de $\mathbb{F}_{q^m}$ y $g \in \mathbb{F}_{q^m}[x]$ un polinomio de Goppa de grado r. Entonces,*

$$\Gamma(L, g) = \mathrm{Alt}_r(\mathbf{a}, \mathbf{b}), \quad \textit{con } b_j = \frac{1}{g(a_j)}.$$

Demostración. La Observación 3.17 nos dice que $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \Gamma(L, g)$ si, y solo si,

$$\sum_{j=1}^{n} c_j \frac{g(x) - g(a_j)}{x - a_j} g(a_j)^{-1} = 0.$$

El lado izquierdo de la igualdad es un polinomio de grado menor que el grado de $g(x)$ y este polinomio es nulo si, y solo si, es 0 módulo $g(x)$.

Sea $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ con $g_i \in \mathbb{F}_{q^m}$. Entonces,

$$\begin{aligned} \frac{g(x) - g(a_j)}{x - a_j} &= \sum_{l=0}^{r} g_l \frac{x^l - a_j^l}{x - a_j} = \sum_{l=0}^{r} g_l \sum_{i=0}^{l-1} x^i a_j^{l-1-i} \\ &= \sum_{i=0}^{r-1} \left(\sum_{l=i+1}^{r} g_l a_j^{l-1-i} \right) x^i. \end{aligned}$$

Por lo tanto, $c \in \Gamma(L, g)$ si, y solo si,

$$\sum_{j=1}^{n} \left(\sum_{l=i+1}^{r} g_l a_j^{l-1-i} \right) g(a_j)^{-1} c_j = 0, \quad \forall i = 0, 1, \ldots, r-1.$$

Esto es, $H_1 c^\top = 0$, donde $H_1 \in \mathbb{F}_{q^m}^{r\times n}$ es una matriz de paridad de dimensiones $r \times n$ con columna j-ésima como sigue:

$$\begin{pmatrix} g_r a_j^{r-1} + g_{r-1} a_j^{r-2} + \cdots + g_2 a_j + g_1 \\ \vdots \\ g_r a_j^2 + g_{r-1} a_j + g_{r-2} \\ g_r a_j + g_{r-1} \\ g_r \end{pmatrix} g(a_j)^{-1} \in \mathbb{F}_{q^m}^{r\times 1}.$$

Recordemos que el polinomio $g(x)$ tiene grado r, por lo que el coeficiente g_r es no nulo. Dividimos la última fila de H_1 por g_r, restamos g_{r-1} veces la fila r de la fila $r-1$ y dividimos la fila $r-1$ por g_r. Reiterando este proceso de transformaciones elementales se prueba que H_1 es equivalente a una matriz $H_2 \in \mathbb{F}_{q^m}^{r\times n}$ con elementos $a_j^{i-1} g(a_j)^{-1}$ en las poisiciones (i, j). Por tanto, H_2 es la matriz generatriz del código $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})$, donde $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ y $b_j = 1/g(a_j)$. De esta forma, $\Gamma(L, g)$ es la restricción de $\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp$, esto es, $\Gamma(L, g) = \mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ por definición. ■

Corolario 3.20. *Sea $g \in \mathbb{F}_{q^m}[x]$ un polinomio de Goppa de grado r. El código Goppa $\Gamma(L, g)$ tiene parámetros $[n, k, d]$, donde*

$$k \geq n - mr \quad y \quad d \geq r + 1.$$

Demostración. Sabemos que un código Goppa es equivalente a un código alternante (Proposición 3.19) y ya conocemos los parámetros de estos códigos (Corolario 3.14). ■

Observación 3.21. Sea $g \in \mathbb{F}_{q^m}[x]$ un polinomio de Goppa de grado r. Por el Corolario 3.20, el código Goppa $\Gamma(L, g)$ tiene distancia mínima $d \geq r + 1$. Sabemos que es equivalente a un código alternante, esto es, una restricción de un código a un subcuerpo de un GRS de distancia mínima $r+1$ (por la Proposición 3.19). Como estos supercódigos tienen un algoritmo eficiente de descodificación que corrige $\lfloor r/2 \rfloor$ errores (véase la Sección 2.3), los mismos algoritmos se pueden aplicar al código Goppa para corregir $\lfloor r/2 \rfloor$ errores.

Definición 3.22. *Un polinomio se dice libre de cuadrados si todos sus factores (irreducibles) tienen multiplicidad uno.*

Observación 3.23. Si $g(x) \in \mathbb{F}_{q^m}[x]$ es un polinomio de Goppa libre de cuadrados entonces $g(x)$ y su primera derivada $g'(x)$ no tienen factores en común.

Proposición 3.24. *Sea g un polinomio de Goppa libre de cuadrados con coeficientes en $\mathbb{F}_{2^m}$. Entonces, el código Goppa $\Gamma(L, g)$ es igual al código $\Gamma(L, g^2)$.*

Demostración. Tenemos que ver que $\Gamma(L,g) = \Gamma(L,g^2)$. Como g divide a g^2, de la Obervación 3.18 se sigue que el código $\Gamma(L,g^2)$ es un subcódigo de $\Gamma(L,g)$.

Probamos ahora que $\Gamma(L,g) \subseteq \Gamma(L,g^2)$. Sean $\mathbf{c} \in \mathbb{F}_2^n$ y $L = \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{2^m}^n$. Definimos el siguiente polinomio:

$$f(x) = \prod_{j=1}^{n} (x - a_j)^{c_j} \in \mathbb{F}_{2^m}[x].$$

De esta manera, $f(x)$ es un polinomio mónico de grado $\mathrm{w_H}(c)$ tal que sus ceros se localizan en los elementos a_j donde $c_j \neq 0$. Derivando f(x) obtenemos:

$$f'(x) = \sum_{j=1}^{n} c_j (x - a_j)^{c_j - 1} \prod_{\substack{l=1 \\ l \neq j}}^{n} (x - a_l)^{c_l} \Rightarrow \frac{f'(x)}{f(x)} = \sum_{j=1}^{n} \frac{c_j}{x - a_j}.$$

Si $\mathbf{c} \in \Gamma(L,g)$ entonces, por definición, ${}^{f'(x)}/_{f(x)} \equiv 0 \mod g(x)$ y, ya que $mcd(f(x), g(x)) = 1$, existen polinomios $p(x)$ y $q(x)$ tales que $p(x)f(x) + q(x)g(x) = 1$. Esto que significa que $p(x)f(x) \equiv 1 \mod g(x)$. Por tanto,

$$p(x)f'(x) \equiv \frac{f'(x)}{f(x)} \equiv 0 \mod g(x).$$

Como $mcd(p(x), g(x)) = 1$, esto nos dice que $g(x)$ divide a $f'(x)$.

Escribimos $f(x) = f_0 + f_1 x + \cdots + f_n x^n$. Entonces,

$$f'(x) = \sum_{i=0}^{n} i f_i x^{i-1} = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} f_{2i+1} x^{2i} = \left(\sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} f_{2i+1}^{2^{m-1}} x^i \right)^2,$$

pues $2if_{2i} = 0$ y $f_{2i+1} = f_{2i+1}^{2^m}$ (recordemos que $f_i \in \mathbb{F}_{2^m}$). Luego, $f'(x)$ es un cuadrado que es divisible por $g(x)$, un polinomio libre de cuadrados, es decir, $f'(x)$ es divisible por $g^2(x)$. Por tanto, $\mathbf{c}$ también es una palabra de $\Gamma(L,g^2)$ y se concluye que $\Gamma(L,g) \subseteq \Gamma(L,g^2)$. ■

Corolario 3.25. *Sea g un polinomio de Goppa libre de cuadrados de grado r con coeficientes en $\mathbb{F}_{2^m}$. Entonces el código Goppa $\Gamma(L,g)$ tiene parámetros [n,k,d], donde*

$$k \geq n - mr \quad y \quad d \geq 2r + 1.$$

Demostración. Por la Proposición 3.24 sabemos que $\Gamma(L,g) = \Gamma(L,g^2)$. Luego, el resultado es directo a partir del Corolario 3.20. La cota inferior de la dimensión usa que $g(x)$ tiene grado r, mientras que la cota inferior de la distancia mínima usa que $g^2(x)$ tiene grado $2r$. ■

Esta propiedad específica de los códigos Goppa definidos en $\mathbb{F}_2$ cuando se considera un polinomio de Goppa separable los hace interesantes para criptografía gracias a su alta capacidad de corrección. Obsérvese que para cualquier código Goppa podemos suponer que su distancia mínima es $d \geq r+1$; sin embargo, los códigos específicos del Corolario 3.25 nos aseguran una mejor distancia mínima, siendo esta $d \geq 2r+1$.

3.4. ¿Qué familia de códigos de evaluación parecen códigos aleatorios?

Para ser capaces de responder a esta pregunta primero necesitaremos introducir cómo se define el *producto estrella* entre dos códigos lineales. Recordemos que el producto estrella $*$ de dos vectores $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ se define como la multiplicación coordenada a coordenada; es decir,

$$\mathbf{a} * \mathbf{b} \coloneqq (a_1 b_1, a_2 b_2, \ldots, a_n b_n), \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

Definición 3.26. *El producto estrella entre dos códigos lineales $\mathcal{C}$ y $\mathcal{D}$ de longitud n en $\mathbb{F}_q$ se define como:*

$$\mathcal{C} * \mathcal{C} = \langle \{ \mathbf{a} * \mathbf{b} \mid \mathbf{a} \in \mathcal{C} \wedge \mathbf{b} \in \mathcal{C} \} \rangle.$$

Cuando $\mathcal{D} = \mathcal{C}$, se dice que $\mathcal{C} * \mathcal{C}$ es el cuadrado del código $\mathcal{C}$ y denotaremos por $\mathcal{C}^2$.

Sea $k(\mathcal{C})$ la dimensión del código $\mathcal{C}$, es fácil comprobar que la dimensión de $\mathcal{C}^2$ verifica que:

$$k(\mathcal{C}^2) \leq \binom{k(\mathcal{C})+1}{2};$$

ya que si $\{\mathbf{a_1}, \ldots, \mathbf{a_k}\}$ es una base de $\mathcal{C}$, entonces $\mathbf{a_i} * \mathbf{a_j}$ genera al código $\mathcal{C}^2$ con $1 \leq i \leq j \leq k$. Es más, si $\mathcal{C}$ es un código lineal aleatorio de dimensión k con $k = \mathcal{O}(\sqrt{n})$, entonces en [4] se demuestra que la probabilidad que:

$$\mathcal{P}\left(k(\mathcal{C}^2) < \binom{k+1}{2}\right) \xrightarrow[n\to\infty]{} 0.$$

Sin embargo, por la Proposición 2.12, sabemos que: si $k \leq \frac{n+1}{2}$, entonces $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})^2 = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$. Por lo tanto, con alta probabilidad, la dimensión del cuadrado de un código lineal crece de forma exponencial, mientras que la dimensión de un código GRS sólo se duplica. Este hecho es fundamental para distinguir códigos Reed-Solomon frente a otras familias de códigos lineales. Es más, esta propiedad es la que hace vulnerable a esta familia de códigos en criptografía de clave pública.

Además en [4] también se demuestra que los códigos Goppa con alta tasa de información son indistinguibles de un código lineal aleatorio. Es por ello que son una buena familia de códigos para el criptosistema de McEliece.

Observación 3.27. A los códigos alternantes no se les aplica el resultado anterior. En efecto, recordemos que el código alternante $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ es un subcódigo del código Reed-Solomon generalizado $\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$. Por lo tanto, es fácil comprobar que el cuadrado del código alternante es de nuevo un subcódigo del cuadrado de un código GRS. En efecto:

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})^{(2)} \subseteq \mathrm{GRS}_{2(n-r)-1}(\mathbf{a}, \mathbf{c}).$$

Sin embargo para que esta propiedad nos permita distinguir los códigos alternantes necesitaríamos que $\mathrm{GRS}_{2(n-r)-1}(\mathbf{a}, \mathbf{c})$ no fuese todo el espacio $\mathbb{F}_q^n$, es decir que $2(n-r) < n$, o de forma equivalente que $r > \frac{n}{2}$. Sin embargo observamos que

$$\dim(\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})) = n - rm \geq 0 \to r < \frac{n}{m} \leq \frac{n}{2} \text{ para todo } m \geq 1.$$

Bibliografía

[1] E. Berlekamp. *Non-binary BCH Decoding.* Information Theory, IEEE Transactions on, vol.14, no.2, p.242, 1968.

[2] T. Berger and P. Loidreau. *How to mask the structure of codes for a cryptographic use.* Des. Codes Cryptogr., 35:63–79, 2005.

[3] D. J. Bernstein, T. Lange. *Post-quantum Cryptography.* Nature Volume 549, pages 188-194, 2017.

[4] J.C. Faugère, V. Gauthier-Umaña, A. Otmani, L.Perret and J.P. Tillich. *A distinguisher for high-rate McEliece cryptosystems.* IEEE Transaction on Information Theory, 59(10): 6830-8644, 2013.

[5] D. Gorenstein, N. Zierler. *A Class Of Error-Correcting Codes In p m Symbols.* Journal of the Society for Industrial and Applied Mathematics, vol.9, no.2, pp.207-214, 1961.

[6] V. Guruswami, M. Sudan. *Improved decoding of Reed-Solomon and algebraic-geometry codes.* IEEE Trans. Inform. Theory, 45(6):1757-1767, 1999.

[7] F.Hernando, M.E. O'Sullivan, E. Popovici and S. Srivastava. *Subfield-Subcodes of Generalized Toric codes.* 2010 IEEE International Symposium on Information Theory (ISIT 2010), 1125 - 1129.

[8] W.C. Huffman, and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2010.

[9] R. Koetter, A. Vardy. *Algebraic Soft-Decision Decoding of Reed-Solomon Codes.* Information Theory, IEEE Transactions on, vol.49, no.11, pp.2809-2825, 2003.

[10] J. L. Massey. *Shift-Register Synthesis and BCH Decoding.* Information Theory, IEEE Transactions on, vol.15, no.1, p.122, 1969.

[11] R. J. McEliece. *A public-key cryptosystem based on algebraic coding theory.* DSN Progress Report, 42–44:114–116, 1978.

[12] L. Minder and A. Shokrollahi. *Cryptanalysis of the Sidelnikov cryptosystem.* In EURO-CRYPT 2007, volume 4515 of Lecture Notes in Comput. Sci., pages 347–360. Springer-Verlag Berlin Heidelberg, 2007.

[13] D. E. Muller. *Application of Boolean algebra to switching circuit design and to error detection.* Transactions of the I.R.E. Professional Group on Electronic Computers. EC-3 (3): 6–12, 1954.

[14] H. Niederreiter. *Knapsack-type cryptosystems and algebraic coding theory.* Problems of Control and Information Theory, 15(2):159–166, 1986.

[15] W. W. Peterson. *Encoding and Error-Correction Procedures for the Bose-Chaudhuri-Codes.* Information and Theory, vol.6, no.4, pp.459- 470, 1960.

[16] R. Pellikaan, X-W. Wu, R. Jurrius, and S. Bulygin. *Codes, Cryptology and Curves with Computer Algebra.* Cambridge University Press, 2017.

[17] I.S. Reed. *A class of multiple-error-correcting codes and the decoding scheme.* Transactions of the IRE Professional Group on Information Theory. 4 (4): 38–49, 1954.

[18] I. S. Reed, G. Solomon. *Polynomial Codes Over Certain Finite Fields.* Journal of Society for Industrial and Applied Mathematics, vol.8, no.2, pp.300-304, 1960.

[19] N. Sendrier. *Code-Based Cryptography: State of the Art and Perspectives.* In IEEE Security and Privacy, vol. 15, no. 4, pp. 44-50, 2017.

[20] V. M. Sidelnikov and S. O. Shestakov. *On the insecurity of cryptosystems based on generalized Reed-Solomon codes.* Discrete Math. Appl., 2:439–444, 1992.

[21] V. M. Sidelnikov. *A public-key crypto system based on binary reed-muller codes.* Discrete Math. Appl., 4(3):191–208, 1994.

[22] M. Sudan. *Decoding of Reed Solomon codes beyond the error-correction bound.* J. Complexity, 13(1):180-193, 1997.

[23] C. Wieschebrink. *Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes.* In Post-Quantum Cryptography, volume 6061 of Lecture Notes in Comput. Sci., pages 61–72. Springer-Verlag Berlin Heidelberg, 2010.

Which family of codes is suitable for code-based cryptography?

Sección de Matemáticas
Universidad de La Laguna

Oswaldo José Pérez Luis

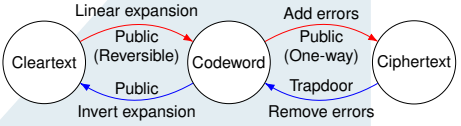
Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0100894141@ull.edu.es

Abstract

In the Introduction, we talk about the differences between Coding Theory and Cryptography, and how they can be merged in Code-based Cryptography (CBC), one of the proposals for post-quantum cryptography. In addition, we explain which families of codes are suitable for CBC according to their security, that is, based on the fact that the chosen family is indistinguishable from a random code. Then, we introduce and we study the fundamental properties of some families of polynomial codes. In particular, Reed-Solomon codes and their generalizations, as well as Reed-Muller codes. We study subfield-subcodes of the previously named families, such as the Goppa codes, which can be studied as a subfield-subcode of a generalized Reed-Solomon code.

1. Code-based Cryptography

Code-based cryptography is one of the few mathematical techniques that enables the construction of public-key cryptosystems that are secure against a quantum computer adversary. In 1978, early in the history of public-key cryptography, McEliece proposed to use a generator matrix as a public key, and encrypted a codeword by adding an specified number of errors to it. The scheme's security relies on two computacional assumptions: generic decoding is hard on average, and the public key (the generator matrix of a Goppa code) is hard to distinguish from a matrix of a random code.



Algorithm 1: McEliece publick-key encryption scheme

Input: A linear code $\mathcal{C}$ with an efficient decoding algorithm $D_{\mathcal{C}}$.
Public key: (G, t) where G is a generator matrix of $\mathcal{C}$ and t is the number of errors we can correct.
Private key: The decoding algorithm $D_{\mathcal{C}}$.
Encryption: $\mathbf{c} = \mathbf{m}G + \mathbf{e}$ with $\mathrm{w_H}(\mathbf{e}) \leq t$.
Decryption: Apply $D_{\mathcal{C}}$ to $\mathbf{c}$.

2. Generalized Reed-Solomon codes

Let n be a positive integer such that $1 \leq n \leq q$. Let $\mathbf{a} \in \mathbb{F}_q^n$ be an n-tuple of mutually distinct elements of $\mathbb{F}_q$ and let $\mathbf{b} \in \mathbb{F}_q^n$ be an n-tuple of non-zeros elements of $\mathbb{F}_q$. Let k be a non negative integer such that $0 \leq k \leq n$. The generalized Reed-Solomon code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ of dimension k is defined by:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) := \left\{ \mathrm{ev}_{k,\mathbf{a}}(f(x)) * \mathbf{b} \,|\, \deg(f(x)) < k \right\}.$$

This codes are Maximum Distance Separable codes, their dual code is again a GRS code, and we have an eficient decoding algorithm for them.
The Generalized Reed-Solomon codes were proposed for code-based cryptography by Niederreiter in 1986 but its strong linear structure allowed Sidelnikov and Shestakov describe an atack in 1992.
Some years later, in 2005, Berger and Loidreau proposed a subcode of an generalized Reed-Solomon code, but this one was atacked by Wieschebrink in 2010.

3. Reed-Muller codes

Let r, m be non negative integers such that $0 \leq r < m(q-1)$ and let $n = q^m$. The Reed-Muller code $\mathrm{RM}_q(r, m)$ of order (or degree) r in m variables is defined as:

$$\mathrm{RM}_q(r, m) := \left\{ \mathrm{ev}_{\mathscr{D}}(f(x)) \,|\, \deg(f(x)) \leq r \right\}.$$

This polynomial codes are, in a wide sense, a generalization of Reed-Solomon codes in multiple variables, and like those, their dual is again an RM code. But we cannot say that they are Maximum Distance Separable codes.
The binary Reed-Muller codes were proposed by Sidelnikov in 1994 although this family also turned to not be secure since Minder and Shokrollahi provided an attack in 2007.

4. Subfield-subcodes of RS codes and GRS codes

Let $\mathscr{D}$ be an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^n$. Let $\mathscr{C}$ be an $\mathbb{F}_{q^m}$-linear code of length n. If $\mathscr{D} \subseteq \mathscr{C} \cap \mathbb{F}_q^n$, then $\mathscr{D}$ is called a subfield subcode. If $\mathscr{D} = \mathscr{C} \cap \mathbb{F}_q^n$, then $\mathscr{D}$ is called the restriction (by scalars) of $\mathscr{C}$.
Let $\mathscr{C}$ be the narrow-sense $[n, k, d]_q$ Reed-Solomon code where $n = q - 1$ and $q = p^r$, and let $\mathscr{D} = \mathscr{C} \cap \mathbb{F}_p^n$ be its restriction to $\mathbb{F}_p$. Then,

$$\mathscr{D} := \left\{ \mathrm{ev}(\mathrm{Tr}(f)) \,|\, f \in \frac{\mathbb{F}_q[x]}{(x^{(q-1)} - 1)} \right\}.$$

Let $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ be the generalized RS code over $\mathbb{F}_{q^m}$ of dimension k. The alternant code $\mathrm{Alt}_k(\mathbf{a}, \mathbf{b})$ is the $\mathbb{F}_q$-linear restriction of $(\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}))^{\perp}$, i.e:

$$\mathrm{Alt}_k(\mathbf{a}, \mathbf{b}) := (\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}))^{\perp} \cap \mathbb{F}_q^n.$$

An interesting property is that every linear code of minimum distance at least 2 is an alternant code.

5. Goppa codes

Let $L = (a_1, a_2, \ldots, a_n)$ be an n-tuple of distinct elements of $\mathbb{F}_{q^m}$. A polynomial g with coefficients in $\mathbb{F}$ such that $g(a_j) \neq 0$ for all j is called a Goppa polynomial with respecto to L. The $\mathbb{F}_q$-linear Goppa code with respect to L and g is defined by:

$$\Gamma(L, g) := \left\{ \mathbf{c} \in \mathbb{F}_q^n \,|\, \sum_{j=1}^{n} \frac{c_j}{x - a_j} \equiv 0 \mod g(x) \right\}.$$

Let $L = \mathbf{a} = (a_1, a_2, \ldots, a_n)$ be an n-tuple of distinct elements of $\mathbb{F}_{q^m}$. Let g ge a Goppa polynomial of degree r. The Goppa code $\Gamma(L, g)$ is equal to the alternat code $\mathrm{ALT}_r(\mathbf{a}, \mathbf{b})$ where $b_j = \frac{1}{g(a_j)}$.
In this work, we first introduced the classical definition of a Goppa code and then its definition as an Alternant code (i.e. a subfield-subcode of a GRS code). Both definitions are equivalent.
Binary Goppa codes were proposed by McEliece in 1978 for CBC and this family still remains secure.

TRABAJO FIN DE GRADO, Convocatoria de Julio, 2019