Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Códigos de Reed–Muller

Autor: Esther Cantero Labazuy
Tutor: Umberto Martínez Peñas
Curso 2024-2025

Índice general

Resumen

Este trabajo se estructura en cinco capítulos en los que se desarrolla el estudio de los códigos Reed-Muller. Se comienza presentando los preliminares necesarios para el desarrollo del trabajo. Se introducen conceptos y resultados sobre los cuerpos finitos y los códigos lineales, que constituyen la base sobre la cual se construyen y analizan los códigos Reed-Muller. En segundo lugar, se estudian los códigos de evaluación, se describe la construcción de los códigos a partir de las evaluaciones de los polinomios, y se presentan dos de sus parámetros fundamentales: la longitud y la dimensión. A continuación, calculamos la distancia mínima, y para ello recurriremos a los ideales monomiales y a la cota de footprint. Posteriormente, se analiza un algoritmo de descodificación, y se estudia su funcionamiento y su justificación teórica. Por último, se introduce el concepto de códigos descodificables localmente y se ve como los Reed-Muller cumplen esta propiedad.

Abstract

This work is structured into five chapters, in which the study of Reed–Muller codes is developed. It begins by presenting the necessary preliminaries for the development of the work. Concepts and results related to finite fields and linear codes are introduced, as they form the foundation upon which Reed–Muller codes are constructed and analyzed. Secondly, evaluation codes are studied: the construction of the codes from polynomial evaluations is described, and two of their fundamental parameters—length and dimension—are presented. Next, the minimum distance is computed, for which monomial ideals and the footprint bound are employed. Subsequently, a decoding algorithm is analyzed, including its operation and theoretical justification. Finally, the concept of locally decodable codes is introduced, and it is shown how Reed–Muller codes satisfy this property.

Introducción

Desde los inicios, la transmisión de la información ha estado expuesta a errores, ya sea por interferencias, defectos técnicos o limitaciones de los canales de comunicación. Para afrontar este desafío, surgió la teoría de la codificación, una rama de las matemáticas que estudia métodos eficientes para detectar y corregir errores en mensajes. Este campo con raíces algebraicas ha demostrado ser esencial en múltiples áreas de la ciencia y la tecnología, y tiene importantes aplicaciones en la transmisión y almacenamiento de la información.

Entre los muchos tipos de códigos correctores que se han desarrollado, los códigos Reed-Muller destacan por su estructura algebraica, su capacidad correctora y sus propiedades que los hacen útiles en contextos como la computación distribuida, la complejidad computacional y la teoría de la información. Estos códigos fueron introducidos en la década de 1950 por Irving S. Reed y David E. Muller, y fueron creados inicialmente para mejorar la fiabilidad en la transmisión de datos a través de canales ruidosos, como los utilizados en las primeras comunicaciones espaciales. A pesar de haber sido propuestos hace medio siglo, los códigos Reed-Muller siguen siendo objeto de estudio.

En este trabajo de fin de grado se realiza un estudio de los códigos Reed-Muller desde una perspectiva algebraica, abordando tanto sus fundamentos teóricos como algunos aspectos relacionados con su descodificación.

El objetivo de este trabajo final de grado es estudiar la construcción, los parámetros fundamentales y métodos de descodificación de los códigos Reed-Muller. Para ello vamos a introducir nociones sobre los cuerpos finitos, los códigos lineales y los códigos de evaluación, ya que constituyen la base sobre la que se construyen los códigos Reed-Muller, vamos a recurrir a herramientas de la teoría de ideales, como los ideales monomiales y la cota de footprint para poder calcular uno de los parámetros fundamentales: la distancia mínima, vamos a estudiar un método de descodificación y a introducir el concepto de localmente descodificable que acabará proporcionándonos métodos de descodificación local.

Capítulo 1

Preliminares

1.1. Cuerpos finitos

Para poder describir un código y las palabras de este vamos a necesitar una estructura algebráica sobre este código, y para esto vamos a definir y estudiar los cuerpos finitos. En este apartado vamos a ver la existencia, la unicidad y la construcción de estos, y todo lo que vayamos a necesitar a la hora de trabajar con los códigos Reed-Muller.
Para la escritura de este capítulo se ha utilizado como referencia [4].

Cardinal de un cuerpo finito

Decimos que un cuerpo es finito si posee un número finito de elementos.
Lo primero que tenemos que comprobar es si estos cuerpos existen, y vamos a ver con este resultado que sí lo hacen:

Proposición 1.1. *El anillo cociente $\mathbb{Z}/\langle p\rangle$ es un cuerpo si y solo si p es un número primo.*

Demostración. Si p es primo entonces todo $m \in \mathbb{Z}/\langle p\rangle$ no nulo es primo con él, con lo cual, por la identidad de Bezout, existen enteros x e y tales que $1 = xm + yp$, y tomando clases módulo p, tenemos que x es el inverso de m y por tanto m es unidad. Pero, si p no es primo, todo divisor no trivial de p es divisor de cero, y por tanto $\mathbb{Z}/\langle p\rangle$ no puede ser un cuerpo. □

Por tanto, tenemos que para todo número natural primo p existe un cuerpo finito de p elementos, con lo que hemos probado la existencia de cuerpos finitos. La pregunta que podemos hacernos ahora es si existen cuerpos finitos con cualquier cardinal, y para esta cuestión vamos a ver el siguiente resultado:

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

Demostración. Sea K cuerpo finito con $q \geq 2$ elementos.
Consideramos 0_K el neutro de K para la suma y 1_K el neutro de K para el producto. Para todo entero n podemos definir lo que denotaremos por $n \cdot 1_K$: si $n = 0$, $n \cdot 1_K := 0_K$, si $n > 0$, $n \cdot 1_K := \overbrace{1_K + \cdots + 1_K}^{n \ \ veces}$, y si $n < 0$, $n \cdot 1_K := -(\overbrace{1_K + \cdots + 1_K}^{-n \ \ veces})$.
Esto nos permite definir una aplicación:

$$\varphi : \mathbb{Z} \longrightarrow K;\ \varphi(n) = n \cdot 1_K.$$

Tenemos que φ es un homomorfismo de anillos, y sabemos que el $\ker(\varphi) = \varphi^{-1}(0_K)$ es un ideal de $\mathbb{Z}$, y como $\mathbb{Z}$ es infinito y K es finito φ no puede ser inyectivo y $\ker(\varphi) \neq \langle 0 \rangle$.
Entonces existe $s \geq 1$ tal que $\ker(\varphi) = \langle s \rangle$.
Como K es un cuerpo en particular es un dominio de integridad y por tanto $\langle 0_K \rangle$ es primo y entonces $\varphi^{-1}(0_K)$ también es primo.
Esto implica que $\ker(\varphi) = \langle p \rangle$ con p primo, ya que si p no fuese primo existirían n y m tales que $p = n \cdot m$, y n y m no estarían en $\ker(\varphi)$ y p si, y el ideal por tanto no sería primo.
Además, tenemos que $K' = \mathrm{Im}(\varphi) \simeq \mathbb{Z}/\ker(\varphi) = \mathbb{Z}/\langle p \rangle$ con lo cual K contiene al subcuerpo K', y por tanto tiene una estructura de espacio vectorial sobre K'. Como tiene un número finito de elementos, es de dimensión finita sobre K'. Si r es tal dimensión puesto que $K \simeq K'^r$ tenemos que K tiene p^r elementos. □

De esta demostración podemos deducir también:

Corolario 1.1. *$\mathbb{Z}/\langle p \rangle$ es el único cuerpo con un número primo p de elementos salvo isomorfismos.*

A estos cuerpos los denotaremos $\mathbb{F}_p$.
Con esto hemos visto cómo es el cardinal de un cuerpo finito, pero ¿existe para todo primo p y todo número natural r un cuerpo con p^r elementos? Para poder responder a esta pregunta vamos a necesitar el suiguiente resultado, que no demostraremos por brevedad, pero se puede encontrar en [4]:

Teorema 1.1. *Para todo número primo p y todo entero $r \geq 1$ existe un polinomio de $\mathbb{F}_p[x]$ irreducible de grado r.*

Este resultado nos va a permitir construir un cuerpo con p^r elementos, y con ello demostrar el siguiente teorema:

Teorema 1.2. *Para todo número primo p y todo número natural r, existe un cuerpo K con p^r elementos.*

Demostración. Tomamos un polinomio $f \in \mathbb{F}_p[x]$ de grado r, irreducible, consideramos $A = \mathbb{F}_p[x]/\langle f \rangle$.
Vamos a ver que A es un cuerpo: tomamos un elemento $\bar{g} \in A$ distinto de 0, como f es irreducible tenemos que $mcd(f, g) = 1$.
Por la identidad de Bezout, sabemos que existen otros dos polinomios $q, t \in \mathbb{F}_p[x]$ tales que: $f \cdot q + g \cdot t = 1$. Esto en A, nos indica que $\bar{g} \times \bar{t} = \bar{1}$ y entonces $\bar{t}$ es el inverso de $\bar{g}$ en A.
Ya hemos visto que es un cuerpo, pero ¿cuántos elementos tiene?
Ocurren dos cosas:
1) Si $g \in \mathbb{F}_p[x]$ es un polinomio arbitrario, entonces si lo dividimos por f obtenemos que existen $q, s \in \mathbb{F}_p[x]$ tales que $g = q \cdot f + s$ y con $deg(s) < r$. Por tanto, $\bar{g} = \bar{s}$ en A, con lo que todo elemento de A tiene un representante con grado menor a r.
2) Si $s, s' \in \mathbb{F}_p[x]$ son dos polinomios distintos en $\mathbb{F}_p[x]$ y ambos con grado menor que r entonces son distintos también en A. Ya que si $\bar{s} = \bar{s'}$ entonces $s - s' \in \langle f \rangle$, y por tanto, $f|(s - s')$, pero el grado de $s - s'$ es menor que r, y por tanto menor que el grado de f, y como el único multiplo de f de grado menos que el de f es el polinomio nulo, esto implica que $s - s' = 0$ con lo cual $s = s'$ con lo que llegamos a una contradicción.
De 1) y 2) concluimos que el número de elementos de A es el número de polinomios de $\mathbb{F}_p[x]$ de grado menor que r, con lo cual, el cardinal de A es p^r.

□

Característica de un cuerpo

Ahora vamos a hablar sobre la característica de un cuerpo:

Definición 1.1. Si K es un cuerpo, la característica de K se define como el menor entero $p > 0$ tal que $\overbrace{1_K + \cdots + 1_K}^{p \ \ veces} = 0$ si existe tal entero. Si no existe decimos que la característica del cuerpo es nula.

Además si un cuerpo K tiene característica p tenemos que para todo $a \in K$

$$p \cdot a = \overbrace{a + \cdots + a}^{p \ \ veces} = (p \cdot 1_K) \cdot a = 0.$$

Si tenemos un cuerpo K con $q = p^r$ elementos, hemos visto en una de las demostraciones anteriores que si consideramos la aplicación $\varphi : \mathbb{Z} \longrightarrow K$ con $\varphi(n) = n \cdot 1_K$, su núcleo es de la forma $\ker(\varphi) = \langle p \rangle$, lo que quiere decir que $\overbrace{1_K + \cdots + 1_K}^{p \ \ veces} = 0$ y que es el mínimo entero mayor que 0 que lo cumple. Por tanto tenemos que la característica de un cuerpo finito de cardinal p^r, con p primo, es p.
Gracias a la característica p de los cuerpos finitos de cardinal p^r, con p primo, tenemos la siguiente propiedad:

Proposición 1.3. *Si $q = p^r$, entonces para cada par de elementos $a, b \in K$, con K cuerpo finito de cardinal q, y cada entero positivo s, se verifica que*

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

Demostración. Vamos a probarlo por inducción:
Para $s = 1$ desarrollamos el término de la izquierda mediante la fórmula del binomio de Newton y tenemos:$(a+b)^p = \sum_{i=0}^{p-1} \binom{p}{i} a^{p-i} b^i$.
Como tenemos que $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$ y p es primo con todo $1 \leq i \leq p-1$ tenemos que $\binom{p}{i}$ es múltiplo de p, y como p es la característica de K, $\binom{p}{i} = 0$ en K, excepto para $i = 0$ e $i = p$ ya que $\binom{p}{0} = \binom{p}{p} = 1$. Con lo cual $(a+b)^p = a^p + b^p$.
Ahora lo suponemos cierto para s, vamos a probarlo para $s+1$. Usando el binomio de Newton, la hipótesis de inducción y lo probado para $s = 1$:
$(a+b)^{p^{s+1}} = ((a+b)^{p^s})^p = (a^{p^s} + b^{p^s})^p = (a^{p^s})^p + (b^{p^s})^p = a^{p^{s+1}} + b^{p^{s+1}}$.
□

Unicidad de los cuerpos finitos

Ya hemos probado la existencia de los cuerpos finitos y que solo existen cuerpos finitos con cardinal $q = p^r$ con p primo y r número natural, lo que nos falta ver es la unicidad, si estos cuerpos que hemos construido son únicos. Vamos a ver que sí, y para ello vamos a probar unos resultados que nos van a ayudar a demostrarlo:

Lema 1.1. *Sea K un cuepo finito contenido, como subcuerpo, en otro cuerpo finito L. Entonces para todo $\alpha \in L$ no nulo, el subconjunto de polinomios de $K[X]$ que tienen α como raiz, no es únicamente el polinomio nulo y coincide con el de múltiplos de un polinomio mónico e irreducible.*

Demostración. L es un espacio vectorial de dimensión finita sobre K, si esta dimensión es r entonces $\{1, \alpha, ..., \alpha^r\}$ es linealmente dependiente sobre K. Una relación de dependencia no trivial nos proporciona un polinomio no nulo que tiene como raíz a α. Sea $f(X)$ el polinomio mónico, no nulo, de grado mínimo (menor o igual a r) que tiene como raíz a α. Como es de grado mínimo $f(X)$ es irreducible, ya que si se diese que $f(X) = f_1(X)f_2(X)$ entonces α tendría que ser raiz de $f_1(X)$ ó de $f_2(X)$ que tienen grado menor que $f(X)$, y esto contradiría que $f(X)$ sea de grado mínimo. Nos falta ver que todo polinomio que tenga a α como raíz es múltiplo de $f(X)$, sea $g(X)$ un polinomio que tiene α como raíz. Realizando la división euclídea, podemos escribir $g(X) = f(X)c(X) + h(X)$, si evaluamos en α para que $g(\alpha) = 0$ necesariamente $h(\alpha) = 0$ y $h(X)$ tiene grado menor que $f(X)$, por tanto $h(X) = 0$ y $g(X)$ en múltiplo de $f(X)$. □

Gracias a este lema podemos definir:

Definición 1.2. El polinomio $f(X)$, cuya existencia y unicidad nos demuestra el lema anterior se denomina polinomio mínimo o irreducible de α sobre K. Lo denotaremos por $\mathrm{Irr}(\alpha, K)$, o si no hay posibilidad de confusión simplemente $\mathrm{Irr}(\alpha)$.

Proposición 1.4. *En un cuerpo finito de q elementos K, todo $a \in K$ verifica que $a^q = a$.*

Demostración. Sabemos que llamamos orden de un grupo G al cardinal de este grupo, y que llamamos orden de x, un elemento de este grupo, al menor entero $n \geq 1$ tal que $x^n = 1_G$. Si denotamos los órdenes por $ord(G)$ y $ord(x)$ por el Teorema de Lagrange tenemos que para todo $x \in G$, $ord(x)|ord(G)$, y entonces para todo $x \in G$, $x^{ord(G)} = 1_G$.
Si esto lo aplicamos ahora al grupo multiplicativo K^* (los elementos no nulos de K), obtenemos que para todo $a \neq 0$ de K, $a^{q-1} = 1_K$, y $a^q = a$. Y si $a = 0$ el enunciado es evidente. □

Corolario 1.2. *El polinomio $X^q - X$ factoriza completamente sobre el cuerpo K de q elementos, es decir,*

$$X^q - X = \prod_{a \in K}(X - a).$$

Demostración. Si consideramos el polinomio $X^q - X$, por lo visto en la proposición anterior, afirmamos que todo $a \in K$ es raiz de este polinomio, con lo cual $\prod_{a \in K}(X - a)|X^q - X$. Como estos dos polinomios tienen el mismo grado y además tienen la misma costante dominante que es 1, deducimos que son iguales. □

Nota 1.1. *La proposición anterior nos muestra que los elementos de K coinciden con las raices del polinomio $X^q - X$ en dicho cuerpo. Esto nos da una definición alternativa de K, como conjunto de raices de este polinomio, pero para que la definición sea la correcta hay que asegurar la existencia de estas raices en algún cuerpo de característica p lo que coduce a la noción de clausura algebraica de $\mathbb{F}_p$ que se define como el más pequeño cuerpo que contenga a este y a las raices de todo polinomio de $\mathbb{F}_p[X]$. De los teoremas de la existencia y unicidad de la clausura algebraica junto con el corolario anterior se deduciría fácilmente la unicidad del cuerpo K.*

Proposición 1.5. *Sea $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado r y sea $q = p^r$. El polinomio $f(X)$ factoriza completamente sobre el cuerpo de q elementos K (es decir, tiene r raíces en K).*

Demostración. Sea el cuerpo con q elementos $\mathbb{F}_p[X]/\langle f(X)\rangle$, y sea x la clase de X en este cuerpo. Como x es una raíz de $f(X)$, entonces $f(X) = \mathrm{Irr}(x, \mathbb{F}_p)$, ya que $f(x) = 0$ implica que $\mathrm{Irr}(x, \mathbb{F}_p)|f(X)$, pero $f(X)$ es irreducible, por tanto tienen que ser iguales. Como x también es raíz de $X^q - X$ por ser un elemento de un cuerpo de cardinal q, por el Lema 1.1, $f(X)|X^q - X$. Dado que $X^q - X$ factoriza completamente en K, ocurre lo mismo para $f(X)$. □

Corolario 1.3. *Sea $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado r y sea $q = p^r$. El cuerpo de q elementos K es isomorfo, como espacio vectorial, al conjunto de expresiones polinomicas $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}$, donde α es una raíz cualquiera de $f(X)$ en K y $a_i \in \mathbb{F}_p$.*

Demostración. Basta probar que el conjunto $\{1, \alpha, ..., \alpha^{r-1}\}$ es una base de K como espacio vectorial sobre $\mathbb{F}_p$. Como el conjunto está formado por r elementos basta con probar que son linealmente independientes, y lo han de ser porque si no: existen $\lambda_i \in \mathbb{F}_p$ no todos nulos, tales que $\sum_{i=0}^{r-1} \lambda_i \alpha^i = 0$, y entonces, si consideramos $g(x) = \sum_{i=0}^{r-1} \lambda_i x^i$, polinomio no nulo ya que no todos los λ_i son nulos, tenemos que $g(\alpha) = 0$ y esto implica que $Irr(\alpha, \mathbb{F}_p) = f(X)|g(X)$ lo cual es absurdo, ya que f tiene grado r y g grado menor o igual a $r-1$. Con lo cual los elementos son linealmente independientes y el conjunto es una base. □

Teorema 1.3. ***(Unicidad de un cuerpo finito)*** *Para toda potencia q de un número primo existe, salvo isomorfismo, un solo cuerpo finito con q elementos.*

Demostración. Sea $q = p^r$ y $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado r. Lo que queremos ver es que el cuerpo K de cardinal q es isomorfo a $\mathbb{F}_p[X]/\langle f(X)\rangle$. Gracias al corolario anterior, tenemos que todos los elementos de K se pueden expresar de la forma $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}$, siendo α una raíz de $f(X)$. Con lo cual el isomorfismo que estamos buscando lo podemos obtener asignando a tal elemento el $a_0 + a_1X + \cdots + a_{r-1}X^{r-1} (\text{mod } f(X))$. □

Notación: Hemos probado que existe un único cuerpo finito de tamaño $q = p^r$, y vamos a denotar este cuerpo único como $\mathbb{F}_q$.

Estructura de los cuerpos finitos

Por último, vamos a estudiar la estructura de los cuerpos finitos.
El cuerpo finito $\mathbb{F}_q$, contiene dos grupos abelianos $(\mathbb{F}_q, +)$ y $(\mathbb{F}_q^*, \cdot)$. Vamos a ver la estructura de ambos.

Teorema 1.4. ***(Estructura aditiva)*** *Si $q = p^r$, el grupo aditivo $(\mathbb{F}_q, +)$ es un producto directo de r grupos cíclicos de orden p:*

$$(\mathbb{F}_q, +) \simeq \mathbb{Z}/\langle p\rangle \times \cdots \times \mathbb{Z}/\langle p\rangle$$

Demostración. Como $\mathbb{F}_q$ es un espacio vectorial sobre $\mathbb{F}_p$, cualquier base induce el isomorfismo anterior. □

Para estudiar la estructura multiplicativa recordamos como ya hemos visto antes en este capítulo que dado un grupo abeliano finito $(G, \cdot)$, el orden de x, un elemento de este grupo, es el menor entero $n \geq 1$ tal que $x^n = 1_G$.

Definición 1.3. Si $(G, \cdot)$ es un grupo abeliano finito, llamaremos exponente de G a $exp(G) := mcm\{ord(x), x \in G\}$.

Por definición, para todo $x \in G$ tenemos que $x^{exp(G)} = 1_G$.
Como ya hemos visto, $ord(x)|ord(G)$, para todo $x \in G$, entonces $exp(G)|ord(G)$ y en particular $exp(G) \leq ord(G)$.
Vamos a tener el siguiente resultado:

Lema 1.2. *Si $(G, \cdot)$ es un grupo abeliano finito existe un elemento $x \in G$ tal que su orden coincide con el exponente de G.*

Demostración. Si descomponemos el exponente de G en producto de primos $exp(G) = p_1^{e_1} \cdots p_m^{e_m}$, afirmamos que para todo i, $1 \leq i \leq m$, por pertenecer $p_i^{e_i}$ a la factorización, existe $x_i \in G$ tal que $ord(x_i) = p_i^{e_i} k_i$ para cierto k_i natural. Tenemos que $x_i^{p_i^{e_i} k_i} = 1$, por tanto, para $y_i = x_i^{k_i}$, el orden de y_i es $p_i^{e_i}$. Ahora si consideramos $x = y_1 \cdots y_m$ tenemos que $ord(x) = p_1^{e_1} \cdots p_m^{e_m} = exp(G)$. □

Teorema 1.5. ***(Estructura multiplicativa)*** *El grupo multiplicativo $(\mathbb{F}_q^*, \cdot)$ es cíclico de orden $q - 1$.*

Demostración. Tenemos que $\mathbb{F}_q^*$ es un grupo de orden $q - 1$, por tanto por lo que hemos visto antes, tenemos que $exp(\mathbb{F}_q^*) \leq q - 1$. Por otra parte, si denotamos $n = exp(\mathbb{F}_q^*)$ por definición n es un múltiplo del orden de cualquier elemento, es decir, que para todo $a \in \mathbb{F}_q^*$, $a^n = 1$, entonces los elementos de el grupo multiplicativo de $\mathbb{F}_q$ son raices del polinomio $X^n - 1$ lo que nos lleva a que $\prod_{a \in \mathbb{F}_q^*}(X - a)|X^n - 1$ y como el primer polinomio tiene grado $q - 1$ y el segundo n llegamos a que $q - 1 \leq n$, y finalmente $n = q - 1$.
Dado que por el lema anterior existe un elemento de orden $q - 1$ el grupo es cíclico. □

Definición 1.4. Llamaremos elemento primitivo de $\mathbb{F}_q$ a todo elemento que genera a $\mathbb{F}_q^*$ como grupo cíclico.

Así, si α es un elemento primitivo de $\mathbb{F}_q$ entonces $\mathbb{F}_q = \{0, \alpha, \alpha^2, ..., \alpha^{q-1} = 1\}$.

Teorema 1.6. *Si $q = p^r$ y α es un elemento primitivo de $\mathbb{F}_q$, entonces $\mathbb{F}_q = \mathbb{F}_p[\alpha]$.*

Demostración. El polinomio mínimo de α debe tener grado r, ya que si este fuera menor por la Proposición 1.5 el polinomio mínimo factorizaría completamente en un cuerpo con menos de q elementos y por tanto sus raíces, incluida α estarán en este cuerpo y α tendría un orden inferior a $q - 1$. Entonces, $\mathbb{F}_p[\alpha]$ tiene al menos q elementos, y como $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_q$ (ya que $\mathbb{F}_p \subseteq \mathbb{F}_q$ y $\alpha \in \mathbb{F}_q$) llegamos a la igualdad. □

Los teoremas que acabamos de ver nos sugieren varias maneras de representar y manejar los elementos de un cuerpo finito:

Representación aditiva: gracias al Teorema 1.4 vemos que los elementos de $\mathbb{F}_q$ se pueden representar como vectores r-dimensionales con coeficientes en $\mathbb{F}_p$, es decir, de la forma $(a_1, a_2, ..., a_r)$ con $a_i \in \{0, 1, ..., p-1\}$. Esta representación permite sumar los elementos fácilmente (coordenada a coordenada módulo p) o multiplicarse escalarmente por un elemento de $\mathbb{F}_p$, pero no permite multiplicar elementos fácilmente.

Representación multiplicativa: gracias al Teorema 1.5 vemos que si α es un elemento primitivo de $\mathbb{F}_q$, entonces $\mathbb{F}_p^* = \{\alpha^i : i = 1, ..., q-1\}$. Esta representación es la más cómoda para la multiplicación de elementos, pero no permite sumar fácilmente y se necesita encontrar un elemento primitivo para utilizarla.

Representación polinómica: el Teorema 1.6 nos permite identificar los elementos de $\mathbb{F}_q$ con expresiones polinómicas en α con grado menor que r y coeficientes en $\{0, 1, ..., p-1\}$. Esta representación nos permite tanto sumar como multiplicar elementos.

Ejemplo 1.1. Sean $p = 2$ y $r = 3$. Si consideramos el cuerpo $\mathbb{F}_2$ y el polinomio de grado 3 $f(x) = x^3 + x + 1$ tenemos que $f(x)$ es irreducible en $\mathbb{F}_2$, ya que al ser de grado 3 basta con comprobar que los elementos de $\mathbb{F}_2$ no anulan al polinomio y en este caso $f(0) = 1$ y $f(1) = 1$.
Por lo visto en el apartado de unicidad de los cuerpos finitos tenemos que $\mathbb{F}_8 \cong \mathbb{F}_2[X]/\langle f(X)\rangle$, y si a es una raíz de dicho polinomio la representación polinómica del cuerpo será:

$$\mathbb{F}_8 = \{0,\ 1,\ a,\ a+1,\ a^2,\ a^2+a,\ a^2+a+1,\ a^2+1\}.$$

Tenemos que $a^3 + a + 1 = 0$, y con esto podemos calcular las potencias de a:

$$a^3 = a + 1, \quad a^4 = a^2 + a, \quad a^5 = a^3 + a^2 = a^2 + a + 1,$$

$$a^6 = a^3 + a^2 + a = a^2 + 1, \quad a^7 = a^3 + a = 1.$$

Vemos entonces que a es un elemento primitivo de $\mathbb{F}_8$, por lo tanto la representación multiplicativa del cuerpo será:

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

Por último, con la representación aditiva los elementos de $\mathbb{F}_8$ se representarían de la forma: $(a_1,\ a_2,\ a_3)$ con $a_i \in \{0, 1\}$, $1 \leq i \leq 3$. Es decir,

$$\mathbb{F}_8 = \{(0,0,0),\ (1,0,0),\ (0,1,0),\ (1,1,0),\ (0,0,1),\ (0,1,1),\ (1,1,1),\ (1,0,1)\}.$$

1.2. Códigos lineales

Ahora introduciremos conceptos sobre los códigos lineales que van a ser necesarios para luego entender y ver cómo funcionan los códigos Reed-Muller.

Definición y parámetros fundamentales

Definición 1.5. Un código lineal $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$ para algún $n \geq 1$.

Los parámetros fundamentales de un código son los que vamos a definir a continuación:

- n es la longitud del código, es decir, el tamaño de las palabras de este código. Si la longitud es n, $\mathcal{C}$ estará en $\mathbb{F}_q^n$.
- k es la dimensión del código, la dimensión como $\mathbb{F}_q$-espacio vectorial, luego su cardinal siempre es una potencia de q, q^k.

Para poder explicar el siguiente parámetro debemos definir antes la distancia de Hamming:

Definición 1.6. Si tenemos dos palabras del código, $x, y \in \mathcal{C}$, $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$, la distancia de Hamming entre x e y es

$$d(x, y) = \sharp\{j : 1 \leq j \leq n, x_j \neq y_j\}.$$

- d es la distancia mínima del código, es decir, el mínimo de la distancia que acabamos de definir entre dos palabras distintas del código: $d = min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}$.

Para abreviar, un código cuyos parámetros son n, k y d se dice que es de tipo $[n, k]$ o $[n, k, d]$.
Asociados a los parámetros fundamentales tenemos otros dos parámetros:

- La redundancia del código, que es $r = n - k$.
- La tasa de transmisión, cuya expresión es $R(\mathcal{C}) = \frac{k}{n}$.

En relación con la distancia de Hamming y la distancia mínima podemos definir el siguiente concepto:

Definición 1.7. Llamamos peso de Hamming de $x \in \mathcal{C}$ y le denotamos $w_H(x)$, al número de dígitos no nulos de x.

Vemos que el peso de Hamming de un elemento x es la distancia de Hamming de x con 0, ya que $w_H(x) = \sharp\{j : 1 \leq j \leq n, x_j \neq 0\} = d(x, 0)$. Esta relación nos permite demostrar:

Lema 1.3. *Si $\mathcal{C}$ es un código lineal de tipo $[n, k, d]$ entonces $d = min\{w_H(c) : c \in \mathcal{C}, c \neq 0\}$.*

Demostración. Si d es la distancia mínima, hay dos palabras distintas $x, y \in \mathcal{C}$ tales que $d = d(x, y)$, también tenemos que $d(x, y) = w_H(x - y)$ y por ser $\mathcal{C}$ un subespacio vectorial $x - y \in \mathcal{C}$, por tanto la distancia mínima es el peso de una palabra. El mínimo de sus pesos a la vez, es la distancia entre el elemento de dicho peso y 0. Con lo cual se cumple la igualdad. □

Matriz generatriz

Si $\mathcal{C}$ es un código lineal de tipo $[n, k]$, es decir, un $\mathbb{F}_q$-espacio vectorial dentro de $\mathbb{F}_q^n$ y de dimensión k, entonces existe una aplicación f, $f : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ lineal e inyectiva donde $\mathcal{C} = \mathrm{Im}(f)$. Podemos entender entonces que f es la aplicación de codificación y que los elementos de $\mathbb{F}_q^k$ es la información que estamos codificando.
A esta aplicación se la puede asociar una matriz $G \in \mathcal{M}_{k\times n}(\mathbb{F}_q)$, y las filas de esta matriz serán una base de $\mathcal{C}$, ya que con esta matriz y los elementos de $\mathbb{F}_q^k$ se puede generar todo el código, es decir, $\mathcal{C} = \{aG : a \in \mathbb{F}_q^k\}$ (escribimos los vectores en forma de filas, no de columnas).

Definición 1.8. Llamamos matriz generatriz del código $\mathcal{C}$ a la matriz $G \in \mathcal{M}_{k\times n}(\mathbb{F}_q)$ asociada a una aplicación lineal e inyectiva $f : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subset \mathbb{F}_q^n$.

Como la base de $\mathcal{C}$ no es única, la matriz generatriz tampoco lo es, pero todas las matrices generatrices de un mismo código tendrán el mismo tamaño $(k \times n)$, el mismo rango (k), y serán semejantes, es decir, si G_1 y G_2 son matrices generatrices de un mismo código existe una matriz inversible P tal que $G_1 = PG_2$.
Por supuesto, distintas matrices generatrices van a estar asociadas a distintas aplicaciones f, y por tanto van a dar lugar a distintas formas de codificar la información.

Ejemplo 1.2. Vamos a considerar el siguiente código de ocho palabras y contenido en $\mathbb{F}_2^4$:

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

Vemos que es un código lineal de longitud 4, y de dimensión 3, el número de palabras como podemos ver es $2^3 = 8$, y la distancia mínima entre sus palabras podemos ver que es 2. Por lo tanto el código es de tipo $[4, 3, 2]$.
Eligiendo tres vectores de $\mathcal{C}$ linealmente independientes podemos obtener una matriz generatriz de este código:

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

Tenemos que el espacio de partida de la aplicación f asociada a esta matriz es $\mathbb{F}_2^3$, entonces multiplicando todos los elementos de este espacio vectorial por la matriz G obtendremos todos los elementos de $\mathcal{C}$. Si cogemos por ejemplo el elemento $(0,\ 1,\ 1)$ la palabra del código que obtendremos es $(0,\ 1,\ 1)\cdot G = (0,\ 1,\ 1,\ 0)$ y será su codificación.

En este ejemplo si en vez de esa base de $\mathcal{C}$ hubiéramos cogido como base los vectores (1 0 0 1), (0 1 0 1) y (0 0 1 1) la matriz habría tenido una forma particular, formada por la identidad 3×3 y una columna a mayores:

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

Vamos a definir a las matrices que son de esta forma:

Definición 1.9. Decimos que una matriz generatriz es de la forma estándar cuando tiene la siguiente forma: $G = (I_k, A)$ donde I_k es la matriz identidad $k \times k$, y A es una matriz $k \times (n-k)$.

Con este tipo de matrices la codificación de una palabra $a \in \mathbb{F}_q^k$ será de la forma (a, z), con $z \in \mathbb{F}_q^{n-k}$. De esta manera, en la palabra resultante tenemos que los k primeros dígitos se encuentra la información y los siguientes son de control. De esta forma la decodificación es mucho más fácil. Este tipo de códigos se llaman *sistemáticos*, es decir, un código es *sitemático* si tiene alguna matriz generatriz con la forma estándar.
No todos los códigos tienen una matriz generatriz estándar, por lo tanto no todos los códigos son sistemáticos, pero con esta definición podremos relacionar los códigos que son sitemáticos y los que no.

Definición 1.10. Diremos que dos códigos $\mathcal{C}_1$ y $\mathcal{C}_2$, de longitud n ambos, son equivalentes si existe una permutación σ de $\{1, ..., n\}$ tal que $\mathcal{C}_2 = \{\sigma(c) : c \in \mathcal{C}_1\}$.

Entonces dos códigos son equivalentes si se diferencian en el orden de sus coordenadas, es decir, si reordenando las columnas de la matriz generatriz de uno de los códigos obtenemos una matriz generatriz del otro. Dos códigos equivalentes además de tener la misma longitud, tienen los mismos parámetros k y d. Recíprocamente, dado un código $\mathcal{C}$,cualquier permutación como la de la definición genera un código equivalente a $\mathcal{C}$.

Proposición 1.6. *Todo código es equivalente a un código sistemático.*

Demostración. Si $\mathcal{C}$ es un código de longitud n y dimensión k su matriz generatriz G tiene dimensión $k \times n$ y tiene rango k, luego tiene k columnas linealmente independientes. Mediante una permutación σ de $\{1, ..., n\}$ podemos tener estas columnas linealmente independientes en la primeras k

posiciones. De esta manera obtenemos $G' = (A, B)$ con A matriz regular $k \times k$. Ahora mediante operaciones elementales, por el método de Gauss, A se puede transformar en la matriz identidad I_k. Realizando estas operaciones en G', obtenemos una matriz en forma estándar que genera por tanto un código sistemático y que es el mismo código que genera G' por lo que es equivalente al generado por G. □

Ejemplo 1.3. Como ya mencionamos, en el ejemplo anterior si hubiéramos escogido otra base podríamos tener como matriz generatriz:

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

Por lo tanto este código es sistemático.
Pero si consideramos el código $\mathcal{C}$ generado por la matriz:

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

tenemos que este código no es sistemático ya que las tres primeras columnas son linealmente dependientes. Pero podemos encontrar un código sistemático al que sea equivalente. Vemos que las columnas 1, 2 y 4 si son linealmente independientes, por lo tanto vamos a elegir la permutación σ siguiente:

$$\sigma(1) = 1,\ \sigma(2) = 2,\ \sigma(3) = 4,\ \sigma(4) = 3.$$

Una matriz generatriz del código resultante de aplicar dicha permutación a $\mathcal{C}$ es:

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Ahora podemos aplicar a esta matriz operaciones elementales hasta obtener una matriz de la forma estándar:

$$G_2 \to \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Matriz control

Ya hemos visto con la matriz generatriz que un código puede describirse mediante un sistema de generadores, pero esta no es la única manera de describir un subespacio de $\mathbb{F}_q^n$, también se puede hacer mediante ecuaciones implícitas. Esta va a ser por tanto otra manera de describir un código, y por lo tanto, vamos a dar la siguiente definición:

Definición 1.11. Una matriz H se dice que es una matriz de control del código $\mathcal{C}$ si es de rango máximo y para todo $x \in \mathbb{F}_q^n$, se verifica que $x \in \mathcal{C}$ si y solo si $Hx^t = \mathbf{0}$.

Esta matriz nos permite saber qué elementos de $\mathbb{F}_q^n$ son palabras del código.
Si $\mathcal{C}$ está definido sobre $\mathbb{F}_q$ y es de tipo $[n, k]$, entonces H está definida en $\mathbb{F}_q$, es de tamaño $(n-k) \times n$ y tiene rango $n-k$, ya que al ser $\mathcal{C}$ un subespacio de $\mathbb{F}_q^n$ de dimensión k, el número de ecuaciones implícitas linealmente independientes necesarias es $n-k$.

Ejemplo 1.4. Si volvemos al Ejemplo 1.2 en el que teníamos como matriz generatriz G, vemos que todos los elementos de este código cumplen que si $(x, y, z, t) \in \mathcal{C}$ entonces $x + y + z + t = 0$ y tenemos también que todos los elementos de $\mathbb{F}_2^4$ que cumplen esta ecuación están en el código, por tanto una matriz de control de este código sería:

$$H = (1\ 1\ 1\ 1)$$

La relación entre la matriz de control y la matriz generatriz va a ser la siguiente:

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

Demostración. Efectuar ambos productos es equivalente a sustituir los vectores de una base de $\mathcal{C}$ en las ecuaciones implícitas de dicho código, lo cual sería igual a 0. □

Si tenemos que G es una matriz generatriz de la forma estándar, es decir, que $G = (I_k, A)$, entonces es fácil ver que la matriz $H = (-A^t, I_{n-k})$ tiene tamaño $(n-k) \times k$, rango $n-k$ y cumple $GH^t = 0$ luego es una matriz de control del código que genera G. Una matriz de control de la forma $H = (B, I_{n-k})$ es una matriz de control de la forma estándar.

Vamos a ver ahora que las matrices de control nos van a poder servir para calcular la distancia mínima de un código.

Lema 1.4. *Si $\mathcal{C}$ es un código lineal y H es su matriz de control entonces: existe una relación de dependencia lineal entre j columnas de H si y sólo si existe una palabra del código de peso j.*

Demostración. Si tenemos una relación de dependencia lineal entre j columnas de H y x es el elemento cuyas coordenadas son los coeficientes de tal combinación lineal tenemos que $Hx^t = 0$ y por lo tanto x está en $\mathcal{C}$ y tenemos que su peso es j.
Recíprocamente, si una palabra x del código tiene peso j esto proporciona (por $Hx^t = 0$) una relación de dependencia lineal entre las j columnas de H correspondientes con las coordenadas no nulas de x. □

Corolario 1.4. *La distancia mínima de un código lineal es el menor número de columnas linealmente dependientes de una matriz de control del código.*

Ejemplo 1.5. Vamos a considerar el código binario $\mathcal{C}$ dado por la siguiente matriz de control:

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

Observando H podemos saber que la longitud del código es 7 y su dimensión 4. La distancia mínima podría ser algo bastante dificil de calcular si no fuera por los resultados que acabamos de ver, gracias a ellos sabemos que como no hay ninguna columna nula en H y ninguna de sus columnas es multiplo de otra entonces $d \geq 3$, y como podemos ver la suma de la primera y la segunda columnas da lugar a la tercera, por tanto hay una relación de dependencia lineal entre tres columnas, con lo que $d = 3$. $\mathcal{C}$ es de tipo $[7, 4, 3]$.
Podemos notar que las columnas de la matriz H son todos los elementos de $\mathbb{F}_2^3$, excepto $(0, 0, 0)$, luego $\mathcal{C}$ es el código binario con dimensión 4 y distancia mínima 3 de mayor longitud posible. Este tipo de códigos se llaman codigos de Hamming binarios, en concreto, $\mathcal{C}$ es un código de Hamming binario de redundancia 3, y se denota $\mathcal{H}_2(3)$.

Dualidad

Si tenemos un código $\mathcal{C}$ y H su matriz de control, como esta tiene rango máximo, podríamos interpretarla como la matriz generatriz de otro código.

Definición 1.12. Dado $\mathcal{C}$ un código lineal con matriz de control H, el código dual de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$, es el código que tiene a H como matriz generatriz.

De esta definición tenemos que:

- Si $\mathcal{C}$ es de tipo $[n, k]$, entonces $\mathcal{C}^\perp$ es de tipo $[n, n-k]$.
- Si G es la matriz generatriz del código $\mathcal{C}$, entonces G es la matriz de control de $\mathcal{C}^\perp$, ya que tiene las dimensiones necesarias y cumple que $GH^t = 0$ y $HG^t = 0$.
- En particular, $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Vamos a recordar ahora algunas nociones de algebra lineal para poder entender mejor la relación entre $\mathcal{C}$ y $\mathcal{C}^\perp$: vamos a considerar sobre $\mathbb{F}_q^n$ la forma bilineal $\bullet$ la cual si $u, v \in \mathbb{F}_q^n$ está definida por:

$$u \bullet v = \sum_{i=1}^{n} u_i v_i$$

Tenemos que dos vectores $u, v \in \mathbb{F}_q^n$ son ortogonales si $u \bullet v = 0$. Con lo cual si tenemos que $S = \{v_1, ..., v_m\}$ es un conjunto de vectores su ortogonal será $S^\perp = \{u \in \mathbb{F}_q^n : u \bullet v_i = 0, \forall i = 1, ..., m\}$. $S^\perp$ es un subespacio vectorial, y si la dimensión de S es k la dimensión de $S^\perp$ es $n - k$. Entonces, si los vectores $v_1, ..., v_k$ son una base de S, los elementos de $S^\perp$ son los u que son solución del sistema del sistema lineal homogéneo con k ecuaciones y n incógnitas: $u \bullet v_i = 0, i = 1, ..., k$.
La intersección de S y su ortogonal puede no ser vacía, ya que puede pasar que si aplicas la forma bilineal sobre un vector y él mismo sea igual a 0, como por ejemplo es el caso de $(1, 1) \in \mathbb{F}_2^2$.
Gracias a este recordatorio podemos enunciar la siguiente proposición:

Proposición 1.8. *Si $\mathcal{C}$ es un código lineal entonces su dual $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$.*

Demostración. Acabamos de ver que los elementos del ortogonal a un conjunto son aquellos elementos que haciendo el producto $\bullet$ con los elementos de la base del conjunto son iguales a 0. Tenemos que los elementos de una base de $\mathcal{C}$ están en G, y los elementos de una base de $\mathcal{C}^\perp$ están en H, así que por $GH^t = 0$ tenemos que $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$. □

Como hemos visto que la intersección de un conjunto con su ortogonal puede no ser vacía tenemos ahora que es posible que $\mathcal{C} \cap \mathcal{C}^\perp \neq \{0\}$. Incluso puede ocurrir que $\mathcal{C} = \mathcal{C}^\perp$, pero para que esto ocurra tiene que darse que la dimensión de ambos sea la misma, es decir $k = n - k$.

Definición 1.13. Un código lineal se dice que es autodual cuando coincide con su código dual.

Capítulo 2

Códigos Reed-Muller

Ahora que ya hemos visto cómo funcionan los cuerpos finitos y los códigos lineales podemos centrarnos en estudiar los códigos Reed-Muller. Los códigos Reed-Muller son una familia infinita de códigos que pertenecen la familia de los códigos de evaluación, y vamos a ver en esta primera sección cómo son estos códigos.
En este capítulo se ha utilizado como referencia [4].

2.1. Códigos de evaluación

Sea $\mathcal{P} = \{P_1, ..., P_n\}$ un conjunto de puntos distintos entre sí que pertenecen a un objeto geométrico $\mathcal{X}$. Si V es un espacio vectorial de funciones $f : \mathcal{X} \to \mathbb{F}_q$, podemos considerar la siguiente aplicación:

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

a la que llamaremos aplicación de evaluación en $\mathcal{P}$.
Esta aplicación es lineal, y su imagen un subespacio vectorial de $\mathbb{F}_q^n$, por tanto, es un código lineal sobre $\mathbb{F}_q$ de longitud n. Las palabras de este código serán cada una de las funciones de V evaluadas por esta aplicación, es decir, los $ev_{\mathcal{P}}(f)$ con $f \in V$. Diremos que el código es obtenido por evaluación en $\mathcal{P}$ de las funciones de V, y sus parámetros pueden deducirse de las propiedades de V excepto la longitud, que depende del número de puntos que haya en $\mathcal{P}$.

Ejemplo 2.1. Si cogemos como conjunto de funciones a evaluar los polinomios en una variable de grado $< k$, y $x_1, ..., x_n$ elementos distintos de $\mathbb{F}_q$ obtenemos un código de evaluación. Estos códigos de evaluación se llaman códigos Reed-Solomon, y son de esta forma:

$$\mathcal{RS}_{k,n} = \{(f(x_1), ..., f(x_n)) \in \mathbb{F}_q^n : f \in \mathbb{F}_q[X], \deg(f) < k\}.$$

Tenemos que una base de los polinomios de grado $< k$ es $\{1, X, X^2, ..., X^{k-1}\}$ y si evaluamos estos polinomios en los elementos $x_1, ..., x_n$ obtendremos una

base del código. Con esta base podemos calcular una matriz generatriz de los códigos Reed-Solomon, que será de esta forma:

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \dots & x_n^{k-1} \end{pmatrix}.$$

En este tipo de códigos vemos que $\mathcal{X} = \mathbb{F}_q$, $\mathcal{P}$ es un subconjunto de $\mathbb{F}_q$ y $V = \{f \in \mathbb{F}_q[X] : \deg(f) < k\}$.
La dimensión de estos códigos es k ya que tenemos que la aplicación de evaluación del código $ev_{\mathcal{P}} : V \longrightarrow \mathbb{F}_q^n$ es lineal e inyectiva. La linealidad está clara, la inyectividad la podemos ver de la siguiente manera: si consideramos $f \in V$ tal que $ev_{\mathcal{P}}(f) = 0$, esto significa que $f(x_1) = ... = f(x_n) = 0$, con lo cual el número de raíces de f es mayor o igual que $n \geq k > \deg(f)$, entonces $f = 0$. Como esta aplicación es inyectiva $\mathcal{RS}_{k,n} = \mathrm{Im}(ev_{\mathcal{P}})$, y esto quiere decir que $\dim(\mathcal{RS}_{k,n}) = \dim(V) = k$.
El último parámetro de estos códigos que nos queda por saber es la distancia mínima. Vamos a ver que $d = n - k + 1$: si consideramos el polinomio $f = (x - x_1) \cdots (x - x_{k-1}) \in V$ tenemos que $ev_{\mathcal{P}}(f) = (0, ..., 0, f(x_k), ..., f(x_n))$, entonces $ev_{\mathcal{P}}(f)$ tiene peso menor o igual que $n - (k - 1) = n - k + 1$, y como $ev_{\mathcal{P}}(f) \neq 0$ esto implica que $d \leq n - k + 1$. Por otro lado, si tenemos un f tal que $f \neq 0$ y $c = ev_{\mathcal{P}}(f) \neq 0$, y $w = w_H(c)$ el número de ceros de f entre $x_1, ..., x_n$ es $n - w$. Como $f \neq 0$, $n - w \leq \deg(f) \leq k - 1$, con lo cual $w \geq n - k + 1$. En conclusión $d = n - k + 1$.
Por tanto alcanzan la cota de Singleton y son MDS, esta cota y la definición de este concepto las podemos encontrar en la sección 2.4 de [3].

Ejemplo 2.2. Para ver otro ejemplo vamos a considerar un código de Hamming binario $\mathcal{H}_2(r)$, ya definimos este tipo de códigos en el Ejemplo 1.5 y vimos que la matriz de control de este código tiene en las columnas todos los elementos de $\mathbb{F}_2^r$ excepto del 0. Entonces, tenemos que $\mathcal{H}_2(r)^{\perp}$ es un código de evaluación, ya que se obtiene de la evaluación de los polinomios de $\mathbb{F}_2[X_1, ..., X_r]$ de grado 1 en los puntos $\mathcal{P} = \mathbb{F}_q^r - \{0\}$, y $\mathcal{X} = \mathbb{F}_q^r$.

2.2. Códigos Reed-Muller

Un caso particular de lo que acabamos de ver tomando $\mathcal{X} = \mathcal{P} = \mathbb{F}_q^m$ y $V = \mathbb{F}_q[X_1, ..., X_m]^{(r)}$, donde $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ denota el conjunto de polinomios de $\mathbb{F}_q[X_1, ..., X_m]$ con grado $\leq r$, son los códigos Reed-Muller. Vamos a ver primero las propiedades del anillo $\mathbb{F}_q[X_1, ..., X_m]$ que se necesitarán más adelante.

Anillo de polinomios $\mathbb{F}_q[X_1, ..., X_m]$

$\mathbb{F}_q[X_1, ..., X_m]$ es como se denota en anillo de polinomios sobre $\mathbb{F}_q$ en las indeterminadas $X_1, ..., X_m$. Un polinomio de este anillo tendrá la siguiente expresión:

$$f(X_1, ..., X_m) = \sum_{i_1 \cdots i_m} a_{i_1 \cdots i_m} X_1^{i_1} \cdots X_m^{i_m}.$$

Donde i_j son números enteros no negativos, $a_{i_1 \cdots i_m} \in \mathbb{F}_q$, y solo una cantidad finita de $a_{i_1 \cdots i_m}$ son no nulos. Si no hay posibilidad de confusión podemos escribir f en lugar de $f(X_1, ..., X_m)$ por simplicidad.

Si evaluamos f en todos los puntos de $\mathbb{F}_q^m$ podemos definir una función, que vamos a denotar también f, $f : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q$ que vamos a llamar función polinómica asociada a f. Si fijamos un orden en los elementos de $\mathbb{F}_q^m$, una forma de describir la función es mediante una tabla en la que a un lado están los elementos de $\mathbb{F}_q^m$ y al otro las evaluaciones de f en esos puntos. Esta tabla se llama tabla de evaluación de f.
Vamos a ver un ejemplo para entender mejor esto:

Ejemplo 2.3. Consideramos el cuerpo $\mathbb{F}_2$, y vamos a establecer en $\mathbb{F}_2^m$ el siguiente orden: un elemento de $\mathbb{F}_2^m$ con coordenadas $(\alpha_1, ..., \alpha_m)$ está en la posición i si $i - 1 = \alpha_1 + 2\alpha_2 + \cdots + 2^{m-1}\alpha_m$. Si $m = 3$ la tabla de evaluación sería la siguiente:

0 0 0	f_1
1 0 0	f_2
0 1 0	f_3
1 1 0	f_4
0 0 1	f_5
1 0 1	f_6
0 1 1	f_7
1 1 1	f_8

Esto significa que $f(0, 0, 0) = f_1$, $f(1, 0, 0) = f_2$, etc.
Si por ejemplo, la función f fuese $f = X_1X_2X_3$, la tabla de evaluación sería:

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

Gracias a estas tablas podemos asociar a cada función f un vector de $\mathbb{F}_q^n$, $\mathbf{f} = (f_1, ..., f_n)$, donde $n = q^m$, ya que estamos evaluando f en todos los elementos de $\mathbb{F}_q^m$. Vamos a poder probar que el recíproco es cierto, es decir, que cada vector proviene de evaluar un polinomio, gracias a lo siguiente:
Si tomamos $V = \mathbb{F}_q[X_1, ..., X_m]$ y $\mathcal{P} = \mathbb{F}_q^m$ podemos considerar la aplicación que definimos al principio de la sección anterior, la aplicación de evaluación en $\mathcal{P}$:

$$ev_{\mathcal{P}} : \mathbb{F}_q[X_1, ..., X_m] \longrightarrow \mathbb{F}_q^n,$$

y tenemos la siguiente proposición:

Proposición 2.1. *La aplicación que acabamos de considerar, $ev_{\mathcal{P}}$ es lineal y sobreyectiva. Y para todo $v \in \mathbb{F}_q^m$ existe un polinomio $F_v \in \mathbb{F}_q[X_1, ..., X_m]$ que cumple:*

1. $F_v(w) = \begin{cases} 1 & \text{si } w = v \\ 0 & \text{si } w \neq v. \end{cases}$

2. $\deg_{X_i}(F_v) \leq q - 1 < q$, *para todo* $i = 1, 2, ..., m$.

Demostración. Que esta aplicación sea lineal es evidente ya que
$ev_{\mathcal{P}}(\lambda f) = (\lambda f(v_1), ..., \lambda f(v_n)) = \lambda(f(v_1), ..., f(v_n)) = \lambda ev_{\mathcal{P}}(f)$ y
$ev_{\mathcal{P}}(f+g) = ((f+g)(v_1), ..., (f+g)(v_n)) = (f(v_1), ..., f(v_n)) + (g(v_1), ..., g(v_n)) = ev_{\mathcal{P}}(f) + ev_{\mathcal{P}}(g)$.
Probemos la sobreyectividad, vamos a definir para todo $v \in \mathbb{F}_q^m$, $v = (\alpha_1, ..., \alpha_m)$ el siguiente polinomio:

$$F_v(X_1, ..., X_m) = \prod_{i=1}^{m} (1 - (X_i - \alpha_i)^{q-1}). \tag{2.1}$$

Vemos que este polinomio va a tomar el valor 1 si lo evaluamos en v ya que el factor $(X_i - \alpha_i)$ se anularía en cada producto y quedaría solo el 1, y si lo evaluamos en $w = (w_1, ..., w_m) \in \mathbb{F}_q^m$ con $w \neq v$, entonces para algún i entre 1 y m, $w_i - \alpha_i \neq 0$ y como $w_i - \alpha_i \in \mathbb{F}_q$, $(w_i - \alpha_i)^{q-1} = 1$ y se anularía en ese i en concreto, y como tenemos que uno de los factores es igual a cero el polinomio seria 0 en este caso. Por tanto la evaluación del polinomio es:

$$F_v(w) = \begin{cases} 1 & \text{si } w = v \\ 0 & \text{si } w \neq v \end{cases}.$$

También vemos que $\deg_{X_i}(F_v) \leq q - 1 < q$, por tanto hemos probado la existencia de un polinomio F_v que cumple las condiciones del enunciado. Además el conjunto $\{ev_{\mathcal{P}}(F_v) : v \in \mathbb{F}_q^m\}$ es la base canónica de $\mathbb{F}_q^n$. Y la linealidad de la aplicación implica, entonces, la sobreyectividad. □

Con esto, ya podemos probar el recíproco.

Proposición 2.2. *Cada elemento de $\mathbb{F}_q^n$ representa una única función polinómica de $\mathbb{F}_q^m$ en $\mathbb{F}_q$.*

Demostración. Por la Proposición 2.1 tenemos que la aplicación $ev_{\mathcal{P}}$ es sobreyectiva. Eso significa que a cada elemento de $\mathbb{F}_q^n$ se le puede asociar un polinomio de $\mathbb{F}_q[X_1, ..., X_m]$ y, por tanto, su función polinómica asociada, que está definida de $\mathbb{F}_q^m$ en $\mathbb{F}_q$.
Esta función es única, ya que si un elemento de $\mathbb{F}_q^n$ está asociado a más de un polinomio por la aplicación $ev_{\mathcal{P}}$ eso significará que las evaluaciones de ambos polinomios en todos los puntos de $\mathbb{F}_q^m$ son iguales, y por tanto, sus funciones asociadas también lo serán, ya que dependen únicamente de las evaluaciones del polinomio. □

Diremos que $\mathbf{f}$ es el vector característico de la función f.
Cuando el cuerpo base es $\mathbb{R}$ o $\mathbb{C}$ distintos polinomios inducen siempre distintas funciones polinómicas, pero, cuando el cuerpo es finito como $\mathbb{F}_q$ existen polinomios que aunque sean distintos inducen las mismas funciones ya que como $a^q = a$, X y X^q inducirán la misma función. Por tanto, en estos cuerpos habrá que considerar el anillo cociente:

$$A = \mathbb{F}_q[X_1, ..., X_m]/\langle X_1^q - X_1, ..., X_m^q - X_m\rangle.$$

Proposición 2.3. *La aplicación de evaluación $ev_{\mathcal{P}}$ se puede definir de A en $\mathbb{F}_q^n$, donde $n = q^m$, y definido así es un isomorfismo de espacios vectoriales sobre $\mathbb{F}_q$.*

Demostración. Primero tenemos que ver que la aplicación $ev_{\mathcal{P}}$ está bien definida, es decir, que si dos polinomios son iguales en A tienen las mismas evaluaciones. Sean f y g dos polinomios iguales en A, entonces $f - g \in \langle X_1^q - X_1, ..., X_m^q - X_m\rangle$, y eso quiere decir que

$$f(X_1, ..., X_m) - g(X_1, ..., X_m) = \sum a_{i_1 \cdots i_m} (X_1^q - X_1)^{i_1} \cdots (X_m^q - X_m)^{i_m}.$$

Pero como para todo $a = (a_1, ..., a_m) \in \mathbb{F}_q^m$ tenemos que $a_i^q = a_i$ para todo i entre 1 y m, entonces $f(a) - g(a) = 0$. Con lo cual las evaluaciones de f y g son iguales para todo elemento de $\mathbb{F}_q$ como queríamos ver.
Probemos ahora la inyectividad, sean f y g dos polinomios en A que tienen la misma imagen con la aplicación $ev_{\mathcal{P}}$, es decir, que tienen las mismas evaluaciones. Vamos a probar que el polinomio $f - g = 0$, y que por tanto, son iguales en A.
Tenemos que $\deg_{X_i}(f - g) < q$ para todo i entre 1 y m, y que para todo $a \in \mathbb{F}_q^m$ $(f - g)(a) = f(a) - g(a) = 0$. Vamos a ver que es igual a 0 por inducción sobre m.
Si $m = 1$ entonces $f - g$ será un polinomio de una sola variable y como se anula en todo $a \in \mathbb{F}_q$ tendremos que tiene $q > deg(f - g)$ raíces, entonces $f - g = 0$.

Supongámoslo cierto para $m-1$, probémoslo para m. Sea $f-g \in \mathbb{F}_q[X_1, ..., X_m]$ si agrupamos los términos con el mismo exponente en X_m tenemos:

$$\begin{aligned}(f-g)(X_1, ..., X_m) = & \, h_0(X_1, ..., X_{m-1}) \\ & + h_1(X_1, ..., X_{m-1})X_m \\ & \vdots \\ & + h_r(X_1, ..., X_{m-1})X_m^r,\end{aligned}$$

donde sabemos que $r < q$ y $h_i(X_1, ..., X_{m-1}) \in \mathbb{F}_q[X_1, ..., X_{m-1}]$ para todo $0 \leq i \leq r$. Si fijamos $(\alpha_1, ..., \alpha_{m-1}) \in \mathbb{F}_q^{m-1}$:

$$\begin{aligned}(f-g)(\alpha_1, ..., \alpha_{m-1}, X_m) = & \, h_0(\alpha_1, ..., \alpha_{m-1}) \\ & + h_1(\alpha_1, ..., \alpha_{m-1})X_m \\ & \vdots \\ & + h_r(\alpha_1, ..., \alpha_{m-1})X_m^r \in \mathbb{F}_q[X_m]\end{aligned}$$

tenemos un polinomio de una variable, que para todo $v \in \mathbb{F}_q$ se anula, por lo que estamos de nuevo en el caso $m = 1$, por tanto $(f-g)(\alpha_1, ..., \alpha_{m-1}, X_m) = 0$, y esto implica que $h_i(\alpha_1, ..., \alpha_{m-1}) = 0$ para todo $0 \leq i \leq r$. Como esto ocurre para todo elemento de $\mathbb{F}_q^{m-1}$ por hipótesis de inducción tenemos que $h_i(X_1, ..., X_{m-1}) = 0$ para todo $0 \leq i \leq r$, con lo que llegamos a $f - g = 0$. Solo nos faltaría probar que la aplicación es sobreyectiva, y por la Proposición 2.1 tenemos que para todo $v \in \mathbb{F}_q^n$ existe un $f \in \mathbb{F}_q[X_1, ..., X_m]$ tal que $ev_{\mathcal{P}}(f) = v$, con lo que queda probado que la aplicación es sobreyectiva. □

Definición 2.1. Si $f \in \mathbb{F}_q[X_1, ..., X_m]$ al polinomio $f^* = \sum b_{j_1 \cdots j_m} X_1^{j_1} \cdots X_m^{j_m}$ que verifica que $0 \leq j_1, ..., j_m \leq q-1$ y que está en la clase de equivalencia de f en A le vamos a llamar polinomio reducido de f.

Corolario 2.1. *Sea $f \in \mathbb{F}_q[X_1, ..., X_m]$. Si $f(v) = 0$ para todo $v \in \mathbb{F}_q^m$ entonces $f^* = 0$.*

Ejemplo 2.4. Si consideramos el cuerpo $\mathbb{F}_2$ para reducir cualquier polinomio f consiste en igualar cada exponente a 1, ya que todo polinomio reducido en $\mathbb{F}_2$ es una suma de monomios en los cuales las potencias de las X_i son o 1 o 0.

Construcción de los códigos

Ya podemos centrarnos en los códigos Reed-Muller y en cómo se construyen estos. Como hemos dicho antes son un caso concreto de los códigos de evaluación considerando $\mathcal{P} = \mathbb{F}_q^m$ y $V = \mathbb{F}_q[X_1, ..., X_m]^{(r)}$, fijamos un orden en los elementos de $\mathbb{F}_q^m$, $\mathbb{F}_q^m = \{v_1, ..., v_n\}$, donde de nuevo tenemos que $n = q^m$, y consideramos la aplicación de evaluación:

$$ev_{\mathcal{P}} : \mathbb{F}_q[X_1, ..., X_m]^{(r)} \longrightarrow \mathbb{F}_q^n, \; ev_{\mathcal{P}}(f) = (f(v_1), ..., f(v_n)).$$

Por la Proposición 2.1 tenemos que la imagen por la aplicación $ev_{\mathcal{P}}$ del espacio vectorial $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ es un subespacio vectorial de $\mathbb{F}_q^n$, y por tanto un código lineal.

Definición 2.2. Un código se dice que es un código de Reed-Muller q-ario de orden r y longitud $n = q^m$ si es la imagen por la aplicación $ev_{\mathcal{P}}$ del espacio vectorial $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$, donde $\mathcal{P} = \mathbb{F}_q^m$. Denotaremos estos códigos como $\mathcal{RM}_q(r, m)$.

$\mathcal{RM}_q(r, m)$ se puede definir de forma alternativa como el conjunto de vectores característicos de los polinomios de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$, ya que si $f \in \mathbb{F}_q[X_1, ..., X_m]^{(r)}$, $ev_{\mathcal{P}}(f)$ es el vector característico de f.
Esta interpretación y el hecho de que $ev_{\mathcal{P}}$ sea sobreyectiva nos llevan a que toda función de $\mathbb{F}_q^m$ en $\mathbb{F}_q$ es polinómica.

Veamos ahora cómo construir una matriz generatriz para estos códigos.

Proposición 2.4. *La matriz que tiene como filas los vectores característicos de los monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ es una matriz generatriz de $\mathcal{RM}_q(r, m)$.*

Demostración. Sabemos que una manera de construir una matriz generatriz de un código es encontrar una base de ese código y colocar los elementos de esa base como filas de la matriz. Tenemos que el conjunto de los monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ forman una base de dicho subespacio, y como hemos visto que $\mathcal{RM}_q(r, m)$ se puede ver como el conjunto de vectores característicos de los elementos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ tenemos que los vectores característicos de la base de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ son un sistema de generadores para estos códigos. Falta probar que son linealmente independientes. Sean $f_1, ..., f_t$ los monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$, si existen $\lambda_1, ..., \lambda_t \in \mathbb{F}_q$ no todos nulos tales que

$$\lambda_1 ev_{\mathcal{P}}(f_1) + \cdots + \lambda_t ev_{\mathcal{P}}(f_t) = 0$$

tendríamos que los vectores característicos de estos monomios son linealmente dependientes, pero entonces

$$\lambda_1 ev_{\mathcal{P}}(f_1) + \cdots + \lambda_t ev_{\mathcal{P}}(f_t) = ev_{\mathcal{P}}(\lambda_1 f_1 + \cdots + \lambda_t f_t) = 0$$

esto significa que el polinomio $\lambda_1 f_1 + \cdots + \lambda_t f_t$ se anula en todo $\mathbb{F}_q^m$ y como es un polinomio reducido por ser suma de monomios reducidos aplicando el Corolario 2.1 tenemos que $\lambda_1 f_1 + \cdots + \lambda_t f_t = 0$ y como teníamos que $f_1, ..., f_t$ son linealmente independientes necesariamente $\lambda_1 = \cdots = \lambda_t = 0$. Con lo cual los vectores característicos de los monomios reducidos son linealmente independientes y forman una base de $\mathcal{RM}_q(r, m)$. □

Corolario 2.2. *Si $r \geq m(q-1)$ entonces $\mathcal{RM}_q(r, m) = \mathbb{F}_q^n$.*

Demostración. Recordamos que un polinomio reducido toma la forma siguiente $\sum b_{j_1 \cdots j_m} X_1^{j_1} \cdots X_m^{j_m}$ tal que $0 \leq j_1, ..., j_m \leq q-1$, con lo cual un polinomio reducido tiene grado $\leq m(q-1)$, por lo tanto, los polinomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$ van a ser los mismos para todo $r \geq m(q-1)$, luego, por lo visto en la proposición anterior, la base de $\mathcal{RM}_q(r, m)$ será la misma para todo $r \geq m(q-1)$, con lo cual el código será el mismo. Y como hemos visto que la aplicación $ev_{\mathcal{P}}$ es sobreyectiva tenemos que para $r \geq m(q-1)$, $\mathcal{RM}_q(r, m) = \mathbb{F}_q^n$. □

Con este corolario vemos que solo tiene sentido considerar los códigos $\mathcal{RM}_q(r, m)$ con $0 \leq r \leq m(q-1)$. Y como tenemos que en $\mathcal{RM}_q(r, m)$ y en $\mathcal{RM}_q(r+1, m)$ la base es la misma salvo que en la segunda se añaden las evaluaciones de los monomios reducidos de grado $r+1$ tenemos la siguiente relación de inclusión:

$$\langle 1 \rangle = \mathcal{RM}_q(0, m) \subsetneq \mathcal{RM}_q(1, m) \subsetneq \cdots \subsetneq \mathcal{RM}_q(m(q-1), m) = \mathbb{F}_q^n.$$

Ejemplo 2.5. Vamos a ver por ejemplo los códigos Reed-Muller con $q = 2$ y $m = 3$, es decir, vamos a ver los códigos Reed-Muller sobre $\mathbb{F}_2$, y los polinomios sobre los que vamos a evaluar son de 3 variables, estos códigos van a tener longitud $2^3 = 8$. Por el corolario que acabamos de ver los monomios reducidos que vamos a tener sobre $\mathbb{F}_2[X_1, X_2, X_3]$ van a ser: 1 (de grado 0), X_1, X_2, X_3 (de grado 1), X_1X_2, X_1X_3, X_2X_3 (de grado 2) y $X_1X_2X_3$ (de grado 3), el resto de monomios de más grado no son monomios reducidos. Entonces $\mathcal{RM}_2(0, 3)$ está generado solo por 1, con lo cual su matriz generatriz será:

$$G = (\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ ).$$

$\mathcal{RM}_2(1, 3)$ estará generado por las evaluaciones de 1, X_1, X_2 y X_3, para obtener la matriz generatriz G tenemos que evaluar estos polinomios en todos los elementos de $\mathbb{F}_2^3$, y vamos a utilizar de orden de evaluación el que utilizamos en el Ejemplo 2.3, con lo cual la matriz generatriz de este código será:

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

$\mathcal{RM}_2(2, 3)$ lo generarán los vectores característicos de 1, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3, por lo tanto evaluándolos en los elementos de $\mathbb{F}_2^3$ obtenemos

la matriz generatriz:

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

Por último, tenemos que $\mathcal{RM}_2(3,3) = \mathbb{F}_2^3$.

Dimensión de los códigos

Vamos a calcular los parámetros de $\mathcal{RM}_q(r,m)$. Sabemos que la longitud de las palabras de este tipo de códigos dependen del número de elementos que evaluemos, y como en los códigos Reed-Muller se evalúan todos los elementos de $\mathbb{F}_q^m$ tenemos que $n = q^m$. Como sabemos que una base son los vectores característicos de los monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$, la dimensión coincidirá con el número de monomios reducidos en $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$. Para poder calcular este valor vamos a necesitar el siguiente lema:

Lema 2.1. *El número de formas de colocar t objetos en m celdas de modo que en ninguna celda haya más de s objetos es*

$$\sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{t - i(s+1) + m - 1}{t - i(s+1)}$$

Demostración. El número de maneras de colocar t objetos en m celdas sin ninguna restricción es

$$\binom{t+m-1}{t}.$$

Mientras que el número de formas de colocar t objetos en m celdas, de las cuales i celdas fijadas tienen al menos $s+1$ objetos, es

$$\binom{t - i(s+1) + m - 1}{t - i(s+1)}.$$

Lo que queremos calcular es el número de formas de colocar t objetos en m celdas de modo que en ninguna celda haya más de s objetos, y esto será igual a calcular el número de formas de colocar t objetos en m celdas menos el número de formas en las que hay más de s objetos en alguna celda. El primer término de esta resta ya lo tenemos, nos falta el segundo.
Si llamamos $A_k = \{$formas de poner t objetos en m celdas con al menos $s+1$ objetos en la k-ésima celda$\}$, tenemos que lo que queremos calcular

es la unión de estos conjuntos desde uno hasta m. Para calcular esta unión podemos utilizar el principio de inclusión-exclusión:

$$|\cup_{j=1}^{m} A_j| = \sum_{i=1}^{m}(-1)^{i+1} \sum_{1\leq k_1<\cdots<k_i\leq m} |A_{k_1}\cap\cdots\cap A_{k_i}|.$$

Por la forma en la que hemos definido a A_k tenemos que $A_{k_1}\cap\cdots\cap A_{k_i}$ son las formas de poner t objetos con al menos $s+1$ objetos en las celdas $k_1, ..., k_i$. Por tanto $\sum_{1\leq k_1<\cdots<k_i\leq m} |A_{k_1}\cap\cdots\cap A_{k_i}|$ será el número de formas de colocar t objetos en m celdas con i celdas con al menos $s+1$ objetos. Esta suma se calculará fijando primero un subconjunto de m de i elementos y después calculando el número de formas de colocar t objetos en m celdas, pero sabiendo que en las i celdas fijadas ponemos $s+1$ objetos en cada una. Con esto llegamos a que el tamaño de la unión de los conjuntos A_k desde uno hasta m es

$$\sum_{i=1}^{m}(-1)^{i+1}\binom{m}{i}\binom{t-i(s+1)+m-1}{t-i(s+1)}.$$

Entonces si al número total de formas le restamos esta unión obtenemos que el número de formas de colocar t objetos en m celdas de modo que en ninguna celda haya más de s objetos es

$$\binom{t+m-1}{t} - \sum_{i=1}^{m}(-1)^{i+1}\binom{m}{i}\binom{t-i(s+1)+m-1}{t-i(s+1)} =$$

$$= \sum_{i=0}^{m}(-1)^{i}\binom{m}{i}\binom{t-i(s+1)+m-1}{t-i(s+1)}.$$

□

Teorema 2.1. *La dimensión de $\mathcal{RM}_q(r,m)$ es*

$$k = \sum_{t=0}^{r}\sum_{i=0}^{m}(-1)^{i}\binom{m}{i}\binom{t-iq+m-1}{t-iq}.$$

Demostración. El número de monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]$ con grado exactamente t, $0 \leq t \leq m(q-1)$, es el número posible de elementos de la forma $(i_1, ..., i_m)$ tales que $0 \leq i_j \leq q-1$ para todo $j = 1, ..., m$ y $i_1 + \cdots + i_m = t$, es decir, el número de formas de colocar t objetos en m celdas de modo que en ninguna haya más de $q-1$ objetos. Por tanto, utilizando el lema anterior, como sabemos que la dimensión de $\mathcal{RM}_q(r,m)$ es el número de monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$, la expresión que obtenemos es la del lema anterior desde que $t=0$ hasta que $t=r$, teniendo en cuenta que $s = q-1$. □

En el caso binario la expresión es más simple:

Corolario 2.3. *La dimensión del código binario $\mathcal{RM}_2(r,m)$ es*

$$k = \sum_{t=0}^{r} \binom{m}{t}.$$

Demostración. En este caso, ya que $q-1=1$ el grado máximo de cada variable va a ser 1, entonces el número de monomios reducidos de grado t es el número de formas posibles de escoger t variables de $X_1, X_2, ..., X_m$, y esto es

$$\binom{m}{t}.$$

□

Dualidad

Ahora vamos a calcular el código dual de un código Reed-Muller y vamos a ver que este código va a ser otro Reed-Muller.

Teorema 2.2. *$\mathcal{RM}_q^{\perp}(r,m) = \mathcal{RM}_q(N-r-1,m)$, donde $N = m(q-1)$.*

Demostración. Por lo visto en la Proposición 1.8 tenemos que el dual de un código es también su ortogonal, por lo tanto queremos ver que $c \bullet v = 0$, siendo $c = ev_{\mathcal{P}}(f)$ y $v = ev_{\mathcal{P}}(g)$, para todo $f \in \mathbb{F}_q[X_1,...,X_m]^{(r)}$, $g \in \mathbb{F}_q[X_1,...,X_m]^{(N-r-1)}$.
Es decir, queremos ver $0 = c \bullet v = \sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v)$.
Cogiendo los polinomios reducidos f^* y g^* en lugar de f y g podemos asumir sin pérdida de generalidad que $\deg_{X_i}(f) < q$, $\deg_{X_i}(g) < q$ para todo $i \in \{1,...,m\}$.
Como son reducidos y definen la misma función de $\mathbb{F}_q^m$ en $\mathbb{F}_q$,

$$f^* \cdot g^* = \sum_{v \in \mathbb{F}_q^m} (fg)(v) \cdot F_v = \sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v) \cdot F_v,$$

son iguales como polinomios.
Sea $\text{coef}(h, X^t)$:= coeficiente de X^t en el polinomio h.
Como $\deg(f \cdot g) = \deg(f) + \deg(g) \leq r + (N-r-1) < m(q-1)$, entonces tenemos que el coeficiente que acompaña a $X_1^{q-1} \cdots X_m^{q-1}$ en el polinomio $f \cdot g$ será 0, ya que sobrepasa el grado del polinomio, con lo cual

$$0 = \text{coef}(f \cdot g, X_1^{q-1} \cdots X_m^{q-1}) = \text{coef}\left(\sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v) \cdot F_v, X_1^{q-1} \cdots X_m^{q-1} \right) =$$

$$= \sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v) \cdot \text{coef}(F_v, X_1^{q-1} \cdots X_m^{q-1}),$$

y si nos fijamos en el polinomio F_v en la ecuación 2.1, podemos ver que $\text{coef}(F_v, X_1^{q-1} \cdots X_m^{q-1}) = (-1)^m$, y sustituyendo en lo anterior

$$0 = (-1)^m \sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v).$$

Por tanto llegamos a $\sum_{v \in \mathbb{F}_q^m} f(v) \cdot g(v) = 0$ que es lo que queríamos ver.
Con esto tenemos que $\mathcal{RM}_q(N - r - 1, m) \subseteq \mathcal{RM}_q^{\perp}(r, m)$.
Para concluir, basta con ver que ambos tienen la misma dimensión, o equivalentemente, que $\dim(\mathcal{RM}_q(N - r - 1, m)) + \dim(\mathcal{RM}_q(r, m)) = n$. Esta comprobación a partir de la fórmula de la dimensión que vimos en el Teorema 2.1 es extremadamente tediosa y extensa, por tanto en lugar de hacer la demostración general, lo demostraremos para el caso $q = 2$. En este caso $N - r - 1 = m(q-1) - r - 1 = m - r - 1$ y por la fórmula de la dimensión para $q = 2$ vista en el Corolario 2.3 :

$$\dim(\mathcal{RM}_2(r, m)) = \sum_{t=0}^{r} \binom{m}{t},$$

$$\dim(\mathcal{RM}_2(m - r - 1, m)) = \sum_{t=0}^{m-r-1} \binom{m}{t} = \sum_{t=0}^{m-r-1} \binom{m}{m-t} = \sum_{j=r+1}^{m} \binom{m}{j}.$$

Entonces, sumando ambas dimensiones y usando la fórmula del binomio de Newton

$$\dim(\mathcal{RM}_2(r, m)) + \dim(\mathcal{RM}_2(m - r - 1, m)) = \sum_{t=0}^{r} \binom{m}{t} + \sum_{j=r+1}^{m} \binom{m}{j} =$$

$$= \sum_{t=0}^{m} \binom{m}{t} = (1+1)^m = 2^m = q^m = n$$

como queríamos ver. □

Capítulo 3

Distancia de los códigos Reed-Muller

Ya hemos visto cuál es la dimensión y la longitud de los códigos Reed-Muller, el parámetro fundamental de este código lineal que nos falta de calcular es la distancia mínima. Vamos a utilizar esta primera sección para hablar del orden y los ideales monomiales, y de las bases de Gröbner, que serán necesarios para poder estudiar y demostrar la cota de Footprint. Esta cota, a la que dedicaremos la segunda sección, nos permitirá estudiar la distancia mínima de estos códigos.
Dos referencias útiles para este capítulo han sido [1] y [2].

3.1. Ideales monomiales y bases de Gröbner

En esta sección vamos a utilizar la siguiente notación: si $\alpha = (\alpha_1, \alpha_2, ..., \alpha_m) \in \mathbb{Z}_{\geq 0}^m$ vamos a denotar con X^α a $X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdots X_m^{\alpha_m} \in \mathbb{F}_q[X_1, ..., X_m]$.
Vamos a comenzar dando la definición de orden monomial:

Definición 3.1. Llamamos orden monomial $>$ sobre $\mathbb{F}_q[X_1, ..., X_m]$ a una relación en $\mathbb{Z}_{\geq 0}^m$, o equivalentemente en el conjunto de monomios X^α con $\alpha \in \mathbb{Z}_{\geq 0}^m$, que satisface:

1. $>$ es un orden total en $\mathbb{Z}_{\geq 0}^m$.
2. Si $\alpha > \beta$ y $\gamma \in \mathbb{Z}_{\geq 0}^m$, entonces $\alpha + \gamma > \beta + \gamma$.
3. $>$ es un buen orden en $\mathbb{Z}_{\geq 0}^m$. Y esto significa que en todo subconjunto no vacío de $\mathbb{Z}_{\geq 0}^m$ existe un mínimo respecto del orden $>$.

Un ejemplo de este tipo de orden es el orden lexicográfico:

Definición 3.2. (Orden lexicográfico) Sean $\alpha = (\alpha_1, ..., \alpha_m)$ y $\beta = (\beta_1, ..., \beta_m)$ en $\mathbb{Z}_{\geq 0}^m$, decimos que $\alpha >_{lex} \beta$ si en la diferencia $\alpha - \beta \in \mathbb{Z}_{\geq 0}^m$ la componente

no nula situada más a la izquierda en el vector es positiva. Y escribiremos $X^\alpha >_{lex} X^\beta$ si $\alpha >_{lex} \beta$.

Vamos a utilizar la siguiente terminología:

Definición 3.3. Sea $f = \sum_\alpha a_\alpha X^\alpha \in \mathbb{F}_q[X_1, ..., X_m]$ un polinomio no nulo, y $>$ un orden monomial. Definimos entonces:

1. El grado total de f es
$$\mathrm{MG}(f) = \mathrm{máx}\{\alpha \in \mathbb{Z}_{\geq 0}^m : a_\alpha \neq 0\}.$$
2. El coeficiente líder de f es
$$\mathrm{LC}(f) = a_{\mathrm{MG}(f)} \in \mathbb{F}.$$
3. El monomio líder de f es
$$\mathrm{LM}(f) = X^{\mathrm{MG}(f)}.$$
4. El término líder de f es
$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Ejemplo 3.1. Si consideramos el polinomio $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$ y el orden lexicográfico tenemos

$$\mathrm{MG}(f) = (3, 0, 0)$$
$$\mathrm{LC}(f) = -5$$
$$\mathrm{LM}(f) = X^3$$
$$\mathrm{LT}(f) = -5X^3$$

El grado total tiene las siguientes propiedades, cuya demostración es elemental.

Lema 3.1. *Sean $f, g \in \mathbb{F}_q[X_1, ..., X_m]$ dos polinomios no nulos. Entonces:*

1. $\mathrm{MG}(f \cdot g) = \mathrm{MG}(f) + \mathrm{MG}(g)$
2. *Si $f + g \neq 0$ entonces $\mathrm{MG}(f + g) \leq \mathrm{máx}(\mathrm{MG}(f), \mathrm{MG}(g))$. Y si $\mathrm{MG}(f) \neq \mathrm{MG}(g)$ se da la igualdad.*

Vamos a introducir también la siguiente definición que será necesaria.

Definición 3.4. Sea I un ideal de $\mathbb{F}_q[X_1, ..., X_m]$. Se define como $V(I)$ a:

$$V(I) = \{(a_1, a_2, ..., a_m) \in \mathbb{F}_q^m : f(a_1, a_2, ..., a_m) = 0, \forall f \in I\}.$$

Sabemos cómo se dividen los polinomios de una variable, pero no cómo es en el caso de los polinomios en varias variables, ni si existe un método para hacerlo. Para saber un poco más sobre ello enunciamos el siguiente teorema:

Teorema 3.1. *(Algoritmo de división) Fijamos un orden monomial $>$ en $\mathbb{Z}_{\geq 0}^m$, y consideramos $F = (f_1, ..., f_s)$ una s-upla de polinomios de $\mathbb{F}_q[X_1, ..., X_m]$. Entonces cada $f \in \mathbb{F}_q[X_1, ..., X_m]$ se puede escribir como*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

donde $a_i, r \in \mathbb{F}_q[X_1, ..., X_m]$, y o bien $r = 0$, o bien r es una combinación lineal, con coeficientes en $\mathbb{F}_q$, de monomios de los cuales ninguno es divisible por $\mathrm{LT}(f_1), ..., \mathrm{LT}(f_s)$.
Llamaremos a r resto de la división por F. Y además, si $a_i f_i \neq 0$, entonces

$$\mathrm{MG}(f) \geq \mathrm{MG}(a_i f_i).$$

La demostración de este teorema y el algoritmo para calcular esta descomposición la podemos encontrar en [1] en la página 64. El resultado de la división no tiene por qué ser único, y va a depender del orden monomial que escojamos.
Ahora vamos a dar una nueva definición para caracterizar los ideales definidos por monomios.

Definición 3.5. Un ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$ es un ideal monomial si existe un subconjunto $A \subset \mathbb{Z}_{\geq 0}^m$ (posiblemente infinito), tal que I está formado por todos los polinomios que son combinaciones lineales finitas de la forma $\sum_{\alpha \in A} h_\alpha X^\alpha$ donde $h_\alpha \in \mathbb{F}_q[X_1, ..., X_m]$. Es decir, I es el ideal generado por los monomios X^α donde $\alpha \in A$, y entonces, el ideal se puede escribir como $I = \langle X^\alpha : \alpha \in A \rangle$.

Podemos caracterizar también los monomios que se encuentran en este ideal:

Lema 3.2. *Sea $I = \langle X^\alpha : \alpha \in A \rangle$ un ideal monomial, entonces el monomio X^β está contenido en I si y sólo si X^β es divisible por X^α para algún $\alpha \in A$.*

Demostración. Si X^β es un múltiplo de X^α entonces por definición de ideal $X^\beta \in I$.
Por otro lado, si $X^\beta \in I$, entonces $X^\beta = \sum_{i=1}^s h_{\alpha(i)} X^{\alpha(i)}$ donde $h_{\alpha(i)} \in \mathbb{F}_q[X_1, ..., X_m]$ y $\alpha(i) \in A$. Como cada $h_{\alpha(i)}$ es una combinación lineal de monomios entonces cada uno de los sumandos se va a poder dividir por un $X^{\alpha(i)}$, y por tanto el término que está en el lado izquierdo de la igualdad también. □

Si tenemos en cuenta que X^β sea divisible por X^α significa que $X^\beta = X^\alpha \cdot X^\gamma$ para algún $\gamma \in \mathbb{Z}_{\geq 0}^m$, y que esto es equivalente a que $\beta = \alpha + \gamma$, entonces

$$\alpha + \mathbb{Z}_{\geq 0}^m = \{\alpha + \gamma : \gamma \in \mathbb{Z}_{\geq 0}^m\}$$

es el conjunto de todos los exponentes de los monomios divisibles por X^α. De esta manera podemos saber qué monomios pueden pertenecer a un ideal monomial.

Ejemplo 3.2. Si $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$ entonces los exponentes de los monomios en I forman el conjunto

$$((4,2) + \mathbb{Z}^2_{\geq 0}) \cup ((3,4) + \mathbb{Z}^2_{\geq 0}) \cup ((2,5) + \mathbb{Z}^2_{\geq 0}).$$

Demostraremos a continuación que, dado un polinomio f, se puede determinar si se encuentra en un ideal monomial observando sus monomios.

Lema 3.3. *Sea I un ideal monomial, y sea $f \in \mathbb{F}_q[X_1, ..., X_m]$. Entonces son equivalentes:*

1. *$f \in I$*
2. *Cada término de f se encuentra en I.*
3. *f es una combinación $\mathbb{F}_q$-lineal de los monomios de I.*

Demostración. Las implicaciones (3) $\Rightarrow$ (2) $\Rightarrow$ (1) son inmediatas por la definición de ideal. Nos falta probar la implicación (1) $\Rightarrow$ (3):
Como $f \in I$ y por ser I ideal monomial $I = \langle X^\alpha : \alpha \in A \rangle$ para un $A \subset \mathbb{Z}^m_{\geq 0}$ podemos escribir f de la forma

$$f = \sum_{i=1}^{s} h_{\alpha(i)} X^{\alpha(i)},$$

donde $h_{\alpha(i)} \in \mathbb{F}_q[X_1, ..., X_m]$ y $\alpha(i) \in A$, y razonando como en la demostración del lema anterior tenemos que cada uno de los sumandos se va a poder dividir por un $X^{\alpha(i)}$, entonces todo término de f se puede dividir por un $X^{\alpha(i)}$ y por el Lema 3.2 están en I. □

Una consecuencia inmediata de la parte (3) del lema es que un ideal monomial está determinado únicamente por sus monomios. Por lo tanto, tenemos el siguiente corolario.

Corolario 3.1. *Dos ideales monomiales son iguales si y sólo si contienen los mismos monomios.*

Ya definimos lo que era el término líder de un polinomio, ahora vamos a definir el término líder de un ideal.

Definición 3.6. Sea $I \subset \mathbb{F}_q[X_1, ..., X_m]$ un ideal distinto de $\{0\}$.

1. Denotamos $\mathrm{LT}(I)$ al conjunto de los términos líderes de los elementos de I. Por tanto,

$$\mathrm{LT}(I) = \{cX^\alpha : \exists f \in I \text{ con } \mathrm{LT}(f) = cX^\alpha\}$$

2. Denotamos $\langle \mathrm{LT}(I) \rangle$ al ideal generado por los elementos de $\mathrm{LT}(I)$.

Decimos que $\langle \mathrm{LT}(I) \rangle$ es el ideal líder de I.

Pero, si tenemos un ideal I, dado por $I = \langle f_1, ..., f_s \rangle$, entonces los ideales $\langle \mathrm{LT}(f_1), ..., \mathrm{LT}(f_s) \rangle$ y $\langle \mathrm{LT}(I) \rangle$ pueden ser diferentes. Es cierto que como $\mathrm{LT}(f_i) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(I) \rangle$, entonces por definición $\langle \mathrm{LT}(f_1), ..., \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(I) \rangle$, sin embargo, la contención puede ser estricta. Para ver que esto puede pasar podemos ver el siguiente ejemplo:

Ejemplo 3.3. Consideramos $I = \langle f_1, f_2 \rangle$, donde $f_1 = X^3 - 2XY$ y $f_2 = X^2Y - 2Y^2 + X$, y el orden lexicográfico.Podemos ver que

$$X \cdot f_2 - Y \cdot f_1 = X(X^2Y - 2Y^2 + X) - Y(X^3 - 2XY) = X^2,$$

entonces como es combinación lineal de f_1 y f_2, $X^2 \in I$. Y por tanto $X^2 = \mathrm{LT}(X^2) \in \langle \mathrm{LT}(I) \rangle$. Sin embargo, tenemos que X^2 no es divisible por $\mathrm{LT}(f_1) = X^3$ ni por $\mathrm{LT}(f_2) = X^2Y$, con lo cual por el Lema 3.2 no puede pertenecer al ideal $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. La contención en este caso, por tanto, vemos que es estricta.

Ahora, vamos a dar una de las definiciones más importantes de esta sección.

Definición 3.7. Fijamos un orden monomial. Sea $I \subset \mathbb{F}_q[X_1, ..., X_m]$ un ideal y $G = \{g_1, ..., g_t\}$ un subconjunto finito de I, se dice que G es una base de Gröbner de I si

$$\langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

Si aplicamos el Lema 3.2 a esta definición vemos que un conjunto $G = \{g_1, ..., g_t\}$ contenido en I es una base de Gröbner de I si y sólo si todos los términos líderes de los elementos de I son divisibles por algún $\mathrm{LT}(g_i)$.

Si volvemos a la cuestión de la división de polinomios de varias variables, recordamos que habíamos visto que el resultado de la división no era único y que podía variar dependiendo del orden monomial que se escogiera, por tanto el resto de la división r también varía dependiendo del orden. Pero ahora que hemos definido las bases de Gröbner podemos ver el siguiente resultado:

Proposición 3.1. *Sea $G = \{g_1, ..., g_t\}$ una base de Gröbner de un ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$, y $f \in \mathbb{F}_q[X_1, ..., X_m]$. Entonces existe un único $r \in \mathbb{F}[X_1, ..., X_m]$ que cumple lo siguiente:*

1. *Ningún término de r es divisible por ningún $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$.*

2. *Existe un $g \in I$ tal que $f = g + r$.*

En particular, r es el resto de la división de f por G, sin importar el orden que se considere en los elementos de G.

Demostración. Sabemos por el Teorema 3.1 que dado un conjunto de polinomios $G = \{g_1, ..., g_t\}$ todo polinomio f se puede escribir como $f = a_1g_1 + \cdots + a_tg_t + r$, donde $a_i, r \in \mathbb{F}_q[X_1, ..., X_m]$, y que r es una combinación lineal de monomios de los cuales ninguno es divisible por ningún $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$, con lo cual tenemos que se cumple (1). Y como el conjunto G es una base de Gröbner del ideal I tenemos que $g = a_1g_1 + \cdots + a_tg_t \in I$, con lo que se cumple también (2).
Nos falta probar la unicidad de r, supongamos que $f = g + r = g' + r'$ y que r' también cumple (1) y (2), entonces tenemos que $r - r' = g' - g$, y como $g', g \in I$ eso quiere decir que $r - r' \in I$, y por lo tanto $\mathrm{LT}(r - r') \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$. Por el Lema 3.2 vemos que $\mathrm{LT}(r - r')$ es divisible por algún $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$. Pero por (2) ningún término de r ni de r' divide a ningún $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$, por tanto $r - r'$ tampoco, con lo cual $\mathrm{LT}(r - r') = 0$ y eso significa que $r - r' = 0$. □

A este resto r a veces se le denomina la forma inicial de f.
Aunque el resto sea único, incluso con las bases de Gröbner, los cocientes a_i no son únicos si se cambia el orden monomial o el orden de $g_1, ..., g_t$.
Como corolario de la proposición que acabamos de ver obtenemos el siguiente criterio para identificar cuándo un polinomio se encuentra en un ideal.

Corolario 3.2. *Sea $G = \{g_1, ..., g_t\}$ una base de Gröbner de un ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$, y $f \in \mathbb{F}_q[X_1, ..., X_m]$. Entonces $f \in I$ si y sólo si el resto de la división de f por G es igual a cero.*

Demostración. Si el resto es cero entonces $f = a_1g_1 + \cdots + a_tg_t$, por lo tanto $f \in I$.
Por el contrario, si $f \in I$ entonces $f = f+0$ cumple (1) y (2) de la Proposición 3.1 por lo tanto el resto de la división de f por G es igual a cero. □

Vamos a utilizar la siguiente notación para el resto.

Definición 3.8. Denotaremos como $\bar{f}^F$ al resto de la división de f por la s-upla $F = (f_1, ..., f_s)$ con un orden fijado.

Ahora, vamos a ver que todos los ideales monomiales de $\mathbb{F}_q[X_1, ..., X_m]$ se generan de forma finita.

Teorema 3.2. *(Lema de Dickson) Sea $I = \langle X^\alpha : \alpha \in A \rangle \subseteq \mathbb{F}_q[X_1, ..., X_m]$ un ideal monomial, entonces podemos escribir I de la forma $I = \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$ donde $\alpha(1), ..., \alpha(s) \in A$. En particular, I tiene un conjunto finito de generadores.*

Demostración. Vamos a probarlo por inducción sobre m, el número de variables.
Si $m = 1$ entonces I está generado por todos los monomios X_1^α con $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Consideramos el elemento más pequeño de A, β, como tenemos que $\beta \leq \alpha$ para todo $\alpha \in A$, entonces X_1^β dividirá al resto de generadores X_1^α. Por tanto, $I = \langle X_1^\beta \rangle$.
Supongámoslo cierto para $m-1$, probémoslo para m. Vamos a escribir las variables como $X_1, ..., X_{m-1}, Y$, de modo que los monomios de $\mathbb{F}_q[X_1, ..., X_{m-1}, Y]$ se pueden escribir de la forma $X^\alpha Y^n$, donde $\alpha = (\alpha_1, ..., \alpha_{m-1}) \in \mathbb{Z}_{\geq 0}^{m-1}$ y $n \in \mathbb{Z}_{\geq 0}$.
Supongamos que $I \subset \mathbb{F}_q[X_1, ..., X_{m-1}, Y]$ es un ideal monomial, para encontrar sus generadores vamos a considerar J, el ideal de $\mathbb{F}_q[X_1, ..., X_{m-1}]$ tal que $X^\alpha \in J$ si $X^\alpha Y^n \in I$ para algún $n \in \mathbb{Z}_{\geq 0}$. J es un ideal monomial de $\mathbb{F}_q[X_1, ..., X_{m-1}]$, así que por hipótesis de inducción tenemos que J está finitamente generado por monomios, lo que significa que ponemos escribir $J = \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$. J se puede entender como una "proyección" de I en $\mathbb{F}_q[X_1, ..., X_{m-1}]$.
Para cada i entre 1 y s, por definición de J tenemos que $X^{\alpha(i)} Y^{n_i} \in I$ para algún $n_i \geq 0$. Sea n el mayor de todos los n_i y, para todo k entre 0 y $n-1$, consideramos el ideal $J_k \subset \mathbb{F}_q[X_1, ..., X_{m-1}]$, generado por todos los monomios X^β tales que $X^\beta Y^k \in I$. Usando de nuevo la hipótesis de inducción, tenemos que $J_k = \langle X^{\alpha_k(1)}, ..., X^{\alpha_k(s_k)} \rangle$.
Podemos comprobar que I está generado por la siguiente lista de monomios:

$$\begin{gathered}
\text{De } J \text{ obtenemos: } X^{\alpha(1)} Y^n, ..., X^{\alpha(s)} Y^n. \\
\text{De } J_0 \text{ obtenemos: } X^{\alpha_0(1)}, ..., X^{\alpha_0(s_0)}. \\
\text{De } J_1 \text{ obtenemos: } X^{\alpha_1(1)} Y, ..., X^{\alpha_1(s_1)} Y. \\
\vdots \\
\text{De } J_{n-1} \text{ obtenemos: } X^{\alpha_{n-1}(1)} Y^{n-1}, ..., X^{\alpha_{n-1}(s_{n-1})} Y^{n-1}.
\end{gathered}$$

Vamos a ver que cada monomio de I es divisible por algún elemento de la lista: sea $X^\alpha Y^p \in I$. Si $p \geq n$ tenemos que Y^p es divisible por Y^n ya que son dos monomios de una sola variable, y como $X^\alpha Y^p \in I$ por definición de J, $X^\alpha \in J$, y como $J = \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$, X^α es divisible por algún $X^{\alpha(i)}$. Por tanto $X^\alpha Y^p$ es divisible por $X^{\alpha(i)} Y^n$, que está en la lista.
Si $p \leq n-1$, como tenemos que $X^\alpha Y^p \in I$ por definición de J_p, $X^\alpha \in J_p$, y como $J_p = \langle X^{\alpha_p(1)}, ..., X^{\alpha_p(s_p)} \rangle$, X^α es divisible por algún $X^{\alpha_p(j)}$. Entonces $X^\alpha Y^p$ es divisible por $X^{\alpha_p(j)} Y^p$, que está en la lista.
Con esto por el Lema 3.2 deducimos que que los monomios anteriores generan un ideal que tiene los mismos monomios que I, y por el Corolario 3.1 los ideales tienen que ser los mismos.
Para completar la demostración, si volvemos a escribir las variables como $X_1, ..., X_m$, nos falta probar que I está finitamente generado por monomios X^α tales que $\alpha \in A$. Acabamos de ver que $I = \langle X^{\beta(1)}, ..., X^{\beta(s)} \rangle$

para $X^{\beta(i)} \in I$. Como para todo $0 \leq i \leq s$, $X^{\beta(i)} \in I = \langle X^{\alpha} : \alpha \in A \rangle$ entonces por el Lema 3.2, $X^{\beta(i)}$ es divisible por $X^{\alpha(i)}$ con $\alpha(i) \in A$ para todo i. Esto implica que $X^{\beta(i)} \in \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$ para todo i, y esto nos lleva a que $\langle X^{\beta(1)}, ..., X^{\beta(s)} \rangle \subset \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$. Y como tenemos que $\langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle \subset I = \langle X^{\beta(1)}, ..., X^{\beta(s)} \rangle$, llegamos finalmente a que $I = \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$ con $\alpha(1), ..., \alpha(s) \in A$. □

Ejemplo 3.4. Vamos a aplicar el mecanismo utilizado en la demostración al ideal $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$ para poder así entender mejor la demostración. En este caso podemos ver que $J = \langle X^2 \rangle$, y como el único monomio de I que tiene a X^2 como producto es X^2Y^5, entonces el n que tomábamos en la demostración en este ejemplo es $n = 5$. Entonces calculamos J_0, J_1, J_2, J_3 y J_4

$$J_0 = J_1 = \{0\}.$$

Ya que en I no hay ningún término que no contenga a Y, ningún término de la forma $X^{\alpha}Y$.

$$J_2 = J_3 = \langle X^4 \rangle.$$

Ya que $X^4Y^2 \in I$ y $X^4Y^3 \in I$ también ya que X^4Y^3 es divisible por X^4Y^2.Por último

$$J_4 = \langle X^3 \rangle.$$

Entonces, siguiendo la prueba del teorema tenemos que

$$I = \langle X^4Y^2, X^4Y^3, X^3Y^4, X^2Y^5 \rangle.$$

Este teorema nos da una manera de describir a los ideales monomiales ya que nos asegura que todos ellos van a tener un conjunto de generadores finito. También nos da una manera de comprobar si un polinomio f está en un ideal o no, ya que si el ideal es de la forma $I = \langle X^{\alpha(1)}, ..., X^{\alpha(s)} \rangle$, f estará en el ideal si al dividirlo por $X^{\alpha(1)}, ..., X^{\alpha(s)}$ el resto es cero.
Con esto que hemos visto, si ahora probamos que $\langle \mathrm{LT}(I) \rangle$ es un ideal monomial tendremos que se genera a partir de un número finito de monomios, y nos va a interesar ver si estos monomios son términos líder de algunos elementos.

Proposición 3.2. *Sea $I \subset \mathbb{F}_q[X_1, ..., X_m]$ un ideal. Entonces se cumple:*

1. *$\langle \mathrm{LT}(I) \rangle$ es un ideal monomial.*
2. *Existen $g_1, ..., g_t \in I$ tales que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$.*

Demostración. Primero vamos a probar (1). Los monomios líderes de los elementos $g \in I - \{0\}$ forman un ideal monomial $\langle \mathrm{LM}(g) : g \in I - \{0\} \rangle$. Como $\mathrm{LM}(g)$ y $\mathrm{LT}(g)$ difieren solamente en una constante distinta de cero, ambas generan los mismos ideales, por tanto $\langle \mathrm{LT}(g) : g \in I - \{0\} \rangle = \langle \mathrm{LT}(I) \rangle$ es un ideal monomial.

A continuación probamos (2). Como $\langle \mathrm{LT}(I)\rangle$ está generado por los monomios $\mathrm{LM}(g)$ con $g \in I - \{0\}$, por el Teorema 3.2 tenemos que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), ..., \mathrm{LM}(g_t)\rangle$ para un número finito de $g_1, ..., g_t \in I$. Como $\mathrm{LM}(g_i)$ y $\mathrm{LT}(g_i)$ difieren solo de una constante no nula, generan los mismos ideales, por tanto, $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)\rangle$. □

Esta proposición nos dice que todo ideal tiene una base de Gröbner, ya que los elementos $g_1, ..., g_t$ cumplen la definición.
Ahora podemos utilizar la proposición que acabamos de probar y el algoritmo de división para probar la existencia de un conjunto finito de generadores en cada ideal polinomial.

Teorema 3.3. *(Teorema de la base de Hilbert) Todo ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$ tiene un conjunto de generadores finito, es decir, $I = \langle g_1, ..., g_t\rangle$, donde $g_1, ..., g_t \in I$.*

Demostración. Si $I = \{0\}$ tomamos como conjunto generador $\{0\}$ que es finito.
Si I contiene un polinomio no nulo vamos a ver cómo encontrar el conjunto de generadores finito de I. Por la Proposición 3.2, hemos visto que existen $g_1, ..., g_t \in I$ tal que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)\rangle$, vamos a probar que estos $g_1, ..., g_t$ son los generadores de I.
Es claro que $\langle g_1, ..., g_t\rangle \subset I$ ya que cada $g_i \in I$. Nos falta ver la otra contención, sea $f \in I$ un polinomio, si dividimos f entre $(g_1, ..., g_t)$ por el Teorema 3.1 podemos obtener la siguiente expresión

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

donde r no tiene ningún término divisible por ningún $\mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)$ o es igual a 0. Pero tenemos que

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I$$

entonces como está en I, $\mathrm{LT}(r) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t)\rangle$, y por el Lema 3.2, $\mathrm{LT}(r)$ es divisible por algún $\mathrm{LT}(g_i)$, con lo cual, necesariamente $r = 0$. Por tanto

$$f = a_1 g_1 + \cdots + a_t g_t \in \langle g_1, ..., g_t\rangle.$$

Esto implica que $I \subset \langle g_1, ..., g_t\rangle$, y se llega a $I = \langle g_1, ..., g_t\rangle$. □

Con este resultado acabamos de ver que una base de Gröbner nos da unos generadores para el ideal. Con lo cual tenemos el siguiente corolario:

Corolario 3.3. *Fijado un orden monomial, todo ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$ no nulo tiene una base de Gröbner. Además, cualquier base de Gröbner para un ideal I es un conjunto de generadores para I.*

Demostración. La Proposición 3.2 nos dice que para todo ideal existen $g_1, ..., g_t \in I$ tales que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$, y el conjunto $G = \{g_1, ..., g_t\}$ cumple exactamente con la definición de base de Gröbner.
Para probar la última afirmación, basta ver que si tenemos $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$ utilizando los razonamientos que hemos utilizado en la demostración del Teorema 3.3 llegamos a que $I = \langle g_1, ..., g_t \rangle$, con lo que la base de Gröbner G es un conjunto de generadores para I. □

3.2. Cota de footprint

En esta sección vamos a probar la cota de footprint, que es una cota superior en el número de ceros de un polinomio de varias variables, y que nos va a servir para en la siguiente sección calcular la distancia mínima de los códigos Reed-Muller.
Vamos a considerar un ideal $I \subset \mathbb{F}_q[X_1, ..., X_m]$ y el conjunto $V(I)$ que recordamos que lo definimos en la sección anterior como los elementos de $\mathbb{F}_q^m$ que anulan a todos los polinomios contenidos en I. La cota de footprint va a consistir en dar una cota para el cardinal de este conjunto.
Para poder dar esta cota vamos a necesitar antes la siguiente proposición.

Proposición 3.3. *Sea $I \subset \mathbb{F}_q[X_1, ..., X_m]$ un ideal, y consideramos el conjunto $\Delta(I) = \{X^\alpha : X^\alpha \notin \mathrm{LT}(I)\}$. Entonces la aplicación*

$$\phi : \mathbb{F}_q[X_1, ..., X_m]/I \longrightarrow \langle \Delta(I) \rangle_{\mathbb{F}_q}$$

dada por $\phi(f + I) = \bar{f}^G$, donde G es una base de Gröbner de I, está bien definida y es un isomorfismo de espacios vectoriales sobre $\mathbb{F}_q$.

Demostración. Primero vamos a ver que la aplicación ϕ está bien definida. Sabemos que los restos de una división por una base de Gröbner son únicos, lo que tenemos que ver es que si f y g están en la misma clase de equivalencia en $\mathbb{F}_q[X_1, ..., X_m]/I$ entonces tienen el mismo resto. Si f y g están en la misma clase de equivalencia tenemos que $f - g \in I$, y por el algoritmo de división $f = f' + r_1$ y $g = g' + r_2$ donde r_1 y r_2 son los restos, entonces $r_1 - r_2 = (f - g) - f' + g' \in I$ ya que $f - g$ está en I y f' y g' también están en I. Pero esto implica que si $G = \{g_1, ..., g_t\}$, algún $\mathrm{LT}(g_i)$ divide a $\mathrm{LT}(r_1 - r_2)$, lo cual es absurdo porque ninguno de los monomios de r_1 ni de r_2 es divisible por ninguno de los $\mathrm{LT}(g_i)$ para todo i entre 1 y t. Por tanto, necesariamente $r_1 - r_2 = 0$, y llegamos a que $r_1 = r_2$.
La aplicación es $\mathbb{F}_q$−lineal, ya que si $f = f' + r_1$ y $g = g' + r_2$ donde r_1 y r_2 son los restos de la división por G, para todo $\lambda_1, \lambda_2 \in \mathbb{F}_q$ tenemos que $\lambda_1 f + \lambda_2 g = \lambda_1 f' + \lambda_2 g' + \lambda_1 r_1 + \lambda_2 r_2$, y $\lambda_1 r_1 + \lambda_2 r_2$ tiene que ser el resto.
Para probar finalmente que es isomorfismo, vamos a considerar la aplicación

$$\varphi : \langle \Delta(I) \rangle_{\mathbb{F}_q} \longrightarrow \mathbb{F}_q[X_1, ..., X_m]/I$$

dada por $\varphi(f) = f + I$, y vamos a ver que es su inversa. Si $f \in \langle \Delta(I) \rangle_{\mathbb{F}_q}$ entonces $\bar{f}^G = f$ ya que $f = 0 + f$, $0 \in I$ y ningún monomio de f es divisible por ninguno de los $\mathrm{LT}(g_i)$. Entonces $\phi(\varphi(f)) = f$. Por otra parte, $\varphi(\phi(f + I)) = f + I$ puesto que $f = f' + \bar{f}^G$ y como $f' \in I$ entonces $\bar{f}^G + I = f + I$.
Con lo que tenemos que es un isomorfismo. □

Ahora podemos probar la cota.

Teorema 3.4. *(Cota de footprint) Sea $I \subset \mathbb{F}_q[X_1, ..., X_m]$ un ideal, entonces se cumple que*

$$|V(I)| \leq |\Delta(I)|.$$

Demostración. Para esta prueba vamos a considerar la aplicación

$$\varepsilon : \mathbb{F}_q[X_1, ..., X_m] \longrightarrow \mathbb{F}_q^{|V(I)|}$$

dada por $\varepsilon(f) = (f(a))_{a \in V(I)}$, es decir, las evaluaciones de los polinomios en los elementos de $V(I)$. Tenemos que la aplicación es $\mathbb{F}_q-$lineal, y vemos por la definición de $V(I)$ que $I \subseteq \ker(\varepsilon)$. Entonces, por el Teorema de isomorfía existe una aplicación

$$\bar{\varepsilon} : \mathbb{F}_q[X_1, ..., X_m]/I \longrightarrow \mathbb{F}_q^{|V(I)|}$$

tal que $\bar{\varepsilon}(f + I) = (f(a))_{a \in V(I)}$, para todo $f \in \mathbb{F}_q[X_1, ..., X_m]$.
Vamos a ver que está bien definida. Si f y g están en la misma clase de equivalencia, entonces $f - g \in I$, esto implica que $(f - g)(a) = 0$ para todo $a \in V(I)$, con lo cual $f(a) = g(a)$ para todo $a \in V(I)$, es decir, $(f(a))_{a \in V(I)} = (g(a))_{a \in V(I)}$.
También tenemos que es sobreyectiva, ya que por la Proposición 2.1 para todo $v \in \mathbb{F}_q^{|V(I)|}$, existe $f \in \mathbb{F}_q[X_1, ..., X_m]$ tal que $(f(a))_{a \in V(I)} = v$.
Por tanto, $\dim(\mathbb{F}_q^{|V(I)|}) \leq \dim(\mathbb{F}_q[X_1, ..., X_m]/I)$. Por la Proposición 3.3 tenemos que como ϕ es un isomorfismo $\dim(\mathbb{F}_q[X_1, ..., X_m]/I) = \dim(\langle \Delta(I) \rangle_{\mathbb{F}_q})$, y $\dim(\langle \Delta(I) \rangle_{\mathbb{F}_q}) = |\Delta(I)|$ porque los monomios son $\mathbb{F}_q-$linealmente independientes. Con lo cual

$$|V(I)| = \dim(\mathbb{F}_q^{|V(I)|}) \leq \dim(\mathbb{F}_q[X_1, ..., X_m]/I) = \dim(\langle \Delta(I) \rangle_{\mathbb{F}_q}) = |\Delta(I)|$$

llegando así a la desigualdad que queríamos probar. □

3.3. Distancia mínima

Queremos calcular la distancia mínima de $\mathcal{RM}_q(r, m)$ que, como sabemos, es el mínimo de los pesos de Hamming de las palabras del código. También sabemos que el peso de una palabra es el número de sus coordenadas menos el número de ellas que son nulas. Como estas palabras vienen

de la evaluaciones de un polinomio estaremos restando al número total de evaluaciones el número de ceros del polinomio. Acabamos de ver en la sección anterior la cota de footprint, que es una cota sobre el número de ceros de un ideal de polinomios, y que nos va a ayudar a demostrar el teorema que nos va a dar el valor de la distancia mínima.
Para poder demostrar ese teorema también va a ser necesario el siguiente lema.
El Lema 3.4 y el Teorema 3.5 que vamos a enunciar y demostrar a continuación los hemos cogido del artículo [2].

Lema 3.4. *Sean $q, m, r \in \mathbb{N}$ tales que $0 \leq r \leq m(q-1)$. Consideramos $(i_1, ..., i_m) \in \mathbb{N}_0^m$ que cumplen que $i_1, ..., i_m < q$, y $i_1 + \cdots + i_m \leq r$.Entonces el mínimo valor de $\prod_{l=1}^{m}(q - i_l)$ es $(q-b)q^{m-a-1}$, donde $a, b \in \mathbb{N}_0$ satisfacen que $r = a(q-1) + b$, con $0 \leq b \leq q-1$.*

Demostración. Para que $\prod_{l=1}^{m}(q - i_l)$ sea lo más pequeño posible bajo las condiciones $i_1, ..., i_m \in \mathbb{N}_0$, $i_1, ..., i_m < q$, y $i_1 + \cdots + i_m \leq r$, claramente vamos a tener que $i_1 + \cdots + i_m = r$. Entre las $m-$uplas $(i_1, ..., i_m)$ que hacen que $\prod_{l=1}^{m}(q - i_l)$ tengan su valor mínimo podemos elegir, gracias a su simetría, aquella que cumple que $i_1 \geq \cdots \geq i_m$. Si elegimos $(i_1, ..., i_m)$ de esta manera no puede haber ningún $t \in \{1, ..., m-1\}$ tal que $0 < i_t < q-1$ y $0 < i_{t+1} < q-1$, ya que si lo hubiese tendríamos que

$$(q-i_1)\cdots(q-i_{t-1})(q-(i_t+1))(q-(i_{t+1}-1))(q-i_{t+2})\cdots(q-i_m) < \prod_{l=1}^{m}(q-i_l),$$

y como la upla $(i_1, ..., i_{t-1}, i_t+1, i_{t+1}-1, i_{t+2}, ..., i_m)$ también cumple las condiciones necesarias, esto entra en contradicción con que $\prod_{l=1}^{m}(q - i_l)$ tiene el mínimo valor posible. Con lo cual, si $i_t < q-1$ entonces $i_{t+1} = 0$. Escribiendo r como en el enunciado, $r = a(q-1) + b$, llegamos a que la única opción es $i_1 = \cdots = i_a = q-1$, $i_{a+1} = b$, y $i_{a+2} = \cdots = i_m = 0$. Sustituyendo por esos valores nos queda que $(q-b)q^{m-a-1}$ es el mínimo valor de $\prod_{l=1}^{m}(q - i_l)$. □

Vamos a definir ahora un orden que es el que vamos a utilizar en el siguiente teorema.

Definición 3.9. Decimos que $X_1^{\alpha_1} \cdots X_m^{\alpha_m} \prec_t X_1^{\beta_1} \cdots X_m^{\beta_m}$ con el orden lexicográfico graduado, si $(\alpha_1, ..., \alpha_m) \neq (\beta_1, ..., \beta_m)$ y $\alpha_1 + \cdots + \alpha_m < \beta_1 + \cdots + \beta_m$, o si $\alpha_1 + \cdots + \alpha_m = \beta_1 + \cdots + \beta_m$ y la primera coordenada distinta de cero de $(\beta_1 - \alpha_1, ..., \beta_m - \alpha_m)$ es positiva.

Teorema 3.5. *Dado $r \in \mathbb{N}_0$, con $0 \leq r \leq m(q-1)$, escribimos $r = a(q-1) + b$, con $a, b \in \mathbb{N}_0$ y $0 \leq b \leq q-1$. Entonces la distancia mínima de $\mathcal{RM}_q(r, m)$ es $(q-b)q^{m-a-1}$.*

Demostración. Como acabamos de comentar la distancia mínima de $\mathcal{RM}_q(r,m)$ es el mínimo de los pesos de Hamming de las palabras del código. Si tenemos el polinomio $F \in \mathbb{F}_q[X_1,...,X_m]$, que cumple $\deg(F) \leq r$ y $\deg_{X_i}(F) < q$, para todo i, $0 \leq i \leq m$, y enumeramos los elementos de $\mathbb{F}_q^m$ como $\{a_1, a_2, ..., a_{q^m}\}$, tendremos que la palabra dada por $c = (F(a_1), ..., F(a_{q^m})) \in \mathbb{F}_q^{q^m}$ tendrá peso $w_H(c) = q^m - |V(F)|$ ya que q^m es el número de puntos que se evalúan y $|V(F)|$ el número de ceros del polinomio F. Por tanto, la distancia mínima es

$$d = \text{mín}\{q^m - |V(F)| : \deg(F) \leq r, \deg_{X_i}(F) < q,\ \forall i, 0 \leq i \leq m\}$$

$$= q^m - \text{máx}\{|V(F)| : \deg(F) \leq r, \deg_{X_i}(F) < q,\ \forall i, 0 \leq i \leq m\}.$$

Así que tenemos que acotar $|V(F)|$. Por la definición de $V(\langle F\rangle)$ tenemos que $|V(F)| = |V(\langle F\rangle)|$, y como los polinomios $X_1^q - X_1, ..., X_m^q - X_m$ se anulan en todo $\mathbb{F}_q^m$ entonces $|V(\langle F\rangle)| = |V(\langle F, X_1^q - X_1, ..., X_m^q - X_m\rangle)|$. Aplicando la Cota de footprint 3.4

$$|V(F)| = |V(\langle F, X_1^q - X_1, ..., X_m^q - X_m\rangle)|$$

$$\leq |\Delta(\langle F, X_1^q - X_1, ..., X_m^q - X_m\rangle)|$$

$$\leq |\Delta(\langle \text{LM}(F), X_1^q, ..., X_m^q\rangle)|,$$

esta última desigualdad se debe a que $\Delta(\langle F, X_1^q - X_1, ..., X_m^q - X_m\rangle) \subseteq \Delta(\langle \text{LM}(F), X_1^q, ..., X_m^q\rangle)$. Si escribimos $\text{LM}(F) = X_1^{i_1} \cdots X_m^{i_m}$, tenemos

$$|\Delta(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, ..., X_m^q\rangle)| = q^m - \prod_{l=1}^{m}(q - i_l).$$

Entonces

$$d \geq q^m - \text{máx}\{q^m - \prod_{l=1}^{m}(q - i_l) : i_1 + \cdots + i_m \leq r,\ i_1, ..., i_m < q\} =$$

$$= q^m - q^m + \text{mín}\{\prod_{l=1}^{m}(q - i_l) : i_1 + \cdots + i_m \leq r,\ i_1, ..., i_m < q\}.$$

Por el Lema 3.4, $d \geq (q-b)q^{m-a-1}$.
Si ahora encontramos una palabra que tenga este peso tendremos la igualdad. Si escribimos $\mathbb{F}_q = \{a_1, ..., a_q\}$ tenemos que el polinomio $\prod_{l=1}^{m}\prod_{n=1}^{i_l}(X_l - a_n)$ tiene como monomio líder $X_1^{i_1} \cdots X_m^{i_m}$ y tiene exactamente $q^m - \prod_{l=1}^{m}(q - i_l)$ ceros. Si tomamos los i_l que minimizan $\prod_{l=1}^{m}(q - i_l)$ tendremos que de nuevo por el Lema 3.4 la palabra dada por este polinomio tiene peso $(q - b)q^{m-a-1}$. □

Capítulo 4

Descodificación de los códigos Reed-Muller

En este capítulo, estudiaremos un algoritmo de corrección de errores para códigos Reed-Muller. Vamos a centrarnos en la descodificación para códigos Reed-Muller binarios, por lo que en los siguientes apartados vamos a considerar $q = 2$.
La referencia en la que se ha basado este capítulo es [4].
En esta primera sección vamos a introducir unos conceptos que vamos a necesitar para el algoritmo de descodificación.

4.1. Geometrías finitas

Consideramos un polinomio reducido f de $\mathbb{F}_2[X_1, ..., X_m]$, si escribimos los elementos de $\mathbb{F}_2^m$ como $\{v_1, ..., v_n\}$ teniendo de nuevo que $n = q^m = 2^m$, y $\mathbf{f} = (f_1, ..., f_n)$ es el vector característico de f, podemos considerar el conjunto $S_f = \{v_i : f_i = 1\} \subseteq \mathbb{F}_2^m$.
Sabemos por la Proposición 2.3 que cada vector de $\mathbb{F}_2^m$ se corresponde con un polinomio reducido f, por lo tanto, se le puede asociar también el conjunto S_f. Recíprocamente, si tenemos un conjunto $S \subseteq \mathbb{F}_2^m$ podemos asociar a este subconjunto un vector de $\mathbb{F}_2^m$, que será aquel que tenga un 1 en la posición i si $v_i \in S$, y tenga un 0 en la posición j si $v_j \notin S$.

Definición 4.1. Sea S un subconjunto de $\mathbb{F}_2^m$. Llamaremos vector característico de S al vector asociado a este conjunto tal y como acabamos de ver. Lo denotaremos como $\mathbf{f}_S$.

Como tenemos que cada vector de $\mathbb{F}_2^m$ se corresponde con un polinomio reducido de $\mathbb{F}_2[X_1, ..., X_m]$, a cada subconjunto $S \subseteq \mathbb{F}_2^m$ se le puede asociar un polinomio. Además, por cómo hemos visto que era el vector característico de S tenemos que $S_f = S$.

Definición 4.2. Sea S un subconjunto de $\mathbb{F}_2^m$. Llamaremos polinomio asociado a S al polinomio reducido $f \in \mathbb{F}_2[X_1, ..., X_m]$ tal que $S = S_f$. Lo denotaremos como f_S.

Recordamos el concepto de variedad afín, que es equivalente al de la clase de equivalencia de un espacio vectorial cociente.

Definición 4.3. Si V es un espacio vectorial de $\mathbb{F}_2^m$ y $a \in \mathbb{F}_2^m$, la variedad afín que pasa por a y tiene dirección V es la clase de equivalencia

$$a + V = \{a + v : v \in V\}.$$

Hay $2^{\dim(V)}$ representantes en $a + V$ y se llama a cada uno punto de la variedad. Llamaremos dimensión de la variedad $a + V$ a la dimensión de V como espacio vectorial.

Ejemplo 4.1. Para entender mejor las variedades vamos a ver con estos ejemplos cómo es una variedad dependiendo de la dimensión de V. Vamos a ver también cuáles son los vectores característicos dependiendo de cada subconjunto.

1. Si V tiene dimensión 0 esto significa que $V = \{0\}$, y entonces la variedad es $a + V = \{a\}$. Con esto vemos que las variedades de dimensión 0 son puntos, y todo punto se puede considerar como una variedad de dimensión 0. Si consideramos el espacio afín $\mathbb{F}_2^3$ podemos asociar a cada variedad un vector característico, en el caso de las variedades de dimensión 0, en la siguiente tabla vemos sus vectores característicos.

Punto	Vector	Punto	Vector
v_1	10000000	v_5	00001000
v_2	01000000	v_6	00000100
v_3	00100000	v_7	00000010
v_4	00010000	v_8	00000001

   Recordamos que los vectores característicos de un subconjunto son aquellos que tienen un 1 en la posición i si v_i está en el subconjunto y un 0 si no lo está.

2. Si V tiene dimensión 1, significa que $V = \{0, u\}$, y entonces la variedad $a+V = \{a, a+u\}$ es una recta afín. Si consideramos de nuevo el espacio afín $\mathbb{F}_2^3$, los vectores característicos de las rectas serán los siguientes.

Recta	Vector	Recta	Vector
$\{v_1, v_2\}$	11000000	$\{v_3, v_5\}$	00101000
$\{v_1, v_3\}$	10100000	$\{v_3, v_6\}$	00100100
$\{v_1, v_4\}$	10010000	$\{v_3, v_7\}$	00100010
$\{v_1, v_5\}$	10001000	$\{v_3, v_8\}$	00100001
$\{v_1, v_6\}$	10000100	$\{v_4, v_5\}$	00011000
$\{v_1, v_7\}$	10000010	$\{v_4, v_6\}$	00010100
$\{v_1, v_8\}$	10000001	$\{v_4, v_7\}$	00010010
$\{v_2, v_3\}$	01100000	$\{v_4, v_8\}$	00010001
$\{v_2, v_4\}$	01010000	$\{v_5, v_6\}$	00001100
$\{v_2, v_5\}$	01001000	$\{v_5, v_7\}$	00001010
$\{v_2, v_6\}$	01000100	$\{v_5, v_8\}$	00001001
$\{v_2, v_7\}$	01000010	$\{v_6, v_7\}$	00000110
$\{v_2, v_8\}$	01000001	$\{v_6, v_8\}$	00000101
$\{v_3, v_4\}$	00110000	$\{v_7, v_8\}$	00000011

3. Si la dimensión de V es 2, tenemos que V es un plano vectorial y $V = \{0, u_1, u_2, u_1+u_2\}$. Ahora la variedad de dimensión 2 será $a+V = \{a, a+u_1, a+u_2, a+u_1+u_2\} = \{a+\lambda_1 u_1+\lambda_2 u_2 : \lambda_1, \lambda_2 \in \mathbb{F}_2\}$, que se llama plano afín. Si de nuevo buscamos los vectores característicos en $\mathbb{F}_2^3$ esta vez de los planos obtenemos la siguiente lista.

Plano	Vector	Plano	Vector
$\{v_1, v_2, v_3, v_4\}$	11110000	$\{v_2, v_3, v_5, v_8\}$	01101001
$\{v_1, v_2, v_5, v_6\}$	11001100	$\{v_2, v_3, v_6, v_7\}$	01100110
$\{v_1, v_2, v_7, v_8\}$	11000011	$\{v_2, v_4, v_5, v_7\}$	01011010
$\{v_1, v_3, v_5, v_7\}$	10101010	$\{v_2, v_4, v_6, v_8\}$	01010101
$\{v_1, v_3, v_6, v_8\}$	10100101	$\{v_3, v_4, v_5, v_6\}$	00111100
$\{v_1, v_4, v_5, v_8\}$	10011001	$\{v_3, v_4, v_7, v_8\}$	00110011
$\{v_1, v_4, v_6, v_7\}$	10010110	$\{v_5, v_6, v_7, v_8\}$	00001111

4. Si V tiene dimensión $m-1$, $V = \{u_1, ..., u_{m-1}\}$ y es un hiperplano vectorial. Entonces, la variedad será $a+V = \{a+\lambda_1 u_1+\cdots+\lambda_{m-1}u_{m-1} : \lambda_1, ..., \lambda_{m-1} \in \mathbb{F}_2\}$, y lo llamamos hiperplano afín. Si consideráramos de nuevo el cuerpo $\mathbb{F}_2^3$, estaríamos en el ejemplo anterior.

Ahora, lo que queremos ver es si teniendo un subespacio vectorial V de $\mathbb{F}_2^m$, y una variedad $a+V$, podemos averiguar cuál es el polinomio asociado a esta variedad, y la relación entre los polinomios asociados y las variedades. Si tenemos que $H = (h_{ij})$ es una matriz control de V, podemos obtener unas ecuaciones implícitas del subespacio, ya que un elemento $x = (x_1, ..., x_m)$ estará contenido en V si y sólo si $h_{i1}x_1 + \cdots + h_{im}x_m = 0$, para todo $i = 1, ..., m-k$, siendo k la dimensión de V. Entonces, si consideramos $k = m-1$ y $a, b \in \mathbb{F}_2^m$, tendremos que $H = (h_1, ..., h_m)$ y que como $b \in a+V$ si y sólo si

$b-a \in V$, esto implicará que $h_1(b_1-a_1)+\cdots+h_m(b_m-a_m)=0$, y llegamos a que $h_1b_1+\cdots+h_mb_m = h_1a_1+\cdots+h_ma_m$. Con lo cual, si llamamos $a_h = h_1a_1+\cdots+h_ma_m$ y consideramos el polinomio $h = h_1X_1+\cdots+h_mX_m+a_h+1$ tendremos que $b \in a+V$ si y sólo si $h(b)=1$. Por lo tanto $a+V = S_h$.
Utilizando este razonamiento podemos probar la siguiente proposición:

Proposición 4.1. *Si S es una variedad en $\mathbb{F}_2^m$ de dimensión k, entonces el polinomio asociado a S tendrá grado $m-k$.*

Demostración. Sea $a \in \mathbb{F}_2^m$, tal que $S = a+V$, y sea $H = (h_{ij})$ la matriz de control de V, que tendrá dimensiones $(m-k)\times m$. Vamos a llamar $a_{h_i} = h_{i1}a_1+\cdots+h_{im}a_m$ y a considerar los polinomios $h_i = h_{i1}X_1+\cdots+h_{im}X_m+a_{h_i}+1$ para cada $i=1,...,m-k$. Razonando como hemos hecho para $k=m-1$, tenemos que $b \in S$ si y sólo si $h_i(b)=1$ para todo $i=1,...,m-k$, con lo cual, si $h = h_1\cdots h_{m-k}$ entonces $S = S_h$. Como tenemos que el grado de h_i es 1 para todo $i=1,...,m-k$, y h es el producto de todos ellos, el grado de h será menor o igual que $m-k$. Y si tomamos la matriz H en la forma estándar, tendremos que uno de los monomios de h será $X_{k+1}\cdots X_m$, luego su grado será exactamente $m-k$. □

Con esta demostración no solo hemos estudiado la relación entre la dimensión de una variedad y el grado de su polinomio asociado, también hemos visto cómo obtener el polinomio asociado a una variedad.

Antes de ver el algoritmo de descodificación vamos a definir una operación que vamos a utilizar en la siguiente sección:

Definición 4.4. Sean $u, v \in \mathbb{F}_q^m$, se define el vector $u*v$ como el vector que tiene en su $i-$ésima componente el producto de las $i-$ésimas componentes de u y v, es decir, $u*v = (u_1v_1,...,u_mv_m)$.

4.2. Algoritmo de descodificación

Ahora ya podemos estudiar un algoritmo de descodificación para los códigos Reed-Muller. Si consideramos $\mathcal{RM}_2(r,m)$ ya hemos visto que la distancia mínima será $(q-b)q^{m-a-1}$, donde $r = a(q-1)+b$, $a,b \in \mathbb{N}_0$ y $b \leq q-1$, como ahora $q=2$, $q-1=1$, y entonces tenemos que $a=r$ y $b=0$. Sustituyendo llegamos a que $d = (2)2^{m-r-1} = 2^{m-r}$. Por tanto, el número de errores que vamos a poder corregir va a ser $2^{m-r-1}-1$.
Vamos a suponer que $c \in \mathcal{RM}_2(r,m)$ es la palabra del código enviada, y la palabra recibida es $y = c+e$, y definimos el siguiente concepto.

Definición 4.5. Sea $S \subseteq \mathbb{F}_2^m$ una variedad, decimos que es par (con respecto a y) si y contiene un número par de errores en las posiciones de $\mathrm{sop}(\mathbf{f}_S)$. Decimos que S es impar (con respecto a y) si y tiene un número de errores impar en las posiciones de $\mathrm{sop}(\mathbf{f}_S)$.

Alternativamente, la paridad de S también se puede definir como la paridad de $w_H(\mathbf{f}_S * e)$. Si consideramos las variedades de dimensión 0, $\{v_i\}$, calcular su paridad va a ser equivalente a comprobar si en la posición i hay un error. Ya que como vimos en el Ejemplo 4.1, el vector característico de la variedad $\{v_i\}$ es aquel que tiene un 1 en la posición i y un 0 en el resto de posiciones, por tanto si $w_H(\mathbf{f}_{\{v_i\}} * e) = 1$ significa que hay un 1 en la posición i de e, es decir, un error. Y si $w_H(\mathbf{f}_{\{v_i\}} * e) = 0$, en esa posición no hay un error. El algoritmo de descodificación se va a centrar en calcular la paridad de estas variedades.
Vamos a ver un lema que va a ser necesario para probar el siguiente resultado.

Lema 4.1. *Si u y v son dos vectores de $\mathbb{F}_2^m$, entonces $w_H(u+v) = w_H(u) + w_H(v) - 2w_H(u * v)$*

Demostración. Tenemos que $w_H(u) = \sharp\text{sop}(u)$, y por estar en un cuerpo binario se cumple $w_H(u + v) = \sharp\text{sop}(u) + \sharp\text{sop}(v) - 2\sharp\{\text{sop}(u) \cap \text{sop}(v)\}$. Vemos también que $\text{sop}(u) \cap \text{sop}(v) = \text{sop}(u * v)$, con lo que queda probado el resultado. □

Proposición 4.2. *Si $S \subseteq \mathbb{F}_2^m$ es una variedad de dimensión $r + 1$, entonces su paridad coincide con la de $w_H(\mathbf{f}_S * y)$.*

Demostración. Si tenemos que la dimensión de S es $r+1$, por la Proposición 4.1 el grado del polinomio asociado a S será $m - r - 1$, y entonces como el vector asociado está dado por las evaluaciones de este polinomio tenemos que $\mathbf{f}_S \in \mathcal{RM}_2(m - r - 1, m)$. Sabemos que $\mathcal{RM}_2(m - r - 1, m) = \mathcal{RM}_2^{\perp}(r, m)$, con lo cual $\mathbf{f}_S \bullet c = 0$, y esto implica que $w_H(\mathbf{f}_S * c)$ tiene que ser par. Aplicando el Lema 4.1, $w_H(\mathbf{f}_S * y) = w_H(\mathbf{f}_S * (c + e)) = w_H(\mathbf{f}_S * c + \mathbf{f}_S * e) = w_H(\mathbf{f}_S * c) + w_H(\mathbf{f}_S * e) - 2w_H(\mathbf{f}_S * c * e)$ vemos que la paridad de $w_H(\mathbf{f}_S * y)$ tiene que coincidir con la de $w_H(\mathbf{f}_S * e)$, y por tanto con la de S. □

Esto nos da la manera de calcular la paridad de una variedad de dimensión $r+1$, pero como las variedades de las que nos interesa conocer la paridad son de las de dimensión 0, vamos a estudiar el mecanismo para averiguar las paridades de las variedades con dimensión $r, r-1, ..., 1, 0$ de maneta iterada a partir de las de dimensión $r + 1$. Para ello, vamos a necesitar los siguientes resultados.

Lema 4.2. *Cada variedad $S \subset \mathbb{F}_2^m$ de dimensión $k < m$, está contenida en $2^{m-k} - 1$ variedades de dimensión $k + 1$.*

Demostración. Para todo $b \in \mathbb{F}_2^m - S$ existe una única variedad de dimensión $k + 1$ que contenga a S y a b. En S, por tener dimensión k, tenemos que hay 2^k elementos, por tanto en $\mathbb{F}_2^m - S$ hay $2^m - 2^k$ elementos y todos ellos pueden formar una variedad de dimensión $k + 1$ en la que esté contenida

S, pero de ellos $2^{k+1} - 2^k$ van a generar la misma variedad. Con lo cual el número de variedades de dimensión $k+1$ que contengan a S van a ser

$$\frac{2^m - 2^k}{2^{k+1} - 2^k} = \frac{2^{m-k} - 1}{2 - 1} = 2^{m-k} - 1.$$

□

Proposición 4.3. *Sea $S \subseteq \mathbb{F}_2^m$ una variedad de dimensión k $(0 \leq k \leq r)$. Si el número de errores de y no supera $2^{m-r-1} - 1$, entonces la paridad de S (con respecto de y) coincide con la paridad de la mayoría de las variedades de dimensión $k+1$ que la contienen.*

Demostración. Vamos a considerar una variedad T que contiene a S y tiene dimensión $k+1$. Si esta variedad tuviera paridad distinta de S existiría un elemento $v_i \in T - S$ tal que en la posición i de y hay un error. Como el número de errores de y es como máximo $2^{m-r-1} - 1$, habrá como mucho $2^{m-r-1} - 1$ variedades con distinta paridad que S. Por el Lema 4.2 tenemos que el número de variedades de dimensión $k+1$ en las que S está contenida son $2^{m-k} - 1$, con lo cual el número de variedades con la misma paridad que S es, como mínimo,

$$(2^{m-k} - 1) - (2^{m-r-1} - 1) = 2^{m-k} - 2^{m-r-1} = 2^{m-r-1}(2^{r+1-k} - 1)$$

y como $k \leq r$, entonces $k+1 \leq r+1$, y esto implica $1 \leq r+1-k$, por tanto

$$2^{m-r-1}(2^{r+1-k} - 1) \geq 2^{m-r-1}(2 - 1) = 2^{m-r-1}.$$

Con esto hemos visto que el número de variedades cuya paridad coincide con la de S es mayor que el número de aquellas con las que no coincide. □

Con estos resultados obtenemos un método para corregir errores: cuando recibimos la palabra y utilizamos la Proposición 4.2 para calcular la paridad de las variedades con dimensión $r+1$. Una vez calculadas, por la Proposición 4.3 podemos obtener la paridad de las variedades de dimensión r, viendo qué paridad tienen la mayoría de las variedades que las contienen. De la misma manera podemos obtener la paridad de las variedades de dimensión $r-1$, y repitiendo el proceso iteradamente, podemos llegar a las variedades de dimensión 0. Como sabemos, los errores de y se encuentran en las posiciones correspondientes a las variedades de dimensión 0 impares, por tanto modificamos estas coordenadas y así corregimos los errores y obtenemos c, la palabra enviada.

A continuación, vamos a ver un ejemplo de cómo aplicar este método:

Ejemplo 4.2. Vamos a considerar $\mathcal{RM}_2(1,3)$, este código tiene distancia mínima $2^{3-1} = 2^2 = 4$, y va a poder corregir $2^{3-1-1} - 1 = 2 - 1 = 1$ error.

Sea $c = (01101001) \in \mathcal{RM}_2(1,3)$ la palabra enviada, e $y = (01100001)$ la palabra recibida, como podemos ver, solo tiene un error, con lo cual con el método que hemos descrito vamos a poder corregirlo. Como en este caso $r = 1$ vamos a comenzar calculando las paridades de las variedades de dimensión 2, por la Proposición 4.2 podemos calcular la paridad de las variedades haciendo el producto $*$ entre el vector característico e y y calculando su peso. En el Ejemplo 4.1 vimos todas las variedades de dimensión 2 de $\mathbb{F}_2^3$ y sus vectores característicos, la paridad por ejemplo de $\{v_1, v_2, v_3, v_4\}$ sería $w_H((11110000)*y) = 2$, par, y la de $\{v_1, v_2, v_5, v_6\}$ es $w_H((11001100)*y) = 1$, impar. Haciendo los cálculos con todos los vectores característicos de todas las variedades obtenemos los siguientes resultados. En la tabla denotaremos por 0 las variedades pares y por 1 las impares.

Variedad	Paridad	Variedad	Paridad
$\{v_1, v_2, v_3, v_4\}$	0	$\{v_2, v_3, v_5, v_8\}$	1
$\{v_1, v_2, v_5, v_6\}$	1	$\{v_2, v_3, v_6, v_7\}$	0
$\{v_1, v_2, v_7, v_8\}$	0	$\{v_2, v_4, v_5, v_7\}$	1
$\{v_1, v_3, v_5, v_7\}$	1	$\{v_2, v_4, v_6, v_8\}$	0
$\{v_1, v_3, v_6, v_8\}$	0	$\{v_3, v_4, v_5, v_6\}$	1
$\{v_1, v_4, v_5, v_8\}$	1	$\{v_3, v_4, v_7, v_8\}$	0
$\{v_1, v_4, v_6, v_7\}$	0	$\{v_5, v_6, v_7, v_8\}$	1

Ahora que tenemos la paridad de las variedades de dimensión 2 vamos a calcular las de dimensión 1. Sabemos por el Lema 4.2 que cada variedad de dimensión 1 va a estar contenida en $2^{3-1} - 1 = 4 - 1 = 3$ de dimensión 2, y tenemos que ver en esas tres cual es la paridad que más se repite. Si consideramos la variedad $\{v_1, v_2\}$ tenemos que las paridades de las variedades que la contienen son $0, 1, 0$, con lo cual su paridad es 0, es decir par. Pero si consideramos $\{v_1, v_5\}$ las paridades son $1, 1, 1$ con lo que su paridad es 1, es decir, impar. De nuevo hacemos una tabla con las paridades de todas las variedades.

Variedad	Paridad	Variedad	Paridad
$\{v_1, v_2\}$	0	$\{v_3, v_5\}$	1
$\{v_1, v_3\}$	0	$\{v_3, v_6\}$	0
$\{v_1, v_4\}$	0	$\{v_3, v_7\}$	0
$\{v_1, v_5\}$	1	$\{v_3, v_8\}$	0
$\{v_1, v_6\}$	0	$\{v_4, v_5\}$	1
$\{v_1, v_7\}$	0	$\{v_4, v_6\}$	0
$\{v_1, v_8\}$	0	$\{v_4, v_7\}$	0
$\{v_2, v_3\}$	0	$\{v_4, v_8\}$	0
$\{v_2, v_4\}$	0	$\{v_5, v_6\}$	1
$\{v_2, v_5\}$	1	$\{v_5, v_7\}$	1
$\{v_2, v_6\}$	0	$\{v_5, v_8\}$	1
$\{v_2, v_7\}$	0	$\{v_6, v_7\}$	0
$\{v_2, v_8\}$	0	$\{v_6, v_8\}$	0
$\{v_3, v_4\}$	0	$\{v_7, v_8\}$	0

Repetimos el proceso para las variedades de dimensión 0. Ahora cada variedad va a estar contenida en $2^3 - 1 = 7$ variedades de dimensión 1, en el caso de $\{v_1\}$ las paridades de las variedades en las que está contenida son $0, 0, 0, 1, 0, 0, 0$, y por tanto su paridad será 0, es decir, par. Mientras que para $\{v_5\}$ las paridades son $1, 1, 1, 1, 1, 1, 1$, con lo cual la suya es 1, es decir, impar. Como estamos estudiando ya las variedades de dimensión 0 esto significa que en la posición 5 hay un error en y. Hacemos una tabla con las paridades de todas.

Variedad	Paridad	Variedad	Paridad
v_1	0	v_5	1
v_2	0	v_6	0
v_3	0	v_7	0
v_4	0	v_8	0

Podemos ver en la tabla que la paridad de todas las variedades es par excepto la de $\{v_5\}$ que es impar, por lo tanto el error de y estará en la posición 5, y la palabra decodificada sería (01101001), que es efectivamente c.

Capítulo 5

Códigos descodificables localmente

En este capítulo vamos a estudiar los códigos localmente descodificables y corregibles, y a ver procedimientos de descodificación local para códigos Reed-Muller. La descodificación local va a consistir en poder corregir una coordenada de una palabra con una probabilidad alta mirando r componentes de la palabra con errores, lo cual supondrá una mejora comparado con corregir la palabra de forma global.
Se usa como referencia en este capítulo [5].

5.1. Códigos descodificables y corregibles localmente

En esta sección vamos a definir los conceptos de códigos localmente descodificables y códigos localmente corregibles, que tienen definiciones distintas, y vamos a ver la relación entre ellas.
Vamos a denotar por $\Delta(x, y)$ a la distancia de Hamming relativa entre x e y, es decir, una fracción de las coordenadas en las que difieren x e y.
Por $\mathcal{A}$ denotaremos un algoritmo aleatorio que tiene como entrada un elemento $y \in \mathbb{F}_q^n$, y como salida una variable aleatoria $\mathcal{A}(y)$ en $\mathbb{F}_q^n$. $\mathcal{A}(y)_i$ será su coordenada número i, que es una variable aleatoria en $\mathbb{F}_q$.

Definición 5.1. Dados un entero positivo r y constantes δ, $\varepsilon > 0$, se dice que un código dado por la aplicación de codificación $f : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, es $(r, \delta, \varepsilon)-$localmente descodificable si existe un algoritmo aleatorio de descodificación $\mathcal{A}$ tal que:

1. Para todo $x \in \mathbb{F}_q^k$, $i \in \{1, ..., k\}$, y todo $y \in \mathbb{F}_q^n$, tal que $\Delta(f(x), y) \leq \delta$ se cumple que
$$P(\mathcal{A}(y)_i = x_i) \geq 1 - \epsilon,$$
donde P es la probabilidad.

2. $\mathcal{A}$ hace como mucho r consultas a y, es decir, $\mathcal{A}$ observa como mucho r componentes del vector y (de ahí el término local).

Un código descodificable localmente permite descodificar probabilisticamente cualquier coordenada de un mensaje mirando solo algunas coordenadas de su codificación con errores. Una propiedad más sólida, que es la que vamos a ver ahora, es la corregibilidad local, que permite recuperar no solo las coordenadas del mensaje, sino también las coordenadas de la codificación.

Definición 5.2. Un código $\mathcal{C}$ contenido en $\mathbb{F}_q^n$ se dice que es $(r, \delta, \varepsilon)-$localmente corregible si existe un algoritmo aleatorio corrector $\mathcal{A}$ tal que:

1. Para todo $c \in \mathcal{C}$, $i \in \{1, ..., n\}$, y todo $y \in \mathbb{F}_q^n$, tal que $\Delta(c, y) \leq \delta$ se cumple que
$$P(\mathcal{A}(y)_i = c_i) \geq 1 - \epsilon,$$
donde P es la probabilidad.

2. $\mathcal{A}$ hace como mucho r consultas a y.

El siguiente resultado relaciona estos dos tipos de códigos y nos muestra como obtener un código localmente descodificable a partir de un código localmente corregible.

Lema 5.1. *Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código $(r, \delta, \varepsilon)-$localmente corregible, entonces existe $\mathcal{C}'$, un código dado por la aplicación de codificación f' que codifica mensajes de longitud $k = dim(\mathcal{C})$ a mensajes de longitud n, que es $(r, \delta, \varepsilon)-$localmente descodificable.*

Demostración. Sea $I \subseteq \{1, ..., n\}$ un subconjunto de cardinal k tal que $\mathcal{C}$ es sistemático sobre I. Tal conjunto sabemos que existe por la Proposición 1.6. Para $c \in \mathcal{C}$ denotamos como $c|_I \in \mathbb{F}_q^k$ al vector con las coordenadas de c correspondientes a I. Dado un mensaje $x \in \mathbb{F}_q^k$ definimos $f'(x)$ como el único elemento $c \in \mathcal{C}$ que cumple que $c|_I = x$. Por tanto, la corregibilidad $(r, \delta, \varepsilon)-$local de $\mathcal{C}$ implica la decodificabilidad $(r, \delta, \varepsilon)-$local de $\mathcal{C}'$. □

5.2. Códigos Reed-Muller localmente descodificables

En esta sección vamos a considerar $\mathcal{RM}_q(r, m)$ tal que $r < q-1$, entonces como en este caso vamos a tener que el número de monomios en m variables de grado $\leq r$ va a ser $\binom{m+r}{r}$, la dimensión de este código será $k = \binom{m+r}{r}$.

Descodificación básica en líneas

Vamos a ver el procedimiento más simple para la corrección local de códigos Reed-Muller. Vamos a tratar con este procedimiento de recuperar el valor de la evaluación de un polinomio $F \in \mathbb{F}_q[X_1, ..., X_m]^{(r)}$ en un punto $w \in \mathbb{F}_q^m$ trazando una línea afín que pase por w.

Proposición 5.1. *Sea q una potencia de un primo y m y r enteros positivos tales que $r < q-1$. Entonces existe un código de dimensión k y longitud $n = q^m$, $(r+1, \delta, (r+1)\delta)-$localmente corregible para todo δ.*

Demostración. Consideramos $\mathcal{RM}_q(r,m)$. El procedimiento de corrección local que vamos a seguir es el siguiente. Tomamos un elemento de este código, que está dado por las evaluaciones de un polinomio $F \in \mathbb{F}_q[X_1, ..., X_m]^{(r)}$, con como mucho $n\delta$ errores. Tomamos también un punto $w \in \mathbb{F}_q^m$ el cual se corresponde con la coordenada de la palabra codificada que queremos corregir, y eligiendo aleatoriamente otro vector $v \in \mathbb{F}_q^m$, consideramos la recta

$$\begin{array}{rccc} L\colon & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^m \\ & \lambda & \longmapsto & w + \lambda v \end{array}$$

Sea S un subconjunto arbitrario de $\mathbb{F}_q^*$ tal que $|S| = r+1$, y consideramos las evaluaciones de F en los puntos $w + \lambda v$, $\lambda \in S$, a las que vamos a denotar como e_λ. A continuación, interpolamos el único polinomio h de una variable y grado a lo sumo r que cumple que $h(\lambda) = e_\lambda$ para todo $\lambda \in S$. El procedimiento termina devolviendo el valor $h(0)$.
Vemos que si las consultas al vector de evaluaciones de F se hacen en coordenadas en las que no están los errores entonces $h(0) = F(w)$, y como las coordenadas del vector se eligen aleatoriamente, la probabilidad de no elegir una coordenada errónea es de $1-(r+1)\delta$. Las consultas que hacemos al vector son $r+1$, y se puede corregir un vector con una proporción de hasta δ errores. Con esto hemos probado que $\mathcal{RM}_q(r,m)$ es un código $(r+1, \delta, (r+1)\delta)-$localmente corregible. □

Vamos a decir que un código $\mathcal{C}$ tolera una fracción δ de errores si $\mathcal{C}$ es $(r, \delta, \varepsilon)-$localmente corregible (o descodificable) para algún $\varepsilon < \frac{1}{2}$. Por tanto, los códigos dados por la Proposición 5.1 van a tolerar una fracción de errores $\delta < \frac{1}{2(r+1)}$. Con lo cual, la tolerancia del código va a ser menor cuanto más grande sea el número de consultas que hagamos. En el siguiente apartado, vamos a ver otro procedimiento para códigos Reed-Muller que va a tolerar una fracción de errores δ cercana a $\frac{1}{4}$ independientemente del número de consultas.

Descodificación mejorada en líneas

A diferencia de el caso anterior, para este procedimiento vamos a necesitar que r sea bastante más pequeño que q.

Proposición 5.2. *Sea $\sigma < 1$ un número real positivo. Sea q una potencia de un primo y m y r enteros positivos tales que $r \leq \sigma(q-1)-1$. Entonces existe un código de dimensión k y longitud $n = q^m$, $(q-1, \delta, \frac{2\delta}{(1-\sigma)})-$localmente corregible para todo δ.*

Demostración. De nuevo vamos a considerar $\mathcal{RM}_q(r,m)$, y vamos a utilizar un procedimiento de corrección local muy similar al de la Proposición 5.1. Tomamos un elemento del código, dado por las evaluaciones del polinomio $F \in \mathbb{F}_q[X_1,...,X_m]^{(r)}$, con como mucho $n\delta$ errores, un punto $w \in \mathbb{F}_q^m$ que se corresponde con la coordenada de la palabra codificada que queremos corregir, escogemos aleatoriamente un $v \in \mathbb{F}_q^m$ y consideramos la recta

$$\begin{array}{rccc} L\colon & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^m \\ & \lambda & \longmapsto & w+\lambda v \end{array}$$

Consultamos las coordenadas del vector de evaluación de F correspondientes a los puntos $w+\lambda v$, para todo $\lambda \in \mathbb{F}_q^*$, y denotamos a estas como e_λ. Calculamos el único polinomio h de una variable y grado a lo sumo r que cumple que $h(\lambda) = e_\lambda$, para todos menos a lo sumo $\lfloor \frac{(1-\sigma)(q-1)}{2} \rfloor$ valores de $\lambda \in \mathbb{F}_q^*$. Terminamos devolviendo el valor $h(0)$. Si el polinomio h no existiese devolveríamos el valor 0. La búsqueda del polinomio h se puede hacer de manera eficiente utilizando algún algoritmo de corrección de errores para códigos Reed-Solomon. Nótese que la restricción de las evaluaciones de F a la recta L menos w, es decir, las evaluaciones de h en $\mathbb{F}_q^*$, dan lugar a una palabra de un código de Reed-Solomon de grado $r+1$ y longitud $q-1$. Por tanto, un algoritmo de descodificación para tal código puede corregir hasta

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{(q-1)-r-1}{2} \right\rfloor \geq \left\lfloor \frac{(q-1)-\sigma(q-1)+1-1}{2} \right\rfloor = \left\lfloor \frac{(1-\sigma)(q-1)}{2} \right\rfloor$$

errores. Véase por ejemplo la sección 5.4 de [3], y el Ejemplo 2.1.
Sabemos que si las coordenadas del vector de evaluación de F que hemos utilizado para encontrar h no tenían errores, o tenían un número de errores corregibles tendremos que $h(0) = F(w)$, vamos a estudiar la probabilidad de que esto suceda. Para un $a \in \mathbb{F}_q^m$, y un $\lambda \in \mathbb{F}_q^*$ vamos a denotar x_a^λ como la función indicadora del suceso aleatorio $L(\lambda) = a$, donde λ y a son fijos, y w, v aleatorios. Está función toma los siguientes valores:

$$x_a^\lambda = \begin{cases} 1 & \text{si } L(\lambda) = a \\ 0 & \text{si } L(\lambda) \neq a. \end{cases}$$

Sea $E \subseteq \mathbb{F}_q^m$ el conjunto de todos aquellos $a \in \mathbb{F}_q^m$ tales que sus evaluaciones en F tienen errores. Asumiremos el peor de los casos, que es aquel en el que $|E| = n\delta$. Consideramos

$$x_E^\lambda = \sum_{a \in E} x_a^\lambda.$$

La cual, por la definición de x_a^λ, tomará los valores

$$x_E^\lambda = \begin{cases} 1 & \text{si } L(\lambda) \in E \\ 0 & \text{si } L(\lambda) \notin E. \end{cases}$$

Es por tanto, la función indicadora del conjunto E.
Si calculamos la esperanza de esta variable aleatoria tenemos que

$$\mathbb{E}(x_E^\lambda) = P(L(\lambda) \in E) = \sum_{a \in E} \mathbb{E}(x_a^\lambda) = \sum_{a \in E} P(L(\lambda) \in a) = \sum_{a \in E} \frac{1}{n} =$$

$$= |E| \cdot \frac{1}{n} = n\delta \cdot \frac{1}{n} = \delta$$

donde $P(L(\lambda) \in a) = \frac{1}{n}$, porque a es fijo, $L(\lambda)$ es uniformemente aleatorio en $\mathbb{F}_q^m$, y $|\mathbb{F}_q^m| = q^m = n$.
Finalmente, consideramos la variable aleatoria

$$x = \sum_{\lambda \in \mathbb{F}_q^*} x_E^\lambda,$$

que cuenta el número de consultas que llegan a coordenadas con errores. Tenemos que la esperanza es

$$\mathbb{E}(x) = (q-1)\delta.$$

Entonces, la probabilidad de elegir una coordenada errónea, utilizando la desigualdad de Markov, es

$$P\left(x \geq \frac{(1-\sigma)(q-1)}{2}\right) \leq \frac{2\delta(q-1)}{(1-\sigma)(q-1)} = \frac{2\delta}{1-\sigma}.$$

El número de consultas que hacemos al vector son el número de elementos que hay en $\mathbb{F}_q^*$, que es $q-1$, y se puede corregir un vector con una proporción de hasta δ errores. Con esto hemos probado que $\mathcal{RM}_q(r,m)$ es un código $(q-1, \delta, \frac{2\delta}{(1-\sigma)})-$localmente corregible. □

En la Proposición 5.2 si queremos que $\varepsilon = \frac{2\delta}{1-\sigma} < \frac{1}{2}$ entonces debemos tener que $\delta < \frac{1}{4}(1-\sigma)$, el cual se acerca a $\frac{1}{4}$ cuando σ es pequeño. En el siguiente apartado, vamos a ver un procedimiento que mejora la tolerancia hasta una facción de errores de $\frac{1}{2}$ aproximadamente.

Descodificación en curvas

Para este procedimiento también vamos a necesitar que r sea bastante más pequeño que q. Vamos a tratar, de nuevo, de obtener la evaluación de un polinomio $F \in \mathbb{F}_q[X_1, ..., X_m]^{(r)}$ en un punto $w \in \mathbb{F}_q^m$, pero en este caso, en vez de utilizar una recta, vamos a utilizar una curva cuadrática paramétrica aleatoria que pase por w.

Proposición 5.3. *Sea $\sigma < 1$ un número real positivo. Sea q una potencia de un primo y m y r enteros positivos tales que $r \leq \sigma(q-1)-1$. Entonces existe un código de dimensión k y longitud $n = q^m$, tal que para todo $0 < \delta < \frac{1}{2} - \sigma$ es $(q-1, \delta, O_{\sigma,\delta}(\frac{1}{q}))-$localmente corregible.*

Demostración. Consideramos $\mathcal{RM}_q(r,m)$, el procedimiento va a ser muy similar a los anteriores. Tomamos un elemento del código, dado por las evaluaciones del polinomio $F \in \mathbb{F}_q[X_1,...,X_m]^{(r)}$, con como mucho $n\delta$ errores, un punto $w \in \mathbb{F}_q^m$ que se corresponde con la coordenada de la palabra codificada que queremos corregir, escogemos aleatoriamente dos vectores $v_1, v_2 \in \mathbb{F}_q^m$ y consideramos la curva cuadrática

$$\begin{array}{rccc} \chi\colon & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^m \\ & \lambda & \longmapsto & w + \lambda v_1 + \lambda^2 v_2 \end{array}$$

Consultamos las coordenadas del vector de evaluación de F correspondientes a los puntos $w + \lambda v_1 + \lambda^2 v_2$, para todo $\lambda \in \mathbb{F}_q^*$, y denotamos a estas como e_λ. Calculamos el único polinomio h de una variable y grado a lo sumo $2r$ que cumple que $h(\lambda) = e_\lambda$, para todos menos a lo sumo $\lfloor \frac{(1-2\sigma)(q-1)}{2} \rfloor$ valores de $\lambda \in \mathbb{F}_q^*$. Para terminar el procedimiento, devolvemos el valor $h(0)$. Si no existiera h devolveríamos 0. El procedimiento tiene éxito si el número de consultas que van a coordenadas con errores es como máximo $\lfloor \frac{(1-2\sigma)(q-1)}{2} \rfloor$. El razonamiento es similar al de la prueba de la Proposición 5.2, es decir, utilizamos un algoritmo de corrección de errores, pero ahora para un código de Reed-Solomon de grado $2r+1$ y longitud $q-1$.
Vamos a analizar la probabilidad de que nuestro procedimiento no tenga éxito. Al igual que como hicimos en la demostración de la Proposición 5.2 para un $a \in \mathbb{F}_q^m$, y un $\lambda \in \mathbb{F}_q^*$ vamos a denotar x_a^λ como la función indicadora del suceso $\chi(\lambda) = a$, donde λ y a son fijos, y w, v_1, v_2 aleatorios. Esta función toma los siguientes valores:

$$x_a^\lambda = \begin{cases} 1 & \text{si } \chi(\lambda) = a \\ 0 & \text{si } \chi(\lambda) \neq a. \end{cases}$$

De nuevo tomamos $E \subseteq \mathbb{F}_q^m$ el conjunto de todos aquellos $a \in \mathbb{F}_q^m$ tales que sus evaluaciones en F tienen errores, y asumimos el peor de los casos, en el que $|E| = n\delta$. Consideramos

$$x_E^\lambda = \sum_{a \in E} x_a^\lambda.$$

Que al ser la función indicadora del conjunto E, tomará los valores

$$x_E^\lambda = \begin{cases} 1 & \text{si } \chi(\lambda) \in E \\ 0 & \text{si } \chi(\lambda) \notin E. \end{cases}$$

Si calculamos la esperanza de esta variable aleatoria tenemos de nuevo que

$$\mathbb{E}(x_E^\lambda) = P(\chi(\lambda) \in E) = \sum_{a \in E} \mathbb{E}(x_a^\lambda) = \sum_{a \in E} P(\chi(\lambda) \in a) = \sum_{a \in E} \frac{1}{n} =$$

$$= |E| \cdot \frac{1}{n} = n\delta \cdot \frac{1}{n} = \delta$$

donde $P(\chi(\lambda) \in a) = \frac{1}{n}$, porque a es fijo, $\chi(\lambda)$ es uniformemente aleatorio en $\mathbb{F}_q^m$, y $|\mathbb{F}_q^m| = q^m = n$.
Entonces, la varianza será

$$\mathrm{Var}(x_E^\lambda) = \mathbb{E}((x_E^\lambda)^2) - \mathbb{E}(x_E^\lambda)^2 = \mathbb{E}(x_E^\lambda) - \mathbb{E}(x_E^\lambda)^2 = \delta - \delta^2.$$

Finalmente, consideramos la variable aleatoria

$$x = \sum_{\lambda \in \mathbb{F}_q^*} x_E^\lambda,$$

que cuenta el número de consultas que llegan a coordenadas con errores. Por independencia, tenemos que la esperanza y la varianza son

$$\mathbb{E}(x) = (q-1)\delta$$

$$\mathrm{Var}(x) = (q-1)(\delta - \delta^2).$$

Con lo cual, utilizando la desigualdad de Chebyshev

$$P\left(x \geq \frac{(1-2\sigma)(q-1)}{2}\right) \leq P\left(|x - \mathbb{E}(x)| \geq \frac{(1-2\sigma)(q-1)}{2} - (q-1)\delta\right) =$$

$$= P\left(|x - \mathbb{E}(x)| \geq \frac{(q-1)(1-2(\sigma+\delta))}{2}\right) \leq \frac{4(q-1)(\delta-\delta^2)}{(q-1)^2(1-2(\sigma+\delta))^2} =$$

$$= \frac{4(\delta-\delta^2)}{(q-1)(1-2(\sigma+\delta))^2} = O_{\sigma,\delta}\left(\frac{1}{q}\right).$$

El número de consultas sigue siendo $(q-1)$, y la proporción de errores que vamos a poder corregir δ. Con esto hemos probado que $\mathcal{RM}_q(r,m)$ es un código $(q-1, \delta, O_{\sigma,\delta}\left(\frac{1}{q}\right))-$localmente corregible. □

Conclusión

Hemos visto en este trabajo que los códigos Reed-Muller se construyen a partir de las evaluaciones de los polinomios en m variables de grado menor o igual que r en todos los puntos de $\mathbb{F}_q^m$. Viendo esto, hemos podido saber que su longitud es el número de elementos de $\mathbb{F}_q^m$, es decir, q^m, y hemos podido calcular su dimensión que es el número de monomios reducidos de $\mathbb{F}_q[X_1, ..., X_m]^{(r)}$.
Hemos llegado también a que la distancia mínima de estos códigos es $(q - b)q^{m-a-1}$, donde $r = a(q-1) + b$ y $a, b \in \mathbb{N}_0$, acotándola inferiormente por la cota de footprint y comprobando que existe una palabra con ese peso.
Hemos estudiado un algoritmo de corrección de errores para códigos Reed-Muller binarios que va a poder corregir $2^{m-r-1} - 1$ errores, utilizando la paridad de las variedades.
Por último, gracias al estudio de los códigos localmente descodificables y a la comprobación de que los códigos sobre los que estamos trabajando son localmente descodificables hemos visto tres algoritmos de corrección local para códigos Reed-Muller, siendo el tercero el que muestra mejores parámetros.

Bibliografía

[1] David Cox, John Little, Donal O'shea, and Moss Sweedler. *Ideals, varieties, and algorithms*, volume 3. Springer, 1997.

[2] Olav Geil. On the second weight of generalized reed-muller codes. *Designs, Codes and Cryptography*, 48:323–330, 2008.

[3] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[4] C Munuera-J Tena. Codificación de la información, ed. *Universidad de Valladolid*, 1997.

[5] Sergey Yekhanin et al. Locally decodable codes. *Foundations and Trends® in Theoretical Computer Science*, 6(3):139–255, 2012.