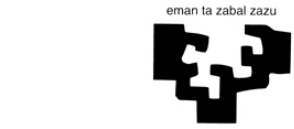

ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Códigos de Reed-Muller

Trabajo Fin de Grado
Grado en Matemáticas

Andoni De Arriba De La Hera

Trabajo dirigido por
María Asunción García Sánchez

Leioa, 20 de Junio de 2016

Índice general

Prefacio **v**

1. Nociones Básicas de la Teoría de Códigos Lineales **1**
1.1. Introducción 1
1.2. Códigos Lineales: Definiciones y Propiedades 2
1.3. Códigos Cíclicos: Definiciones y Propiedades 3
1.4. Problemas Resueltos 5

2. Códigos de Reed-Muller **9**
2.1. Aspectos Históricos 9
2.2. Construcción y Propiedades Generales 10
2.2.1. Códigos de Evaluación 10
2.2.2. Construcción General 11
2.3. Carácter Cíclico de los Códigos de Reed-Muller p-arios 19
2.4. Problemas Resueltos 23

3. Códigos de Reed-Muller Binarios **25**
3.1. Construcción Mediante Funciones Booleanas 25
3.2. Construcción Recursiva de Plotkin 27
3.3. Construcción Geométrica 31
3.3.1. Geometría Finita $EG(m, 2)$ 32
3.3.2. Interpretación Geométrica $\mathcal{RM}(r, m)$ 33
3.4. Problemas Resueltos 36

4. Codificación y Decodificación **39**
4.1. Generalidades 39
4.1.1. Codificación en Códigos Lineales y Cíclicos 39
4.1.2. Métodos Generales de Decodificación 40
4.2. Codificación en Códigos de Reed-Muller 41
4.3. Decodificación en Códigos de Reed-Muller: Algoritmo de Reed 43
4.4. Problemas Resueltos 46

A. Programación **47**

Bibliografía **53**

Prefacio

Esta memoria tiene como objetivo estudiar los códigos de Reed-Muller, que son una de las familias más antiguas y mejor conocidas entre los códigos lineales. Estos son un tipo muy especial de códigos detectores y correctores de errores, con ricas propiedades algebraicas, que se utilizan habitualmente en la transmisión de la información.

En la redacción de esta memoria han sido utilizados conceptos matemáticos explicados en las asignaturas *Álgebra Lineal y Geometría I*, *Matemática Discreta*, *Álgebra Lineal y Geometría II*, *Álgebra Conmutativa*, *Estructuras Algebraicas* y, por supuesto, *Códigos y Criptografía*. Todas ellas se cursan en el Grado en Matemáticas de la UPV/EHU.

Las referencias básicas que hemos consultado se encuentran recogidas en la Bilbliografía, que figura al final del documento. Al comienzo de cada capítulo se especifican aquellas que se han utilizado en la redacción del mismo. Sólo mencionar que este documento ha sido redactado con el fin de seguir una estructura análoga a [9].

Esta memoria consta de cuatro capítulos que se completan con un apéndice. En el primero de ellos, se realiza un resumen de los conceptos básicos sobre los códigos lineales. El segundo y tercer capítulo se dedican al estudio de los códigos de Reed-Muller, analizando primero el caso general y luego el caso binario. Pese a que históricamente la primera construcción fue la correspondiente al caso binario, se ha decidido presentar primero la construcción en cualquier cuerpo finito para evitar repetir las mismas ideas y tener así divido el trabajo en dos bloques, facilitando al lector la comprensión del mismo. El último capítulo muestra los procedimientos de codificación y decodificación para estos códigos en el caso binario. Además, al final de cada capítulo, pueden encontrarse los problemas resueltos, seleccionados con distintos objetivos (mostrar propiedades que no han sido desarrolladas en la parte teórica, resultados relacionados con el contenido del capítulo que se aplicarán posteriormente, construcción de ejemplos,...). Cabe destacar que la resolución de estos problemas junto con el diseño de los programas recogidos en el apéndice, más la elaboración personal de los capítulos, constituyen la aportación

y el trabajo personal del autor de esta memoria.

Como ya se ha indicado, en el Capítulo 1 se establecen las bases del trabajo, presentando las nociones básicas de la teoría de códigos lineales. Por tanto, se definen los llamados códigos lineales y códigos cíclicos, resaltando las principales propiedades de los mismos. Finalmente, en uno de los problemas resueltos, se presenta una construcción especial de ciertos códigos lineales que resultará útil en capítulos posteriores.

En el Capítulo 2 se presentan la construcción general y las principales propiedades de los códigos de Reed-Muller para cualquier cuerpo finito. Esta es una generalización de la construcción original que se dio en un principio para el caso binario. Hecho esto, se hace una breve introducción al carácter cíclico de estos códigos para cuando el cuerpo tiene característica un número primo.

En el Capítulo 3 pasamos al estudio de los códigos de Reed-Muller binarios. Se dan tres construcciones: la particularización de la construcción general vista en el capítulo anterior (la primera históricamente), la recursiva basada en una construcción estudiada en un problema del Capítulo 1 y la geométrica, que emplea geometrías finitas.

Finalmente, en el Capítulo 4 se recuerdan los métodos de codificación y decodificación generales en códigos lineales y cíclicos, y, una vez hecho eso, se establecen los procedimientos de codificación y decodificación para los códigos de Reed-Muller binarios. En particular, se presenta un método de decodificación propio para los códigos de Reed-Muller binarios.

Capítulo 1

Nociones Básicas de la Teoría de Códigos Lineales

El objetivo de este primer capítulo es el de recopilar las principales definiciones y propiedades estudiadas en la asignatura optativa de Cuarto del Grado en Matemáticas de la UPV/EHU *Códigos y Criptografía*. Estas serán necesarias para comprender correctamente los capítulos posteriores.

1.1. Introducción

Supongamos que un emisor desea enviar un mensaje $\mathbf{x}$ a través de un canal a un receptor. A lo largo de este proceso, este mensaje $\mathbf{x}$ suele verse alterado debido al "ruido" del canal, de manera que el mensaje recibido por el receptor pase a ser $\mathbf{x}'$, donde, en general, se tiene que $\mathbf{x}' \neq \mathbf{x}$.

Aquí es donde entran los llamados *códigos detectores y correctores de errores*. La idea consiste en que, antes de enviar el mensaje, el emisor lo *codifica* como $\mathbf{c}$, añadiéndole información redundante. De esta manera, si el canal produce un "ruido" $\mathbf{r}$ debido al cual el receptor recibe el mensaje alterado $\mathbf{c}' = \mathbf{c} + \mathbf{r}$, tras un proceso de *decodificación*, este es capaz de recuperar $\mathbf{c}$ y de ahí deducir $\mathbf{x}$. El objetivo de la teoría de los códigos detectores y correctores de errores es lograr que este proceso tenga éxito de la manera lo más eficiente posible (tanto en tiempo, como en memoria).

Es conveniente aclarar que, salvo que se diga lo contrario, nuestros mensajes serán vectores (que llamaremos *palabras*) del $\mathbb{F}_q$-espacio vectorial finito $\mathbb{F}_q^n$, siendo $q = p^s$ con p primo ($\mathbb{F}_q$ será lo que llamaremos *alfabeto*, y a sus elementos los denominaremos *letras*). Por simplicidad, siempre que no de lugar a confusión, denotaremos los elementos de $\mathbb{F}_q^n$ por:

$$\mathbf{x} = (x_1, x_2, ..., x_n) \underset{not.}{\equiv} x_1 x_2 \dots x_n.$$

De esta manera, podemos definir matemáticamente un código como un subconjunto (que suele denotarse por $\mathcal{C}$) no vacío de palabras (llamadas *palabras código*, que suelen denotarse por $\mathbf{c}$) de un mismo alfabeto.

1.2. Códigos Lineales: Definiciones y Propiedades

A primera vista, parece muy complicado trabajar con la definición de código desde el punto de vista matemático. Es por esta razón por la que se introducen los llamados códigos lineales.

Definición 1.2.1. Un *código lineal* $\mathcal{C}$ de longitud n y dimensión s sobre $\mathbb{F}_q$ es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$ de dimensión $s \leq n$.

Estos suelen llamarse habitualmente códigos lineales q-arios de longitud n y dimensión s.

La principal ventaja que tiene el uso de códigos lineales es que, por ser estos subespacios vectoriales de dimensión s, admiten bases de la forma $\mathcal{B} = \{\mathbf{c}_1, ..., \mathbf{c}_s\}$, tales que toda palabra código de $\mathcal{C}$ puede expresarse de manera única como combinación lineal de elementos de $\mathcal{B}$. Así, escribiendo $\mathbf{c}_i = c_{i1}...c_{in}$, para todo $i \in \{1, ..., s\}$, podemos construir la matriz $G \in \in \mathrm{Mat}_{s\times n}(\mathbb{F}_q)$ dada por:

$$G = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{s1} & c_{s2} & \cdots & c_{sn} \end{pmatrix}.$$

Esta se conoce por *matriz generadora* de $\mathcal{C}$. Es evidente que para toda palabra código $\mathbf{c} \in \mathcal{C}$, existen únicos escalares $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_q$ tales que $\mathbf{c} = (\alpha_1 \ldots \alpha_s)G$. Por tanto, para dar un código lineal, basta dar una matriz generadora del mismo.

Recordemos que se define por *distancia de Hamming* entre dos palabras $\mathbf{x}$ e $\mathbf{y}$ de igual longitud (que se trata de una distancia en el sentido topológico) al entero no negativo

$$d(\mathbf{x}, \mathbf{y}) = |\{i \in \{1, ..., n\} \mid x_i \neq y_i\}|. \tag{1.1}$$

Por otra parte, se define como *peso* de una palabra $\mathbf{x}$ al entero no negativo

$$\omega(\mathbf{x}) = |\{i \in \{1, ..., n\} \mid x_i \neq 0\}|. \tag{1.2}$$

Dado un código $\mathcal{C}$ cualquiera, a partir de (1.1) y (1.2) podemos definir

$$\omega \underset{not.}{\equiv} \omega(\mathcal{C}) = \min\{\omega(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \ \wedge \ \mathbf{c} \neq \mathbf{0}\}$$

y

$$d \underset{not.}{\equiv} d(\mathcal{C}) = \min\{d(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in \mathcal{C} \ \wedge \ \mathbf{c} \neq \mathbf{c}'\},$$

donde d se conoce como *distancia mínima* del código $\mathcal{C}$, mientras que ω es el llamado *peso mínimo* del código $\mathcal{C}$. Si $\mathcal{C}$ es lineal, se demuestra que $d = \omega$.

Se dice que un código lineal $\mathcal{C}$ *detecta s errores* si, recibida $\mathbf{y} = \mathbf{c} + \mathbf{e}$ ($\mathbf{c}$ palabra código enviada y $\mathbf{e}$ error dado en la transmisión) con $\omega(\mathbf{e}) \leq s$, entonces podemos asegurar que $\mathbf{y} \notin \mathcal{C}$. A su vez, decimos que un código lineal $\mathcal{C}$ *corrige t errores* si, recibida $\mathbf{y} = \mathbf{c} + \mathbf{e}$ ($\mathbf{c}$ palabra código enviada y $\mathbf{e}$ error dado en la transmisión), se cumple que toda palabra código $\mathbf{c}' \in \mathcal{C}$ ($\mathbf{c} \neq \mathbf{c}'$) verifica que $d(\mathbf{y}, \mathbf{c}') > t$. Se sabe que cualquier código $\mathcal{C}$ detecta hasta $d - 1$ errores, mientras que corrige hasta $\lfloor \frac{d-1}{2} \rfloor$.

Es también necesario introducir el concepto de códigos equivalentes. Se dice que dos códigos $\mathcal{C}$ y $\mathcal{C}'$ son *equivalentes* si pueden obtenerse las palabras de uno de ellos a partir de las palabras del otro realizando una combinación finita de las operaciones siguientes: permutar entre sí las letras de dos posiciones fijadas de todas las palabras código, o aplicar, en una posición fijada, una biyección de las letras a todas las palabras código. Cabe observar que una condición necesaria para que dos códigos sean equivalentes es que sus distancias mínimas coincidan. Lo mismo sucede con los pesos mínimos si estos resultan ser códigos lineales.

Finalmente, se define como *código dual* de un código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$ de dimensión s, el cual suele denotarse por $\mathcal{C}^\perp$, al conjunto

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid < \mathbf{x}, \mathbf{c} >= 0, \quad \forall \mathbf{c} \in \mathcal{C}\},$$

donde $<\cdot, \cdot>$ denota el producto escalar en $\mathbb{F}_q^n$. Si se cumple que $\mathcal{C} = \mathcal{C}^\perp$, decimos que $\mathcal{C}$ es un *código autodual*. El código dual $\mathcal{C}^\perp$ de un código lineal $\mathcal{C}$ de longitud n y dimensión s es también un código lineal de longitud n, pero de dimensión $n - s$. Por tanto, se cumple que $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = n$. Este hecho nos permite afirmar que $\mathcal{C}^\perp$ admite una matriz generadora $H \in \in \mathrm{Mat}_{(n-s)\times n}(\mathbb{F}_q)$. A esta matriz H se la conoce como *matriz de control* del código lineal $\mathcal{C}$. Entre las propiedades más importantes de H destaca que podemos definir $\mathcal{C}$ a partir de esta. En efecto, se tiene que

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H^T = \mathbf{0}\}.$$

Otra propiedad a tener en cuenta es que $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Esto se debe a que toda matriz generadora G de $\mathcal{C}$ y toda matriz de control H de $\mathcal{C}$ están relacionadas mediante la igualdad $GH^T = 0$, que equivale a que $HG^T = 0$.

1.3. Códigos Cíclicos: Definiciones y Propiedades

Un caso particular de los códigos lineales que merece ser mencionado es el de los llamados códigos cíclicos. Para estos, con el objetivo de facilitar el

desarrollo posterior, dada una palabra $\mathbf{x}$ de longitud n, denotaremos, para cada $i \in \{0, 1, ..., n-1\}$,

$$\mathbf{x}^{(i)} = (x_{n-i}, x_{n-i+1}, ..., x_{n-1}, x_0, ..., x_{n-i-1}) \underset{not.}{\equiv}$$

$$\underset{not.}{\equiv} x_{n-i}x_{n-i+1}\dots x_{n-1}x_0...x_{n-i-1},$$

siendo

$$\mathbf{x}^{(0)} = \mathbf{x} = (x_0, x_1, ..., x_{n-1}) \underset{not.}{\equiv} x_0x_1\dots x_{n-1}.$$

Definición 1.3.1. Sea $\mathcal{C}$ un código lineal q-ario de longitud n y dimensión s. Se dice que $\mathcal{C}$ es un *código cíclico* si se cumple que

$$\forall \mathbf{c} \in \mathcal{C} \Longrightarrow \mathbf{c}^{(1)} \in \mathcal{C}. \tag{1.3}$$

La forma más habitual de trabajar con los códigos cíclicos es empleando el anillo cociente $\mathbb{F}_q[x]/(x^n-1)$ junto con el epimorfismo de anillos

$$\begin{array}{rccl} \varphi\colon & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/(x^n-1) \\ & \mathbf{y} & \longmapsto & \varphi(\mathbf{y}) = y_0 + y_1x + \cdots + y_{n-1}x^{n-1}. \end{array}$$

Dado un código lineal $\mathcal{C}$ de longitud n y dimensión s, definimos como $\mathcal{C}(x)$ a la imagen directa a través de φ de $\mathcal{C}$, es decir $\mathcal{C}(x) = \{c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \mid c_0c_1...c_{n-1} \in \mathcal{C}\}$. El interés en este tipo particular de códigos lineales radica en la relación existente entre los códigos cíclicos de longitud n y los ideales del anillo cociente $\mathbb{F}_q[x]/(x^n-1)$. En efecto, se tiene que $\mathcal{C}$ es un código cíclico si, y sólo si, $\mathcal{C}(x)$ es un ideal del anillo cociente $\mathbb{F}_q[x]/(x^n-1)$. Este hecho nos permite garantizar la existencia y unicidad de un polinomio mónico $g(x)$ de grado lo menor posible tal que $\mathcal{C}(x) = (g(x))$ y $g(x)|(x^n-1)$ cuando $\mathcal{C}$ es un código cíclico. A este polinomio $g(x)$ se le conoce por *polinomio generador* de $\mathcal{C}$. Tal y como sugiere su nombre, este sirve para determinar una matriz generadora. En efecto, si $g(x) = \sum_{i=0}^{r} g_ix^i$ es el polinomio generador de grado r del código cíclico $\mathcal{C}$, se puede probar que una matriz generadora $G \in \mathrm{Mat}_{s\times n}(\mathbb{F}_q)$ del mismo viene dada por:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_r \end{pmatrix}.$$

Destacamos de esta matriz que la longitud y dimensión de $\mathcal{C}$ están relacionadas con el grado de su polinomio generador $g(x)$ mediante la igualdad $n = r + s$. Además, es fácil ver que $g_0 \neq 0$.

Por otro lado, al polinomio mónico $h(x)$ tal que $h(x)g(x) = x^n - 1$ se le conoce como *polinomio de control* de $\mathcal{C}$. Este tiene grado s, y nos sirve para

determinar una matriz de control. En efecto, si $h(x) = \sum_{i=0}^{s} h_i x^i$ es el polinomio de control del código cíclico $\mathcal{C}$, se puede probar que una matriz de control $H \in \mathrm{Mat}_{r\times n}(\mathbb{F}_q)$ viene dada por:

$$H = \begin{pmatrix} h_s & h_{s-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_s & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_s & h_{s-1} & h_{s-2} & \cdots & h_0 \end{pmatrix}.$$

Más aún, se tiene que el código dual de un código cíclico va a ser también cíclico, pero con polinomio generador $h_1(x) = h_0^{-1} x^s h(x^{-1})$, donde h_0^{-1} denota al inverso de h_0 en $\mathbb{F}_q$.

1.4. Problemas Resueltos

Problema 1.1. Sean $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ dos códigos lineales de distancia mínima d_i, dimensión k_i y matriz generadora $G_i \in \mathrm{Mat}_{k_i\times n}(\mathbb{F}_q)$, siendo $i \in \{1, 2\}$.

(i) Demostrar que

$$\mathcal{C}_1 + \mathcal{C}_2 = \{\mathbf{c}_1 + \mathbf{c}_2 \mid \mathbf{c}_i \in \mathcal{C}_i,\ i \in \{1, 2\}\}$$

es un código lineal con distancia mínima $d \leq \min\{d_1, d_2\}$.

(ii) Probar que si $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0 \ldots 0\}$, entonces $\dim(\mathcal{C}_1 + \mathcal{C}_2) = k_1 + k_2$ y una matriz generadora de $\mathcal{C}_1 + \mathcal{C}_2$ viene dada por $G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$.

Solución.

(i) Por Álgebra Lineal, si $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ son $\mathbb{F}_q$-subespacios de $\mathbb{F}_q^n$, entonces $\mathcal{C}_1 + \mathcal{C}_2$ es también un $\mathbb{F}_q$-subespacio de $\mathbb{F}_q^n$. Consecuentemente, $\mathcal{C}_1 + \mathcal{C}_2$ es un código lineal. La desigualdad entre las distancias mínimas es consecuencia de (1.2) y de que $\mathcal{C}_i \subseteq \mathcal{C}_1 + \mathcal{C}_2$, para $i \in \{1, 2\}$, pues

$$d = \omega = \min\{\omega(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 + \mathcal{C}_2 \ \wedge\ \mathbf{c} \neq \mathbf{0}\} =$$

$$= \min\{\omega(\mathbf{c}_1 + \mathbf{c}_2) \mid (\mathbf{c}_1 \in \mathcal{C}_1 \ \wedge\ \mathbf{c}_2 \in \mathcal{C}_2) \ \wedge\ \mathbf{c}_1 + \mathbf{c}_2 \neq \mathbf{0}\} \leq$$

$$\leq \min\{\omega(\mathbf{c}_i) \mid \mathbf{c}_i \in \mathcal{C}_i \ \wedge\ \mathbf{c}_i \neq \mathbf{0}\} = \omega_i = d_i, \quad \forall i \in \{1, 2\}.$$

Luego $d \leq \min\{d_1, d_2\}$.

(ii) La primera igualdad es inmediata, ya que, por ser estos tres conjuntos subespacios vectoriales finitos, se tiene que

$$\dim(\mathcal{C}_1 + \mathcal{C}_2) = \dim(\mathcal{C}_1) + \dim(\mathcal{C}_2) - \dim(\mathcal{C}_1 \cap \mathcal{C}_2).$$

Sustituyendo

$$\dim(\mathcal{C}_1 + \mathcal{C}_2) = k_1 + k_2 - \dim(\{0 \dots 0\}) = k_1 + k_2.$$

Además, si $\mathcal{B}_1 = \{\mathbf{c}_{11}, ..., \mathbf{c}_{1k_1}\}$ y $\mathcal{B}_2 = \{\mathbf{c}_{21}, ..., \mathbf{c}_{2k_2}\}$ son bases, respectivamente, de $\mathcal{C}_1$ y $\mathcal{C}_2$ tales que las matrices generadoras asociadas a estas son G_1 y G_2, entonces $\mathcal{B} = \{\mathbf{c}_{11}, ..., \mathbf{c}_{1k_1}, \mathbf{c}_{21}, ..., \mathbf{c}_{2k_2}\}$ es también una base de $\mathcal{C}_1 + \mathcal{C}_2$ por ser $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0 \dots 0\}$. Así, la matriz generadora asociada a esta es, precisamente, G.

□

Problema 1.2. Sean $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$ códigos lineales de longitud n_i, distancia mínima d_i, dimensión k_i, matriz generadora $G_i \in \mathrm{Mat}_{k_i \times n_i}(\mathbb{F}_q)$ y matriz de control $H_i \in \mathrm{Mat}_{(n-k_i)\times n}(\mathbb{F}_q)$, siendo $i \in \{1, 2\}$. Demostrar que la *concatenación* de $\mathcal{C}_1$ con $\mathcal{C}_2$, dada por:

$$\mathcal{C}_1 * \mathcal{C}_2 = \{\mathbf{c}_1 * \mathbf{c}_2 = c_{11}...c_{1n_1}c_{21}...c_{2n_2} \mid \mathbf{c}_i \in C_i,\ i \in \{1, 2\}\},$$

es un código lineal de longitud $n_1 + n_2$, dimensión $k_1 + k_2$, distancia mínima $d = \min\{d_1, d_2\}$, matriz generadora $G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ y matriz de control $H = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$.

Solución. Veamos primero que $\mathcal{C}_1 * \mathcal{C}_2$ es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^{n_1+n_2}$. En efecto, basta observar que $\mathcal{C}_1 * \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1+n_2}$ y que, dados $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_1 * \mathcal{C}_2$ y $\alpha, \beta \in \mathbb{F}_q$ arbitrarios, entonces $\alpha\mathbf{c} + \beta\mathbf{c}' \in \mathcal{C}_1 * \mathcal{C}_2$. Ambas condiciones son consecuencia inmediata de la definición de concatenación de códigos lineales.

Sean $\mathcal{B}_1 = \{\mathbf{c}_{11}, ..., \mathbf{c}_{1k_1}\}$ y $\mathcal{B}_2 = \{\mathbf{c}_{21}, ..., \mathbf{c}_{2k_2}\}$ bases, respectivamente, de $\mathcal{C}_1$ y $\mathcal{C}_2$. Entonces, el conjunto $\mathcal{B} = \{\mathbf{c}_{11} * \mathbf{0}, ..., \mathbf{c}_{1k_1} * \mathbf{0}, \mathbf{0} * \mathbf{c}_{21}, ..., \mathbf{0} * \mathbf{c}_{2k_2}\}$ es una base de $\mathcal{C}_1 * \mathcal{C}_2$, ya que se trata de un conjunto linealmente independiente y genera nuestro código por como se define la concatenación de palabras. Así, dado que la dimensión de un código lineal es el cardinal de una base de este, se tiene que $\dim(\mathcal{C}_1 * \mathcal{C}_2) = k_1 + k_2$. Por como se construyen las matrices generadoras, es inmediato que G es una matriz generadora de $\mathcal{C}_1 * \mathcal{C}_2$. Además, H es una matriz de control de $\mathcal{C}_1 * \mathcal{C}_2$, pues $GH^T = 0$.

Calculemos ahora la distancia mínima del código $\mathcal{C}_1 * \mathcal{C}_2$ en términos de las distancias mínimas de los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$. Es inmediato observar por (1.2) que, dados $\mathbf{c}_1 \in \mathcal{C}_1$ y $\mathbf{c}_2 \in \mathcal{C}_2$ arbitrarios, entonces $\omega(\mathbf{c}_1 * \mathbf{c}_2) = \omega(\mathbf{c}_1) + \omega(\mathbf{c}_2)$. Luego

$$\omega(\mathbf{c}_1 * \mathbf{c}_2) = \omega(\mathbf{c}_1) + \omega(\mathbf{c}_2) \geq \max\{\omega(\mathbf{c}_1), \omega(\mathbf{c}_2)\} \geq \min\{\omega_1, \omega_2\} =$$

$$= \min\{d_1, d_2\},$$

y tomando el mínimo de los pesos $\omega(\mathbf{c}_1 * \mathbf{c}_2) \neq \mathbf{0}$ tales que $\mathbf{c} = \mathbf{c}_1 * \mathbf{c}_2 \in \mathcal{C}_1 * \mathcal{C}_2$, se sigue que $d \geq \min\{d_1, d_2\}$. Por otra parte, como $\omega(\mathcal{C}_1) = \omega_1$, sabemos que existe $\mathbf{c}_1 \in \mathcal{C}_1$ tal que $\omega(\mathbf{c}_1) = \omega_1$. Por tanto, tomando $\mathbf{c} = \mathbf{c}_1 * \mathbf{0} \in \mathcal{C}_1 * \mathcal{C}_2$, se sigue que $d \leq \omega(\mathbf{c}) = d_1$. Análogamente, como $\omega(\mathcal{C}_2) = \omega_2$, sabemos que existe $\mathbf{c}_2 \in \mathcal{C}_2$ tal que $\omega(\mathbf{c}_2) = \omega_2$. Por consiguiente, tomando $\mathbf{c} = \mathbf{0} * \mathbf{c}_2 \in$ $\in \mathcal{C}_1 * \mathcal{C}_2$, se sigue que $d \leq \omega(\mathbf{c}) = d_2$. De aquí se comprueba inmediatamente que $d \leq \min\{d_1, d_2\}$, y por tanto concluimos que $d = \min\{d_1, d_2\}$ según lo ya visto. □

Problema 1.3. Sean $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ dos códigos lineales de distancia mínima d_i, dimensión k_i, matriz generadora $G_i \in \mathrm{Mat}_{k_i \times n}(\mathbb{F}_q)$ y matriz de control $H_i \in \mathrm{Mat}_{(n-k_i)\times n}(\mathbb{F}_q)$, siendo $i \in \{1, 2\}$. Demostrar que

$$\mathcal{C}_1 \circledast \mathcal{C}_2 = \{(\mathbf{c}_1 | \mathbf{c}_1 + \mathbf{c}_2) | \mathbf{c}_i \in \mathcal{C}_i,\ i \in \{1, 2\}\},$$

donde $(\mathbf{c}_1 | \mathbf{c}_1 + \mathbf{c}_2) = \mathbf{c}_1 * (\mathbf{c}_1 + \mathbf{c}_2) = \mathbf{c}_1 * \mathbf{c}_1 + \mathbf{0} * \mathbf{c}_2$, para $\mathbf{c}_1 \in \mathcal{C}_1$ y $\mathbf{c}_2 \in \mathcal{C}_2$, es un código lineal de longitud $2n$, dimensión $k_1 + k_2$, distancia mínima $d = \min\{2d_1, d_2\}$, matriz generadora $G = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$ y matriz de control $H = \begin{pmatrix} H_1 & 0 \\ -H_2 & H_2 \end{pmatrix}$.

Solución. Veamos para empezar que $\mathcal{C}_1 \circledast \mathcal{C}_2$ es un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^{2n}$. En efecto, $\mathcal{C}_1 \circledast \mathcal{C}_2 \subseteq \mathbb{F}_q^{2n}$ por como están definidos los elementos de $\mathcal{C}_1 \circledast \mathcal{C}_2$, y dados $\mathbf{c} = (\mathbf{c}_1 | \mathbf{c}_1 + \mathbf{c}_2)$, $\mathbf{c}' = (\mathbf{c}_1' | \mathbf{c}_1' + \mathbf{c}_2') \in \mathcal{C}_1 \circledast \mathcal{C}_2$ y $\alpha, \beta \in \mathbb{F}_q$ arbitrarios, tenemos que

$$\alpha\mathbf{c} + \beta\mathbf{c}' = \alpha(\mathbf{c}_1 | \mathbf{c}_1 + \mathbf{c}_2) + \beta(\mathbf{c}_1' | \mathbf{c}_1' + \mathbf{c}_2') =$$

$$= (\alpha\mathbf{c}_1 + \beta\mathbf{c}_1' | (\alpha\mathbf{c}_1 + \beta\mathbf{c}_1') + (\alpha\mathbf{c}_2 + \beta\mathbf{c}_2')) \in \mathcal{C}_1 \circledast \mathcal{C}_2,$$

Supongamos ahora que $\mathcal{B}_1 = \{\mathbf{c}_{11}, ..., \mathbf{c}_{1k_1}\}$ y $\mathcal{B}_2 = \{\mathbf{c}_{21}, ..., \mathbf{c}_{2k_2}\}$ son bases, respectivamente, de $\mathcal{C}_1$ y $\mathcal{C}_2$. Afirmamos que $\mathcal{B} = \{\mathbf{c}_{11} * \mathbf{c}_{11}, ..., \mathbf{c}_{1k_1} * \mathbf{c}_{1k_1}, \mathbf{0} * * \mathbf{c}_{21}, ..., \mathbf{0} * \mathbf{c}_{2k_2}\}$ es una base de $\mathcal{C}_1 \circledast \mathcal{C}_2$. En efecto, como $\mathcal{B}_1$ es base de $\mathcal{C}_1$, para cada $\mathbf{c}_1 \in \mathcal{C}_1$ arbitrario existen únicos $\alpha_1, ..., \alpha_{k_1} \in \mathbb{F}_q$ tales que $\mathbf{c}_1 = \alpha_1\mathbf{c}_{11} + \cdots + \alpha_{k_1}\mathbf{c}_{1k_1}$. Análogamente, como $\mathcal{B}_2$ es base de $\mathcal{C}_2$, para cada $\mathbf{c}_2 \in \mathcal{C}_2$ existen únicos $\beta_1, ..., \beta_{k_2} \in \mathbb{F}_q$ tales que $\mathbf{c}_2 = \beta_1\mathbf{c}_{21} + \cdots + \beta_{k_2}\mathbf{c}_{2k_2}$. Entonces

$$(\mathbf{c}_1 | \mathbf{c}_1 + \mathbf{c}_2) = \mathbf{c}_1 * (\mathbf{c}_1 + \mathbf{c}_2) =$$

$$= (\alpha_1\mathbf{c}_{11} + \cdots + \alpha_{k_1}\mathbf{c}_{1k_1}) * ((\alpha_1\mathbf{c}_{11} + \cdots + \alpha_{k_1}\mathbf{c}_{1k_1}) + (\beta_1\mathbf{c}_{21} + \cdots + \beta_{k_2}\mathbf{c}_{2k_2})) =$$

$$= \alpha_1(\mathbf{c}_{11} * \mathbf{c}_{11}) + \cdots + \alpha_{k_1}(\mathbf{c}_{1k_1} * \mathbf{c}_{1k_1}) + \beta_1(\mathbf{0} * \mathbf{c}_{21}) + \cdots + \beta_{k_2}(\mathbf{0} * \mathbf{c}_{2k_2}).$$

Por tanto $\mathcal{B}$ es un sistema generador de $\mathcal{C}_1 \circledast \mathcal{C}_2$. Además, $\mathcal{B}$ es libre por como se define la concatenación de palabras. En resumen, $\mathcal{B}$ es una base de

$\mathcal{C}_1 \circledast \mathcal{C}_2$, de donde se sigue que $\dim(\mathcal{C}_1 \circledast \mathcal{C}_2) = k_1 + k_2$. Una vez más, por como se definen las matrices generadoras, usando esta base observamos que G es una matriz generadora de $\mathcal{C}_1 \circledast \mathcal{C}_2$. A partir de este hecho ver que H es una matriz de control de $\mathcal{C}_1 \circledast \mathcal{C}_2$ se reduce a probar que $GH^T = 0$.

Pasemos a estudiar la relación entre las distancias mínimas del código $\mathcal{C}_1 \circledast \mathcal{C}_2$ y las distancias mínimas de los códigos $\mathcal{C}_1$ y $\mathcal{C}_2$. Sean $\mathbf{c} = (\mathbf{c}_1|\mathbf{c}_1 + \mathbf{c}_2)$, $\mathbf{c}' = (\mathbf{c}'_1|\mathbf{c}'_1 + \mathbf{c}'_2) \in \mathcal{C}_1 \circledast \mathcal{C}_2$ cualesquiera. Tenemos por (1.1) que

$$d(\mathbf{c}, \mathbf{c}') = d(\mathbf{c}_1 * (\mathbf{c}_1 + \mathbf{c}_2), \mathbf{c}'_1 * (\mathbf{c}'_1 + \mathbf{c}'_2)) = d(\mathbf{c}_1, \mathbf{c}'_1) + d(\mathbf{c}_1 + \mathbf{c}_2, \mathbf{c}'_1 + \mathbf{c}'_2) =$$

$$= \omega(\mathbf{c}_1 - \mathbf{c}'_1) + \omega((\mathbf{c}_1 - \mathbf{c}'_1) + (\mathbf{c}_2 - \mathbf{c}'_2))$$

Ahora bien, tomando $\mathbf{c}_2 = \mathbf{c}'_2$, entonces $d(\mathbf{c}, \mathbf{c}') = 2\omega(\mathbf{c}_1 - \mathbf{c}'_1) = 2d(\mathbf{c}_1, \mathbf{c}'_1) \geq$ $\geq 2d_1$. Mientras que si $\mathbf{c}_2 \neq \mathbf{c}'_2$, observamos que $d(\mathbf{c}, \mathbf{c}') \geq \omega(\mathbf{c}_2 - \mathbf{c}'_2) =$ $= d(\mathbf{c}_2, \mathbf{c}'_2) \geq d_2$. En cualquier caso $d(\mathbf{c}, \mathbf{c}') \geq \min\{2d_1, d_2\}$, para cualesquiera $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_1 \circledast \mathcal{C}_2$, de donde por definición de distancia mínima es $d \geq \min\{2d_1, d_2\}$. Nos falta por ver que $d \leq \min\{2d_1, d_2\}$, pero esto se sigue trivialmente de los dos hechos siguientes. Por una parte, de que $d \leq 2d_1$, puesto que si tomamos $\mathbf{c}_1 \in \mathcal{C}_1$ tal que $\omega(\mathbf{c}_1) = d_1$, entonces $\omega((\mathbf{c}_1|\mathbf{c}_1 + \mathbf{0})) = 2d_1 \geq d$. Y, por otra parte, de que $d \leq d_2$, pues si elegimos $\mathbf{c}_2 \in \mathcal{C}_2$ tal que $\omega(\mathbf{c}_2) = d_2$, entonces $\omega((\mathbf{0}|\mathbf{0} + \mathbf{c}_2)) = d_2 \geq d$. En definitiva, relacionando todo lo que hemos conseguido, se concluye que $d = \min\{2d_1, d_2\}$. □

Nota 1.4.1. Es inmediato observar que $\mathcal{C}_1 \circledast \mathcal{C}_2 \subseteq (\mathcal{C}_1 * \mathcal{C}_1) + (\{\mathbf{0}\} * \mathcal{C}_2)$.

Observación 1.4.1. Al código lineal $\mathcal{C}_1 \circledast \mathcal{C}_2$ se le conoce por *construcción de Plotkin*[*] de $\mathcal{C}_1$ con $\mathcal{C}_2$. Esta construcción tendrá una gran importancia en el Capítulo 3 a la hora de estudiar la construcción recursiva de los códigos de Reed-Muller binarios.

[*] *Morris Plotkin*, véase [7].

Capítulo 2

Códigos de Reed-Muller

En este capítulo se estudiarán la construcción general y las propiedades más importantes de los códigos de Reed-Muller desde un punto de vista general. La mayor parte del capítulo puede encontrarse en [6, Capítulo 12], aunque también se recogen algunos resultados de [2, Section 2.4]. Comenzaremos dando una visión histórica de su aparición.

2.1. Aspectos Históricos

Los *códigos de Reed-Muller* son una familia infinita de códigos, que toman su nombre de los dos matemáticos que los propusieron en el año 1954 al mismo tiempo, en trabajos independientes: I. S. Reed[*] y D. E. Muller[**]. Ambos centraron su estudio en los códigos de Reed-Muller binarios. Hoy se sabe que el primero en realizar su construcción fue Muller (el lector interesado puede consultar [10]), mientras que su estudio en detalle y la sencilla decodificación por la que son tan conocidos e importantes es obra de Reed (la información original puede hallarse en [5]). Posteriormente, estos fueron generalizados a cualquier cuerpo finito en 1968. Esta generalización puede encontrarse tanto en [4] como en [13].

Estos estudios están situados dentro en la Teoría de la Información, cuyas bases fueron establecidas por Shannon[***] a través de un artículo publicado en el *Bell System Technical Journal* en la década de los años 40 titulado *"A Mathematical Theory of Communication"*. Hoy día, la Teoría de la Información es una rama de las matemáticas y de la computación que se ocupa del estudio de la información y de todo lo relacionado con ella.

[*] *Irving Stoy Reed*, matemático e ingeniero estadounidense, 1923 - 2012.

[**] *David Eugene Muller*, matemático e informático teórico estadounidense, 1924 - 2008.

[***] *Claude Elwood Shannon*, matemático; ingeniero electrónico y criptógrafo estadounidense, 1916 - 2001.

Los códigos de Reed-Muller tienen una gran importancia en la historia. Su estudio en la década de los años 50 fue fundamental para que en los años posteriores se hiciesen grandes avances en la exploración espacial. Así, desde 1969 hasta 1977, todas las naves espaciales de la NASA iban equipadas con un código de Reed-Muller binario de longitud 32, dimensión 6 y distancia mínima 16. Se trataba por tanto de un código lineal de bajo coste debido a su pequeña dimensión en comparación a su longitud, y con buenas capacidades de corrección de errores por su elevada distancia mínima. Trabajaremos con dicho código en los **Problemas 3.1 y 4.1**.

Una de las misiones más destacadas que se llevo a cabo con el uso de estos códigos fue la de la sonda Mariner 9, que fue la primera que permitió la observación fotográfica de la superficie del planeta Marte. La sonda Mariner 9 fue lanzada hacia su destino el 30 de mayo de 1971, llegando a Marte el 13 de noviembre del mismo año, convirtiéndose así en la primera nave espacial en orbitar un planeta distinto al nuestro. Científicamente, esta misión, que constituyó una continuación de las observaciones de Marte adquiridas por las sondas Mariner 6 y 7, tenía como objetivo mostrar las primeras fotografías de la superficie marciana. En un principio la misión se complicó debido a las grandes tormentas de arena que se dieron sobre todo el conjunto de la superficie del planeta. Finalmente, en 1972, cuando por fin amainaron las tormentas, se obtuvieron las primeras fotografías claras del planeta que cambiaron completamente la visión que se tenía hasta entonces del planeta rojo. La sonda tomó fotografías en blanco y negro de $600 \times 600 = 3600$ píxeles, donde a cada píxel se le asignó una 6-tupla para representar el brillo. De esta manera, cada píxel era codificado como una palabra de longitud 32, esto es, se emplearon 26 bits de redundancia.

2.2. Construcción y Propiedades Generales

Empezaremos nuestro estudio dando una visión general de los códigos de Reed-Muller sobre cualquier cuerpo finito $\mathbb{F}_q$. En su forma general, estos constituyen una familia infinita de códigos que a su vez forman parte de un grupo mucho más amplio: los *códigos de evaluación*. Estos son, esencialmente, un tipo especial de códigos lineales, cuya construcción está basada en una determinada aplicación lineal.

2.2.1. Códigos de Evaluación

Vamos a denotar por χ a un conjunto de elementos, que llamaremos puntos (lo que habitualmente se conoce por *objeto geométrico*). Damos así la siguiente definición que recoge, entre otros, a los códigos de Reed-Muller.

Definición 2.2.1. Sean $\mathcal{P} = \{\mathbf{p}_1, ..., \mathbf{p}_n\}$ un subconjunto finito ($n \in \mathbb{N}$) de un cierto objeto geométrico χ y V un $\mathbb{F}_q$-espacio vectorial de aplicaciones $f\colon \chi \to \mathbb{F}_q$ (con las operaciones interna ($+$) y externa ($\cdot$) correspondientes). Se llama *evaluación en $\mathcal{P}$ de las aplicaciones de V* a la aplicación

$$\begin{array}{rccl} ev_{\mathcal{P}}\colon & V & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & ev_{\mathcal{P}}(f) = f(\mathbf{p}_1)\dots f(\mathbf{p}_n). \end{array}$$

Como V es un $\mathbb{F}_q$-espacio vectorial, si $ev_{\mathcal{P}}$ resulta ser una aplicación lineal, entonces su imagen directa $ev_{\mathcal{P}}(V)$ será un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q^n$, es decir, un código lineal de longitud n sobre $\mathbb{F}_q$ cuyas palabras son las imágenes de las aplicaciones de V a través de $ev_{\mathcal{P}}$. Bajo todas estas circunstancias, se conoce al código $ev_{\mathcal{P}}(V)$ así obtenido por *código de evaluación en $\mathcal{P}$ de las aplicaciones de V*. Los parámetros que definen al código pueden deducirse de las propiedades de V como $\mathbb{F}_q$-espacio vectorial.

Los códigos de Reed-Muller son un caso particular de códigos de evaluación, donde $\mathcal{P} = \chi = \mathbb{F}_q^m$ (que en este caso es un anillo conmutativo y unitario con estructura de $\mathbb{F}_q$-espacio vectorial) y $V = \mathbb{F}_q[x_1, ..., x_m]$ (que, además de ser un $\mathbb{F}_q$-espacio vectorial, también tiene estructura de anillo conmutativo y unitario). Para evitar confusiones en la notación, denotaremos a lo largo de este capítulo a los polinomios de $\mathbb{F}_q[x_1, ..., x_m]$ por $F = F(x_1, ..., x_m)$, reservando las letras minúsculas, entre otras, para las aplicaciones. Recordemos que el *grado de un polinomio* se define de manera general como el grado del monomio de mayor grado que lo forma, siendo el grado de un monomio la suma de los exponentes de todas las indeterminadas que este posee.

2.2.2. Construcción General

Pasamos ya a realizar la construcción general de los códigos de Reed-Muller q-arios. Para ello, son necesarios unos cuantos conceptos y resultados previos de la Teoría Generalizada de Boole[****].

Definición 2.2.2. Una *aplicación q-aria de m variables* es una aplicación $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$.

Se denota al conjunto de todas las aplicaciones q-arias de m variables por $\mathfrak{B}_m^q$.

Observaciones 2.2.1.

- Si se fija un orden en los $n = q^m$ elementos de $\mathbb{F}_q^m$, es posible describir toda aplicación q-aria $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ de manera unívoca a través de una tabla con todos los elementos de $\mathbb{F}_q^m$ y los respectivos valores que toma esta aplicación f en cada uno de estos. Una tabla de este tipo se llama *tabla de verdad asociada a f*.

[****] *George Boole*, matemático y lógico británico, 1815 - 1864.

- Podemos dotar a $\mathfrak{B}_m^q$ de una estructura de anillo conmutativo y unitario. En efecto, basta definir la operación interna suma $(+)$ como

$$\begin{array}{rccc} +: & \mathfrak{B}_m^q \times \mathfrak{B}_m^q & \longrightarrow & \mathfrak{B}_m^q \\ & (f,g) & \longmapsto & f+g, \end{array}$$

donde

$$(f+g)(u) = f(u) + g(u), \qquad \forall u \in \mathbb{F}_q^m,$$

y la operación interna producto $(\cdot)$ como

$$\begin{array}{rccc} \cdot: & \mathfrak{B}_m^q \times \mathfrak{B}_m^q & \longrightarrow & \mathfrak{B}_m^q \\ & (f,g) & \longmapsto & f \cdot g, \end{array}$$

donde

$$(f \cdot g)(u) = f(u)g(u), \qquad \forall u \in \mathbb{F}_q^m.$$

Más aún, si definimos la operación externa

$$\begin{array}{rccc} \cdot_{\mathbb{F}_q}: & \mathbb{F}_q \times \mathfrak{B}_m^q & \longrightarrow & \mathfrak{B}_m^q \\ & (\alpha, f) & \longmapsto & \alpha \cdot_{\mathbb{F}_q} f, \end{array}$$

donde

$$(\alpha \cdot_{\mathbb{F}_q} f)(u) = \alpha f(u), \qquad \forall u \in \mathbb{F}_q^m,$$

se tiene que $\mathfrak{B}_m^q$ también posee estructura de $\mathbb{F}_q$-espacio vectorial. Por simplicidad, denotaremos tanto la ley de composición interna producto como la operación externa simplemente por yuxtaposición, siempre que ello no dé lugar a dudas.

- Fijado un orden $\mathbb{F}_q^m = \{\mathbf{v}_1, ..., \mathbf{v}_n\}$ en los $n = q^m$ elementos de $\mathbb{F}_q^m$, dada $f \in \mathfrak{B}_m^q$, introducimos la notación siguiente:

$$f_i \underset{not.}{\equiv} f(\mathbf{v}_i), \qquad \forall i \in \{1, ..., n\}.$$

Llamaremos a este valor *coordenada i-ésima de f bajo el orden establecido*. Fijado un orden en $\mathbb{F}_q^m$, se observa que toda aplicación q-aria f puede identificarse de manera unívoca mediante el uso de tablas de verdad con la correspondiente palabra $f_1 \dots f_n \in \mathbb{F}_q^n$. Denotaremos a esta por $\mathbf{f}$. Así, bajo estas condiciones, podemos trabajar con el conjunto $\mathbb{F}_q^m = \{\mathbf{v}_1, ..., \mathbf{v}_n\}$ ordenado a la hora de hacer uso de aplicaciones q-arias. A la palabra $\mathbf{f} \in \mathbb{F}_q^n$ se la conoce por *palabra característica de f bajo el orden establecido*. En particular, se deduce de este hecho que $|\mathfrak{B}_m^q| = q^n = q^{q^m} < \infty$.

Ejemplo 2.2.1. En particular, cuando $q = 2$, se conoce a toda aplicación 2-aria de m variables por *función Booleana de m variables*. En estos casos, denotaremos por simplicidad al conjunto de las funciones Booleanas de m variables por $\mathfrak{B}_m$. Este conjunto es conocido como *Álgebra de Boole* con las operaciones antes definidas.

Dado un polinomio arbitrario $F \in \mathbb{F}_q[x_1, ..., x_m]$, como $|\mathbb{F}_q| = q < \infty$, es evidente que evaluando F en todos los elementos de $\mathbb{F}_q^m$ se induce una aplicación q-aria $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$. Este hecho nos da pie a dar la siguiente definición.

Definición 2.2.3. Sea $F \in \mathbb{F}_q[x_1, ..., x_m]$ un polinomio. Si $n = q^m$, se conoce por *aplicación polinómica asociada a* F a la aplicación q-aria $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ tal que, para cualquier m-tupla $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$, verifica que $f(a_1, \ldots, a_m) = = F(a_1, \ldots, a_m)$.

Nota 2.2.1. Se mantienen las notaciones antes establecidas para las aplicaciones q-arias de m variables con los polinomios $F \in \mathbb{F}_q[x_1, ..., x_m]$. En particular, fijado un orden $\mathbb{F}_q^m = \{\mathbf{v}_1, ..., \mathbf{v}_n\}$, llamaremos a la palabra característica inducida por la aplicación polinómica asociada a F como *palabra característica de* F *bajo el orden establecido*, e inducimos la notación siguiente:

$$F_i \underset{not.}{\equiv} F(\mathbf{v}_i), \qquad \forall i \in \{1, ..., n\}.$$

Denotaremos a esta palabra por $\mathbf{F}$. Conviene resaltar que, al igual que se hizo con las aplicaciones q-arias de m variables, podemos considerar tablas de verdad asociadas a polinomios de $\mathbb{F}_q[x_1, ..., x_m]$.

En lo que queda de sección, y salvo que se diga lo contrario, vamos a suponer que tenemos fijado un orden $\mathbb{F}_q^m = \{\mathbf{v}_1, ..., \mathbf{v}_n\}$ para los $n = q^m$ elementos de $\mathbb{F}_q^m$. De esta manera, podremos trabajar con las palabras de $\mathbb{F}_q^n$, en vez de emplear aplicaciones q-arias de m variables.

Bajo estas condiciones, podemos dar el siguiente resultado clave.

Proposición 2.2.1. *La aplicación evaluación en* $\mathbb{F}_q^m$ *de los polinomios de* $\mathbb{F}_q[x_1, ..., x_m]$ *en* $\mathbb{F}_q^n$ *dada por:*

$$\begin{array}{rccl} ev_{\mathbb{F}_q^m}\colon & \mathbb{F}_q[x_1, ..., x_m] & \longrightarrow & \mathbb{F}_q^n \\ & F & \longmapsto & ev_{\mathbb{F}_q^m}(F) = \mathbf{F} = F_1 \ldots F_n, \end{array} \tag{2.1}$$

es un epimorfismo de anillos, que además es lineal.

Demostración. Es evidente que $ev_{\mathbb{F}_q^m}$ es un homomorfismo de anillos por como está definido. En efecto:

- $ev_{\mathbb{F}_q^m}(1) \underset{not.}{\equiv} ev_{\mathbb{F}_q^m}(x_1^0 \cdots x_n^0) \underset{def.}{=} 1 \ldots 1 \underset{not.}{\equiv} \mathbf{1}$.
- $ev_{\mathbb{F}_q^m}(F + G) \underset{def.}{=} (F_1 + G_1) \ldots (F_n + G_n) = (F_1 \ldots F_n) + (G_1 \ldots G_n) \underset{def.}{=}$ $\underset{def.}{=} ev_{\mathbb{F}_q^m}(F) + ev_{\mathbb{F}_q^m}(G), \qquad \forall F, G \in \mathbb{F}_q[x_1, ..., x_m]$.
- $ev_{\mathbb{F}_q^m}(FG) \underset{def.}{=} (F_1 G_1) \ldots (F_n G_n) = (F_1 \ldots F_n)(G_1 \ldots G_n) \underset{def.}{=}$ $\underset{def.}{=} ev_{\mathbb{F}_q^m}(F) ev_{\mathbb{F}_q^m}(G), \qquad \forall F, G \in \mathbb{F}_q[x_1, ..., x_m]$.

Más aún, este es lineal para la operación externa correspondiente, puesto que, para todo $F \in \mathbb{F}_q[x_1, ..., x_m]$ y para todo $\alpha \in \mathbb{F}_q$, se tiene que

$$ev_{\mathbb{F}_q^m}(\alpha F) \underset{def.}{=} (\alpha F_1) \dots (\alpha F_n) = \alpha(F_1 \dots F_n) \underset{def.}{=} \alpha ev_{\mathbb{F}_q^m}(F).$$

Sólo falta probar que (2.1) es suprayectivo. Para verlo, dado $\mathbf{x} \in \mathbb{F}_q^n$ cualquiera, tenemos que ser capaces de encontrar un polinomio $F \in \mathbb{F}_q[x_1, ..., x_m]$ tal que $ev_{\mathbb{F}_q^m}(F) = \mathbf{x}$. Sea $\mathbf{x} \in \mathbb{F}_q^n$ arbitrario. Fijado el orden $\mathbb{F}_q^m = \{\mathbf{v}_1, ..., \mathbf{v}_n\}$, suponiendo que $\mathbf{v}_i = (\alpha_1^i, \dots, \alpha_m^i) \in \mathbb{F}_q^m$ (con $i \in \{1, ..., n\}$), definimos

$$F_{\mathbf{v}_i}(x_1, ..., x_m) = \prod_{j=1}^{m} (1 - (x_j - \alpha_j^i)^{q-1}) \in \mathbb{F}_q[x_1, ..., x_m], \qquad \forall i \in \{1, ..., n\}.$$

Es evidente por el **Teorema de Lagrange** que, para todo $\mathbf{w} \in \mathbb{F}_q^m$ y todo $i \in \{1, ..., n\}$, es

$$F_{\mathbf{v}_i}(\mathbf{w}) = \begin{cases} 1, & \text{si } \mathbf{w} = \mathbf{v}_i; \\ 0, & \text{si } \mathbf{w} \neq \mathbf{v}_i. \end{cases} \tag{2.2}$$

Por tanto, es inmediato comprobar por como se define la aplicación (2.1) que el conjunto $\mathcal{B} = \{ev_{\mathbb{F}_q^m}(F_{\mathbf{v}_i}) \mid i \in \{1, ..., n\}\}$ se corresponde con la base canónica de $\mathbb{F}_q^n$. En efecto, ya que por (2.2) tenemos que

$$\begin{array}{ccc} ev_{\mathbb{F}_q^m}(F_{\mathbf{v}_1}) & = & 100\dots00, \\ ev_{\mathbb{F}_q^m}(F_{\mathbf{v}_2}) & = & 010\dots00, \\ \vdots & \vdots & \vdots \\ ev_{\mathbb{F}_q^m}(F_{\mathbf{v}_n}) & = & 000\dots01. \end{array}$$

En consecuencia, por ser $\mathcal{B}$ una base de $\mathbb{F}_q^n$ y por la linealidad de $ev_{\mathbb{F}_q^m}$, existen escalares $k_i \in \mathbb{F}_q$ (con $i \in \{1, ..., n\}$) tales que

$$\mathbf{x} = \sum_{i=1}^{n} k_i ev_{\mathbb{F}_q^m}(F_{\mathbf{v}_i}) = ev_{\mathbb{F}_q^m}(\sum_{i=1}^{n} k_i F_{\mathbf{v}_i}).$$

Así, tomando $F = \sum_{i=1}^{n} k_i F_{\mathbf{v}_i}$, es evidente que $ev_{\mathbb{F}_q^m}(F) = \mathbf{x}$. □

Observación 2.2.1. El hecho de que $ev_{\mathbb{F}_q^m}$ sea suprayectiva implica que toda aplicación q-aria de m variables es polinómica. En efecto, toda aplicación q-aria de m variables está unívocamente determinada por las palabras de $\mathbb{F}_q^n$, y acabamos de probar que $ev_{\mathbb{F}_q^m}$ nos determina una aplicación suprayectiva entre $\mathbb{F}_q[x_1, ..., x_m]$ y $\mathbb{F}_q^n$. Sin embargo, es fácil comprobar que el recíproco no es cierto, esto es, distintos polinomios de $\mathbb{F}_q[x_1, ..., x_m]$ inducen la misma aplicación polinómica. Para obtener un contraejemplo, basta hacer uso del **Teorema de Lagrange**, dado que este nos dice que $\alpha^q = \alpha$, para todo $\alpha \in \mathbb{F}_q$, y por tanto los polinomios x_i y x_i^q (con $i \in \{1, ..., m\}$), pese a ser distintos, inducen la misma aplicación polinómica.

La **Observación 2.2.1** nos obliga a considerar el anillo cociente (que también posee estructura de $\mathbb{F}_q$-espacio vectorial) siguiente:

$$\mathcal{P}_m^q \underset{not.}{\equiv} \frac{\mathbb{F}_q[x_1, ..., x_m]}{(x_1^q - x_1, ..., x_m^q - x_m)}.$$

Se conocen a los elementos de este anillo cociente por *polinomios reducidos de la $\mathbb{F}_q$-álgebra* $\mathbb{F}_q[x_1, ..., x_m]$. Es evidente que cada clase de equivalencia $\overline{F} = F + (x_1^q - x_1, ..., x_m^q - x_m) \in \mathcal{P}_m^q$ posee un único representante

$$F^* \underset{not.}{\equiv} \sum a_{i_1 ... i_m} x_1^{i_1} \cdots x_m^{i_m},$$

verificando que $0 \leq i_1, ..., i_m \leq q-1$. Este polinomio F^* está unívocamente determinado reduciendo los exponentes de todas las indeterminadas módulo q, y tiene por tanto grado $m(q-1)$ a lo más. Diremos que un polinomio F *está en su forma reducida* cuando $F^* = F$.

Nota 2.2.2. El conjunto $\mathcal{B} = \{x_1^{r_1} \cdots x_m^{r_m} \mid r_i \in \{0, 1, \ldots, q-1\} \ , \ \forall i \in \in \{1, ..., m\}\}$ es una base del $\mathbb{F}_q$-espacio vectorial cociente $\mathcal{P}_m^q$. Por tanto, este es finito como $\mathbb{F}_q$-espacio vectorial. Llamaremos a los elementos de esta base monomios reducidos de la $\mathbb{F}_q$-álgebra $\mathbb{F}_q[x_1, ..., x_m]$.

Ejemplo 2.2.2. Si $q = 2$, podemos considerar los polinomios reducidos de la $\mathbb{F}_2$-álgebra $\mathbb{F}_2[x_1, ..., x_m]$, a los que llamaremos *polinomios Booleanos de m indeterminadas*. Según todo lo explicado, se obtienen los monomios Booleanos aplicando las reglas

$$\underbrace{x_i x_j = x_j x_i}_{\text{Conmutatividad en } \mathbb{F}_2[x_1,...,x_m]} \qquad \text{y} \qquad \underbrace{x_i^2 = x_i}_{\text{Pequeño Teorema de Fermat en } \mathbb{F}_2} \quad ,$$

para cualesquiera $i, j \in \{1, ..., m\}$ distintos ($i \neq j$), hasta que los factores que generan nuestro monomio sean diferentes. Consecuentemente, se obtienen los polinomios Booleanos aplicando estas reglas a cada uno de los monomios Booleanos que los forman. Por simplicidad, denotaremos por $\mathcal{P}_m$ al conjunto de los polinomios Booleanos de m indeterminadas. Además, con un simple argumento de combinatoria, es fácil ver que el número de monomios Booleanos de m indeterminadas de grado k es $\binom{m}{k}$. Así, el cardinal del conjunto de todos los monomios Booleanos de m indeterminadas viene dado por $\sum_{k=0}^{m} \binom{m}{k} = 2^m$, y se tiene por la **Nota 2.2.2** que $|\mathcal{P}_m| = 2^{2^m}$.

Lema 2.2.2. *Sea $F \in \mathbb{F}_q[x_1, ..., x_m]$. Si $F(\mathbf{v}) = 0$ para todo $\mathbf{v} \in \mathbb{F}_q^m$ (en particular $F^*(\mathbf{v}) = 0$ para todo $\mathbf{v} \in \mathbb{F}_q^m$), entonces $F^* \equiv 0$.*

Demostración. Vamos a razonar por inducción sobre el número de indeterminadas m. Si $m = 1$ el resultado es inmediato, ya que por hipótesis F^* tendría $q = |\mathbb{F}_q| > \deg(F^*)$ raíces, lo cual necesariamente implica que

$F^* \equiv 0$. Supongamos cierto el resultado para polinomios de $m-1$ indeterminadas, y probémoslo para todo polinomio de m indeterminadas. Sea $F \in \mathbb{F}_q[x_1, ..., x_m]$ arbitrario verificando que $F(\mathbf{v}) = 0$, para todo $\mathbf{v} \in \mathbb{F}_q^m$, y consideremos su polinomio reducido F^*. Agrupando los monomios de F^* con el mismo exponente en la indeterminada x_m, obtenemos que

$$F^* = G_0(x_1, ..., x_{m-1}) + \cdots + x_m^r G_r(x_1, ..., x_{m-1}), \tag{2.3}$$

donde $r < q$ y $G_0, \ldots, G_r \in \mathbb{F}_q[x_1, ..., x_m]$. Obsérvese que todos estos polinomios $G_0, \ldots, G_r$ están reducidos por estarlo F^*. Ahora, dado un vector $\mathbf{v} = (\alpha_1, ..., \alpha_{m-1}) \in \mathbb{F}_q^{m-1}$ arbitrario, definimos

$$F_{\mathbf{v}}(x_m) \underset{not.}{\equiv} F^*(\alpha_1, ..., \alpha_{m-1}, x_m) = G_0(\mathbf{v}) + \cdots + x_m^r G_r(\mathbf{v}) \in \mathbb{F}_q[x_m]. \tag{2.4}$$

Es inmediato observar que este polinomio es reducido y que por hipótesis tiene por raíces a todos los elementos de $\mathbb{F}_q$. Así, por el mismo razonamiento que hemos hecho en el caso de $m = 1$, será $F_{\mathbf{v}}(x_m) \equiv 0$. En consecuencia, igualando coeficientes en (2.4), tenemos que $G_i(\mathbf{v}) = 0$, para todo $i \in \{1, ..., r\}$. Pero como $\mathbf{v} \in \mathbb{F}_q^{m-1}$ es arbitrario, tenemos que todos los polinomios G_i verifican que $G_i(\mathbf{v}) = 0$, para todo $i \in \{1, ..., r\}$ y $\mathbf{v} \in \mathbb{F}_q^{m-1}$. Por tanto, aplicando la hipótesis de inducción a todos estos polinomios G_i (pues no olvidemos que son polinomios de $m-1$ indeterminadas), obtenemos que $G_i \equiv 0$, para todo $i \in \{1, ..., r\}$, de donde se sigue por (2.3) que $F^* \equiv 0$. □

Teorema 2.2.3. *Los conjuntos $\mathbb{F}_q^n$ y $\mathcal{P}_m^q$ son isomorfos como $\mathbb{F}_q$-álgebras. En consecuencia, cada polinomio de una misma clase de equivalencia determina la misma aplicación polinómica.*

Demostración. Consideremos la aplicación (2.1). Sabemos que esta es un epimorfismo de anillos en virtud de la **Proposición 2.2.1**, así que por el **Primer Teorema de Isomorfia de Anillos** se sigue que

$$\frac{\mathbb{F}_q[x_1, ..., x_m]}{\mathrm{Ker}(ev_{\mathbb{F}_q^m})} \cong \mathrm{Im}(ev_{\mathbb{F}_q^m}) = \mathbb{F}_q^n.$$

Veamos ahora que $\mathrm{Ker}(ev_{\mathbb{F}_q^m}) = (x_1^q - x_1, ..., x_m^q - x_m)$. En efecto, por la **Observación 2.2.1**, deducimos inmediatamente que $\mathrm{Ker}(ev_{\mathbb{F}_q^m}) \supseteq (x_1^q - x_1, ..., x_m^q - x_m)$. Para el otro contenido, se argumenta por reducción al absurdo: dado $F \in \mathrm{Ker}(ev_{\mathbb{F}_q^m})$ arbitrario, vamos a suponer que $F \notin (x_1^q - x_1, ..., x_m^q - x_m)$. Entonces $F = R(x_1, ..., x_m) + (x_1^q - x_1, ..., x_m^q - x_m)$, donde R es la forma reducida de F. Como $ev_{\mathbb{F}_q^m}(F) = \mathbf{0}$ (pues $F \in \mathrm{Ker}(ev_{\mathbb{F}_q^m})$), estamos ante las condiciones del **Lema 2.2.2**, luego $F^* = R \equiv 0$, en contra de la hipótesis hecha. Por tanto $\mathrm{Ker}(ev_{\mathbb{F}_q^m}) = (x_1^q - x_1, ..., x_m^q - x_m)$ y se cumple que

$$\mathcal{P}_m^q = \frac{\mathbb{F}_q[x_1, ..., x_m]}{(x_1^q - x_1, ..., x_m^q - x_m)} \cong \mathbb{F}_q^n,$$

donde recordemos que el propio **Teorema de Isomorfía** nos da explícitamente este isomorfismo, el cual es

$$\begin{array}{rccc} \overline{ev_{\mathbb{F}_q^m}}: & \mathcal{P}_m^q & \longrightarrow & \mathbb{F}_q^n \\ & \overline{F} & \longmapsto & \overline{ev_{\mathbb{F}_q^m}}(\overline{F}) = ev_{\mathbb{F}_q^m}(F). \end{array} \tag{2.5}$$

Sólo falta ver que este isomorfismo de anillos es también lineal, pero esto es consecuencia de la linealidad de $ev_{\mathbb{F}_q^m}$. En efecto, sólo tenemos que ver que se preserva el producto exterior (pues la suma se conserva por el hecho de ser este un isomorfismo de anillos), y esto se prueba rápidamente ya que, para todo $F \in \mathbb{F}_q[x_1, ..., x_m]$ y para todo $\alpha \in \mathbb{F}_q$, se cumple que

$$\overline{ev_{\mathbb{F}_q^m}}(\overline{\alpha F}) \underset{def.}{=} ev_{\mathbb{F}_q^m}(\alpha F) \underset{lineal.}{=} \alpha ev_{\mathbb{F}_q^m}(F) \underset{def.}{=} \alpha \overline{ev_{\mathbb{F}_q^m}}(\overline{F}).$$

En resumen, se tiene que la aplicación $\overline{ev_{\mathbb{F}_q^m}}$ que hemos obtenido es un isomorfismo entre $\mathbb{F}_q$-álgebras. □

Sea ahora $\mathcal{P}_m^q(r)$ el conjunto de los polinomios reducidos de m indeterminadas sobre $\mathcal{P}_m^q$ con grado menor o igual que r. Este es trivialmente un $\mathbb{F}_q$-subespacio vectorial de $\mathcal{P}_m^q$ de dimensión finita. Empleando entonces el **Teorema 2.2.3** que acabamos de probar, estamos en condiciones de dar la definición de código de Reed-Muller q-ario.

Definición 2.2.4. Dado $q = p^s$, con p primo, sean m y r dos números naturales tales que $r \leq m(q-1)$. Se define por *código de Reed-Muller q-ario* de orden r y longitud q^m, que denotaremos por $\mathcal{RM}_q(r, m)$, a la imagen directa de $\mathcal{P}_m^q(r)$ a través de la aplicación (2.5). Dicho de otra forma, se trata del conjunto de las palabras características de los polinomios de $\mathcal{P}_m^q$ con grado menor o igual que r.

Por convenio,

$$\mathcal{RM}_q(l, m) = \{0 \dots 0\}, \qquad \forall l < 0.$$

Ejemplo 2.2.3. Sean $m, s, p \in \mathbb{N}$, p primo, $q = p^s$ y $n = q^m$. Entonces,

$$\mathcal{RM}_q(m(q-1), m) = \mathbb{F}_q^n,$$

y

$$\mathcal{RM}_q(0, m) = \{\underbrace{0 \dots 0}_{n}, \underbrace{1 \dots 1}_{n}, \dots, \underbrace{q-1 \dots q-1}_{n}\}.$$

En efecto, la primera igualdad es consecuencia directa de que $\overline{ev_{\mathbb{F}_q^m}}$ sea una biyección, pues trivialmente $\mathcal{P}_m^q(m(q-1)) = \mathcal{P}_m^q$, mientras que la segunda igualdad se debe a que $\mathcal{P}_m^q(0) = \mathbb{F}_q$.

Observaciones 2.2.2. Como consecuencia de la **Definición 2.2.4**, se verifican los resultados siguientes:

- Todo código de Reed-Muller $\mathcal{RM}_q(r,m)$ es equivalente a otro código de Reed-Muller con los mismos parámetros si sólo se realizan permutaciones en las letras de dos posiciones fijadas en todas las palabras del código. Por tanto, dado un código de Reed-Muller $\mathcal{RM}_q(r,m)$ bajo un cierto orden en los elementos de $\mathbb{F}_q^m$, al cambiar dicho orden, obtenemos otro código de Reed-Muller, con los mismos parámetros, equivalente al anterior.

- Para todo par de enteros $i \leq j$ (con $i,j \in \{0,1,...,m(q-1)\}$), se tiene que $\mathcal{RM}_q(i,m) \subseteq \mathcal{RM}_q(j,m)$.

- Es evidente por el **Teorema 2.2.3** y por ser $\mathcal{P}_m^q(r)$ un $\mathbb{F}_q$-subespacio vectorial de $\mathcal{P}_m^q$ que $\mathcal{RM}_q(r,m)$ es un código lineal.

Proposición 2.2.4. *La matriz que tiene como filas las palabras características de los monomios reducidos de $\mathcal{P}_m^q(r)$ es una matriz generadora de $\mathcal{RM}_q(r,m)$.*

Demostración. Basta probar que las palabras características de todos los monomios reducidos de $\mathcal{P}_m^q(r)$ constituyen una base de $\mathcal{RM}_q(r,m)$. Es bien conocido que una base de $\mathcal{P}_m^q(r)$ está formada por los monomios que contiene. Por tanto, las palabras características de todos los monomios reducidos de este espacio constituyen un sistema generador de $\overline{ev_{\mathbb{F}_q^m}}(\mathcal{P}_m^q(r)) = \\ = \mathcal{RM}_q(r,m)$ por la linealidad de (2.5). Veamos que estas también forman un conjunto libre. Sean $F_1,\ldots,F_t \in \mathcal{P}_m^q(r)$ monomios reducidos distintos. Supongamos mediante un argumento de reducción al absurdo que existen $k_1,\ldots,k_t$ escalares, no todos nulos, tales que

$$k_1\overline{ev_{\mathbb{F}_q^m}}(F_1) + \cdots + k_t\overline{ev_{\mathbb{F}_q^m}}(F_t) = \mathbf{0}.$$

Esto es, que existe un conjunto de palabras características asociadas a algunos monomios reducidos de $\mathcal{P}_m^q(r)$ linealmente dependientes. Entonces, por la linealidad de $\overline{ev_{\mathbb{F}_q^m}}$,

$$\overline{ev_{\mathbb{F}_q^m}}(k_1F_1 + \cdots + k_tF_t) = k_1\overline{ev_{\mathbb{F}_q^m}}(F_1) + \cdots + k_t\overline{ev_{\mathbb{F}_q^m}}(F_t) = \mathbf{0}.$$

Ahora bien, como la suma de monomios reducidos es un polinomio reducido, por el **Lema 2.2.2**, se tiene que necesariamente $k_1F_1 + \cdots + k_tF_t$ se corresponde con el polinomio idénticamente nulo. Así, dado que todos los monomios $F_1,\ldots,F_t$ son distintos, forzosamente $k_1 = \cdots = k_t = 0$, contradiciendo que, precisamente, estos escalares no pueden ser todos nulos bajo la hipótesis hecha. En consecuencia, todo conjunto de palabras características asociadas a monomios reducidos de $\mathcal{P}_m^q(r)$ ha de ser linealmente independiente, y por tanto, en particular, las palabras características de todos los monomios reducidos son linealmente independientes. □

Corolario 2.2.5. *La dimensión de $\mathcal{RM}_q(r,m)$ como $\mathbb{F}_q$-subespacio vectorial es el número de soluciones de las ecuaciones $i_1 + \cdots + i_m = t$ tales que*

$0 \leq i_1, ..., i_m \leq q-1$, *para todo* t *variando en el conjunto* $\{0, 1, ..., r\}$. *Esto es,*

$$\dim(\mathcal{RM}_q(r,m)) = \sum_{t=0}^{r} |\{(i_1, \ldots, i_m) \mid i_1 + \cdots + i_m = t \ , \ 0 \leq i_j \leq q-1\}|.$$

Demostración. Por la **Proposición 2.2.4**, basta probar que el número de monomios reducidos de $\mathcal{P}_m^q(r)$ coincide con el número de soluciones de las ecuaciones $i_1 + \cdots + i_m = t$ tales que $0 \leq i_1, ..., i_m \leq q-1$, para todo t variando en el conjunto $\{0, 1, ..., r\}$. Para ello, basta traducir el cálculo del número de monomios reducidos de grado t que se encuentran en $\mathbb{F}_q[x_1, ..., x_m]$ a términos combinatorios. En efecto, fijado $t \in \{0, 1, ..., r\}$, es fácil observar que el número de monomios reducidos de $\mathbb{F}_q[x_1, ..., x_m]$ de grado exactamente t coincide con el número de m-tuplas $(i_1, ..., i_m)$ tales que $0 \leq i_j \leq q-1$ ($j \in \{1, ..., m\}$), siendo $i_1 + \cdots + i_m = t$. Pero este se corresponde con el número de soluciones de la ecuación $i_1 + \cdots + i_m = t$, donde $0 \leq i_1, ..., i_m \leq$ $\leq q-1$. Así, por el **Principio Aditivo**, se obtiene el resultado. □

2.3. Carácter Cíclico de los Códigos de Reed-Muller p-arios

Para terminar este estudio general de los códigos de Reed-Muller, veamos que estos pueden ser vistos como *códigos cíclicos extendidos* cuando $q = p$, con p primo. Esencialmente, un código extendido es un código que se obtiene añadiendo a cada palabra del código original una letra de control de paridad en la última posición. Por tanto, lo que venimos a decir es que los códigos de Reed-Muller p-arios pueden ser vistos, para una ordenación conveniente de los elementos de $\mathbb{F}_p^m$ (la cual denominaremos *ordenación cíclica*), como códigos extendidos de un cierto código cíclico. El objetivo principal es probar que todo código de Reed-Muller p-ario es equivalente a un código cíclico extendido. Esto permite obtener algunas propiedades generales de los códigos de Reed-Muller p-arios. Sin embargo, para no extendernos con el trabajo, no vamos a incluir ninguna de estas propiedades. El lector interesado puede consultar [13] o [2, Section 4.10].

En primer lugar, es conveniente aclarar que son los códigos extendidos. A su vez, también necesitamos hablar de los códigos pinchados.

Definición 2.3.1. Sea $\mathcal{C}$ un código lineal q-ario de longitud n y dimensión s, con distancia mínima d. El *código extendido* de $\mathcal{C}$, el cual suele denotarse por $\overline{\mathcal{C}}$, es el código definido por:

$$\overline{\mathcal{C}} = \{c_1 \ldots c_n c_{n+1} \mid c_1 \ldots c_n \in \mathcal{C} \ \wedge \ c_1 + \cdots + c_n + c_{n+1} = 0\} \qquad (2.6)$$

Esto es, añadimos a cada palabra de $\mathcal{C}$ una componente de control de paridad en la última posición.

Observación 2.3.1. Se comprueba inmediatamente a partir de la **Definición 2.3.1** que $\overline{\mathcal{C}}$ es también un código lineal, pero de longitud $n+1$, dimensión s y distancia mínima d ó $d+1$.

Definición 2.3.2. Sea $\mathcal{C}$ un código lineal q-ario de longitud n y dimensión s, con distancia mínima d. Fijada una posición coordenada $j \in \{1, ..., n\}$, se define el *código pinchado* de $\mathcal{C}$ *para la coordenada* j*-ésima*, que denotaremos por $\mathcal{C}_j^*$, al código que se obtiene borrando la coordenada j-ésima de todas las palabras de $\mathcal{C}$.

Observación 2.3.2. Se comprueba inmediatamente a partir de la **Definición 2.3.2** que, para toda posición $j \in \{1, ..., n\}$ fijada, $\mathcal{C}_j^*$ es también un código lineal, pero de longitud $n-1$, dimensión s ó $s-1$ y distancia mínima menor o igual que d.

Nota 2.3.1. Las **Definiciones 2.3.1 y 2.3.2** que acabamos de dar pueden considerarse "duales". En efecto, dado un código lineal $\mathcal{C}$, si lo extendemos y luego pinchamos por la coordenada $n+1$, obtenemos el código inicial.

Para estudiar el carácter cíclico de $\mathcal{RM}_p(r, m)$, es necesario tener en mente algunos conceptos de la asignatura *Ecuaciones Algebraicas* que recordaremos a continuación. Consideremos un *elemento primitivo* α de $\mathbb{F}_{p^m}$, es decir, un generador del grupo cíclico $(\mathbb{F}_{p^m}^*, \cdot)$ para el que se cumple además que $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$. Ahora, suponiendo que $\mathrm{Irr}(\alpha, \mathbb{F}_p) = a_0 + \cdots + a_{m-1}x^{m-1} + x^m$, sea $A(\alpha, p)$ la *matriz compañera de* α, que viene dada por:

$$A(\alpha, p) \underset{not.}{\equiv} \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}.$$

Es bien sabido que el grupo cíclico generado por esta matriz $A(\alpha, p)$ tiene orden $n-1$ ($n = p^m$) por el **Teorema de Cayley-Hamilton**, y por tanto podemos identificar este grupo con $\mathbb{F}_{p^m}^*$.

Bajo estas condiciones, es posible construir una ordenación de los elementos de $\mathbb{F}_p^m$ asociada a la matriz $A(\alpha, p)$. En efecto, fijado un elemento $\mathbf{w}_1 \in \mathbb{F}_p^m$ no nulo, definimos recursivamente los vectores $\mathbf{w}_2, \mathbf{w}_3, ..., \mathbf{w}_{n-1}$ a través de $\mathbf{w}_1$ siguiendo la regla

$$\mathbf{w}_i = \mathbf{w}_{i-1}A(\alpha, p) = \mathbf{w}_1 A(\alpha, p)^{i-1}, \qquad \forall i \in \{2, 3, ..., n-1\}. \tag{2.7}$$

Los elementos que acabamos de definir mediante la regla (2.7) verifican la propiedad siguiente:

Proposición 2.3.1. *Bajo las notaciones que se acaban de fijar,* $\mathbf{w}_i = \mathbf{w}_j$ *si, y sólo si, se cumple que* $i \equiv j(mod\ n-1)$.

Demostración. Empezamos probando la condición suficiente, suponiendo que $i \equiv j(\text{mod } n-1)$. Como $A(\alpha, p)$ genera un grupo cíclico de orden $n-1$, es evidente que bajo nuestra hipótesis se cumple que $A(\alpha,p)^{i-1} = A(\alpha,p)^{j-1}$. En consecuencia, se tiene que $\mathbf{w}_i = \mathbf{w}_1 A(\alpha,p)^{i-1} = \mathbf{w}_1 A(\alpha,p)^{j-1} = \mathbf{w}_j$. Recíprocamente, para la condición necesaria, basta probar que si $\mathbf{w}_i = = \mathbf{w}_j$ para índices $i, j \in \{1, ..., n-1\}$, entonces $i = j$. Vamos a argumentar por reducción al absurdo, suponiendo que $i \neq j$. Por hipótesis, se tiene que $\mathbf{w}_1(A(\alpha,p)^{i-1} - A(\alpha,p)^{j-1}) = 0$. Ahora bien, como hay una identificación entre el subgrupo generado por $A(\alpha, p)$, que suele denotarse por $< A(\alpha,p) >$, y $\mathbb{F}^*_{p^m}$, sabemos que existe $h \in \{1, ..., n-1\}$ tal que $\mathbf{w}_1(A(\alpha,p)^{i-1} - A(\alpha,p)^{j-1}) = \mathbf{w}_1 A(\alpha,p)^h = 0$, luego $\mathbf{w}_1 \in \text{Ker}(A(\alpha,p)^h)$. Además, es evidente que $\det(A(\alpha,p)^h) \neq 0$, dado que $A(\alpha,p)$ es cuadrada y $\det(A(\alpha,p)) = -a_0 \neq 0$ (esto se debe a la definición de polinomio irreducible de α sobre $\mathbb{F}_p$). En resumen, se tiene que $\text{Ker}(A(\alpha,p)^h) = \{\mathbf{0}\}$, en contradicción con la elección hecha de $\mathbf{w}_1$. □

Como consecuencia inmediata de la **Proposición 2.3.1** que se acaba de ver, se tiene que $\mathbb{F}_p^m - \{\mathbf{0}\} = \{\mathbf{w}_1, ...\mathbf{w}_{n-1}\}$, siendo $n = p^m$.

En resumen, dados α elemento primitivo de $\mathbb{F}_{p^m}$ y $\mathbf{w}_1 \in \mathbb{F}_p^m - \{\mathbf{0}\}$ (como por ejemplo $\mathbf{w}_1 = (1, 0, ..., 0)$), definimos un orden sobre $\mathbb{F}_p^m$ a través de la regla vista en (2.7) dado por $\mathbb{F}_p^m = \{\mathbf{0}, \mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_{n-1}\}$. Llamaremos a este *orden cíclico* de $\mathbb{F}_p^m$ con base $\mathbf{w}_1$ respecto de α.

Consideramos ahora el código pinchado obtenido borrando la primera coordenada de todas las palabras de $\mathcal{RM}_p(r,m)$ para cualquier orden cíclico $\mathbb{F}_p^m = \{\mathbf{0}, \mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_{n-1}\}$. Obtenemos el código lineal siguiente:

$$\mathcal{C}_p(r,m) \underset{not.}{\equiv} \mathcal{RM}_p(r,m)^*_1 = \{F(\mathbf{w}_1)\dots F(\mathbf{w}_{n-1}) \mid F \in \mathcal{P}^p_m(r)\}.$$

Es sencillo probar que este es un código cíclico. Para ello, es conveniente tener en cuenta las notaciones introducidas al comienzo de la Sección 1.3.

Teorema 2.3.2. *Para cualesquiera enteros* r *y* m *tales que* $0 \leq r \leq m$, *se tiene que* $\mathcal{C}_p(r,m)$ *es un código cíclico.*

Demostración. Para ver que $\mathcal{C}_p(r,m)$ es un código cíclico, veamos que se cumple la condición (1.3) de la **Definición 1.3.1** de código cíclico. Sea $\mathbf{x} = F(\mathbf{w}_1)\dots F(\mathbf{w}_{n-1}) \in \mathcal{C}_p(r,m)$ una palabra código ($F \in \mathcal{P}^p_m(r)$). Sea el polinomio $G(x_1, ..., x_n) = F((x_1...x_n)A(\alpha,p))$. Es evidente que $\deg(F) = = \deg(G)$, luego $G \in \mathcal{P}^p_m(r)$ y

$$G(\mathbf{w}_1)\dots G(\mathbf{w}_{n-1}) = F(\mathbf{w}_1 A(\alpha,p))\dots F(\mathbf{w}_{n-2}A(\alpha,p))F(\mathbf{w}_{n-1}A(\alpha,p)) =$$

$$= F(\mathbf{w}_2)\dots F(\mathbf{w}_{n-1})F(\mathbf{w}_1) = \mathbf{x}^{(n-1)} \in \mathcal{C}_p(r,m).$$

Reiterando este procedimiento, tras un número finito de pasos n, obtenemos que $\mathbf{x}^{(1)} \in \mathcal{C}_p(r,m)$. □

Corolario 2.3.3. *Todo código obtenido pinchando un código de Reed-Muller p-ario en las letras correspondientes a la evaluación en el vector* $\mathbf{0}$ *es equivalente a un código cíclico.*

Demostración. Este resultado es consecuencia inmediata del **Teorema 2.3.2** que acabamos de demostrar, ya que un código de Reed-Muller p-ario es, en virtud de las **Observaciones 2.2.2**, equivalente al código de Reed-Muller p-ario con los mismos parámetros construido a partir del orden cíclico de $\mathbb{F}_p^m$ antes determinado. □

Finalmente, veamos que todo código de Reed-Muller puede verse, para cualquier ordenación cíclica de $\mathbb{F}_p^m$, como un código cíclico extendido. Es necesario dar antes el siguiente resultado, que es cierto en cualquier cuerpo finito $\mathbb{F}_q$ y que probaremos en general (pues, aunque ahora nos basta con verlo para $q = p$, necesitaremos el resultado general en el **Problema 2.2**)

Lema 2.3.4. *Sea* $F \in \mathbb{F}_q[x_1,...,x_m]$. *Si* $deg(F^*) < m(q-1)$. *Entonces,*

$$\sum_{\mathbf{v}\in\mathbb{F}_q^m} F(\mathbf{v}) = 0. \tag{2.8}$$

Demostración. Dado $\mathbf{v} = (\alpha_1,...,\alpha_m) \in \mathbb{F}_q^m$, sea $F_\mathbf{v}$ el polinomio que introdujimos en la demostración de la **Proposición 2.2.1** dado por:

$$F_\mathbf{v} = \prod_{i=1}^{m}(1-(x_i-\alpha_i)^{q-1}).$$

Recordemos que para este polinomio se verifica, dado $\mathbf{w} \in \mathbb{F}_q^m$, que:

$$F_\mathbf{v}(\mathbf{w}) = \begin{cases} 1, & \text{si } \mathbf{w} = \mathbf{v}; \\ 0, & \text{si } \mathbf{w} \neq \mathbf{v}. \end{cases}$$

Es inmediato observar que este polinomio está dado en su forma reducida (pues la mayor potencia en el exponente de cada indeterminada es $q-1$), y además

$$F^* = \sum_{\mathbf{v}\in\mathbb{F}_q^m} F(\mathbf{v})\ F_\mathbf{v},$$

donde, como por el **Teorema del Binomio de Newton** es $(x_i-\alpha_i)^{q-1} = = x_i^{q-1} + \alpha_i x_i^{q-2} + \dots + \alpha_i^{q-1}$, podemos escribir $F_\mathbf{v} = (-1)^m x_1^{q-1}\cdots x_m^{q-1} + +$ términos de menor grado. En consecuencia

$$F^* = \sum_{\mathbf{v}\in\mathbb{F}_q^m} [F(\mathbf{v})(-1)^m x_1^{q-1}\cdots x_m^{q-1} + \text{términos de menor grado}] =$$

$$= [(-1)^m \sum_{\mathbf{v}\in\mathbb{F}_q^m} F(\mathbf{v})] x_1^{q-1} \cdots x_m^{q-1} + \text{ términos de menor grado,}$$

de donde, como $\deg(F^*) < m(q-1)$, se sigue necesariamente (2.8). □

Corolario 2.3.5. *Todo código de Reed-Muller p-ario es equivalente a un código cíclico extendido.*

Demostración. Este resultado es consecuencia inmediata de que todo código de Reed-Muller p-ario construido a partir de la ordenación cíclica de $\mathbb{F}_p^m$ es un código cíclico extendido y del **Corolario 2.3.3**. En efecto, por la **Definición 2.3.1** de código extendido y el **Lema 2.3.4**, a partir de (2.6), se obtiene que, para la ordenación cíclica de $\mathbb{F}_p^m$, $\mathcal{RM}_p(r,m)$ es el código extendido de $\mathcal{C}_p(r,m)$, el cual es un código cíclico por el **Teorema 2.3.2**. □

2.4. Problemas Resueltos

Problema 2.1. Demostrar que el conjunto $\mathfrak{B}_m^q$ es una $\mathbb{F}_q$-álgebra con las operaciones definidas en las **Observaciones 2.2.1**.

Solución. Se trata de probar que el conjunto $\mathfrak{B}_m^q$ es un anillo conmutativo y unitario con estructura de $\mathbb{F}_q$-espacio vectorial para las operaciones definidas en las **Observaciones 2.2.1**, y que además se verifica la propiedad

$$\alpha \cdot_{\mathbb{F}_q} (f \cdot g) = (\alpha \cdot_{\mathbb{F}_q} f) \cdot g = f \cdot (\alpha \cdot_{\mathbb{F}_q} g),$$

para cualesquiera $\alpha \in \mathbb{F}_q$ y $f, g \in \mathfrak{B}_m^q$ arbitrarios. Sólo nos queda comprobar esto último, lo cual es inmediato por como se han definido los productos interno y externo, ya que

$$\alpha \cdot_{\mathbb{F}_q} (f \cdot g) = (\alpha \cdot_{\mathbb{F}_q} f) \cdot g$$

y

$$\alpha \cdot_{\mathbb{F}_q} (f \cdot g) \underset{conmut.}{=} \alpha \cdot_{\mathbb{F}_q} (g \cdot f) = (\alpha \cdot_{\mathbb{F}_q} g) \cdot f \underset{conmut.}{=} f \cdot (\alpha \cdot_{\mathbb{F}_q} g),$$

puesto que por la propiedad asociativa de $\mathbb{F}_q$ se tiene que

$$\alpha(f(u)g(u)) = (\alpha f(u))g(u) \qquad \text{y} \qquad \alpha(g(u)f(u)) = (\alpha g(u))f(u),$$

para cualquier $u \in \mathbb{F}_q^m$. □

Problema 2.2.

(i) Probar que $\mathcal{RM}_q(r,m)^\perp = \mathcal{RM}_q(m(q-1)-r-1, m)$.

(ii) Deducir de (i) que forma tienen los códigos de Reed-Muller autoduales.

Solución.

(i) Veamos primero que $\mathcal{RM}_q(m(q-1)-r-1,m) \subseteq \mathcal{RM}_q(r,m)^{\perp}$. Sean F y G polinomios reducidos de $\mathbb{F}_q[x_1,...,x_m]$ de grados a lo más r y $m(q-1)-r-1$, respectivamente. Recuperamos la aplicación (2.1). Es evidente por definición que $ev_{\mathbb{F}_q^m}(F) = \mathbf{F} \in \mathcal{RM}_q(r,m)$ y $ev_{\mathbb{F}_q^m}(G) = = \mathbf{G} \in \mathcal{RM}_q(m(q-1)-r-1,m)$. Entonces, como por linealidad $ev_{\mathbb{F}_q^m}(FG) = ev_{\mathbb{F}_q^m}(F)ev_{\mathbb{F}_q^m}(G)$, en virtud del **Lema 2.3.4** (pues $\deg((FG)^*) = \deg(FG) = \deg(F)+\deg(G) \leq (r)+(m(q-1)-r-1) = = m(q-1)-1 < m(q-1)$) se sigue que

$$< \mathbf{F}, \mathbf{G} >= \sum_{\mathbf{v}\in\mathbb{F}_q^m} (FG)(\mathbf{v}) = 0.$$

Este hecho implica la inclusión deseada por la definición de código dual.

Para obtener la igualdad, por como están relacionadas las dimensiones de un código lineal y su dual, basta ver que las dimensiones de $\mathcal{RM}_q(r,m)$ y $\mathcal{RM}_q(m(q-1)-r-1,m)$ suman q^m. En efecto, por el **Corolario 2.2.5**, la dimensión de $\mathcal{RM}_q(m(q-1)-r-1,m)$ coincide con el número de soluciones de las ecuaciones $i_1+\cdots+i_m = t$, para t variando en $\{0,1,...,m(q-1)-r-1\}$, donde $0 \leq i_1,...,i_m \leq q-1$. Haciendo ahora el cambio de variable $l = m(q-1)-t$, se trata de hallar el número de soluciones de las ecuaciones $j_1+\cdots+j_m = l$, para l variando en $\{r+1,...,m(q-1)\}$, donde $0 \leq j_1,...,j_m \leq q-1$. En consecuencia, por el **Corolario 2.2.5** aplicado a $\mathcal{RM}_q(r,m)$, el valor de $\dim(\mathcal{RM}_q(r,m)) + \dim(\mathcal{RM}_q(m(q-1)-r-1,m))$ va a coincidir con el número de soluciones de $i_1+\cdots+i_m = t$, para t variando en $\{0,1,...,r,r+1,...,m(q-1)\}$, donde $0 \leq i_1,...,i_m \leq q-1$. Pero este se corresponde en términos combinatorios con el número de variaciones con repetición de m elementos tomados de q en q, que es q^m.

(ii) Como consecuencia de (i) podemos ver que forma tienen los códigos de Reed-Muller autoduales. En efecto, basta hallar los valores naturales de $r \leq m(q-1)$ para los que se verifica la igualdad $2r = m(q-1)-1$. Para que exista solución entera de r, es necesario que $m(q-1)$ sea impar. Para ello, m tiene que ser impar y q par (esto es, potencia de 2). Supongamos que $m = 2n+1$, con $n \in \mathbb{N}$. Entonces

$$2r = m(q-1)-1 = (2n+1)(q-1)-1 = 2(n(q-1)+\frac{q}{2}-1)$$

$$\Updownarrow$$

$$r = n(q-1)+\frac{q}{2}-1 = \frac{1}{2}(m(q-1)-1) \leq m(q-1)$$

En resumen, los códigos de Reed-Muller autoduales son aquellos tales que q es una potencia par, siendo m impar y $r = \frac{1}{2}(m(q-1)-1)$.

□

Capítulo 3

Códigos de Reed-Muller Binarios

El objetivo de este capítulo es centrar el estudio realizado en el Capítulo 2 al caso binario. Precisamente, es en la Sección 3.1 donde se realiza la particularización de la construcción general vista en del capítulo anterior. Recordemos que esta fue la construcción original que presentó Muller. A continuación, damos otra construcción válida sólo en el caso binario, que está basada en la construcción de Plotkin vista en el **Problema 1.3**. Finalmente, cerraremos el capítulo con una interpretación geométrica de los códigos de Reed-Muller binarios a través de geometrías finitas.

3.1. Construcción Mediante Funciones Booleanas

Como ya hemos adelantado, esta no es más que una particularización de la construcción general ya estudiada. Sin embargo, conviene hacer hincapié en ciertos aspectos para obtener varios resultados importantes del caso binario. Esta sección está basada en [3, Lección 7] y [11, Section 6.2].

Manteniendo las notaciones establecidas en el Capítulo 2 y usando los **Ejemplos 2.2.1 y 2.2.2**, como consecuencia inmediata del **Teorema 2.2.3** para $q = 2$, obtenemos el siguiente resultado:

Teorema 3.1.1. *Fijado un orden en los elementos de $\mathbb{F}_2^m$, se tiene que el conjunto de los polinomios Booleanos $\mathcal{P}_m$ es isomorfo, como $\mathbb{F}_2$-álgebra, a $\mathbb{F}_2^{2^m}$ a través de la aplicación*

$$\begin{array}{rccl} \psi_m \underset{not.}{\equiv} \overline{ev_{\mathbb{F}_2^m}}: & \mathcal{P}_m & \longrightarrow & \mathbb{F}_2^{2^m} \\ & F & \longmapsto & \overline{ev_{\mathbb{F}_2^m}}(F) = \mathbf{F} = F_1 \dots F_{2^m}. \end{array} \tag{3.1}$$

En consecuencia, bajo estas condiciones, cada polinomio Booleano tiene asociada una, y sólo una, palabra binaria $\mathbf{x} \in \mathbb{F}_2^{2^m}$.

Fijado un orden en $\mathbb{F}_2^m$, podemos dar la siguiente definición, que es equivalente, para el caso de binario, a la **Definición 2.2.4**.

Definición 3.1.1. Sean m y r dos números naturales, donde $0 \leq r \leq m$. Se define por *código de Reed-Muller binario* de longitud 2^m y orden r, lo cual denotaremos por simplicidad como $\mathcal{RM}(r,m)$, al conjunto de todas las palabras binarias de longitud 2^m asociadas a todos los polinomios Booleanos de m indeterminadas y grado menor o igual que r.

Finalmente, se pueden resumir las principales propiedades de los códigos de Reed-Muller binarios ya vistas en el siguiente resultado:

Proposición 3.1.2. *El código de Reed-Muller binario $\mathcal{RM}(r,m)$ es un código lineal de longitud 2^m sobre $\mathbb{F}_2$, y su dimensión como $\mathbb{F}_2$-subespacio vectorial viene dada por la fórmula siguiente:*

$$\dim(\mathcal{RM}(r,m)) = \sum_{k=0}^{r} \binom{m}{k}. \tag{3.2}$$

Además, la matriz

$$G(r,m) = \begin{pmatrix} \psi_m(1) \\ \psi_m(x_1) \\ \vdots \\ \psi_m(x_m) \\ \psi_m(x_1x_2) \\ \vdots \\ \psi_m(x_{m-r+1}\dots x_m) \end{pmatrix}, \tag{3.3}$$

*donde ψ_m es la aplicación (3.1) definida en el **Teorema 3.1.1**, es una matriz generadora de $\mathcal{RM}(r,m)$.*

Demostración. Para empezar, que $\mathcal{RM}(r,m)$ es un código lineal se deduce de las **Observaciones 2.2.2**. Ahora, para obtener la fórmula de la dimensión, por el **Corolario 2.2.5**, debemos hallar el número de soluciones de las ecuaciones $i_1 + \cdots + i_m = t$, con t variando en $\{0,1,...,r\}$, tales que $0 \leq i_1,...,i_m \leq 1$. Sin embargo, fijado t, este valor coincide con el número de subconjuntos de t elementos distintos elegidos de un conjunto de cardinal m sin importar el orden. Pero esta es la definición de las combinaciones de m elementos tomadas de t en t. El resultado a partir de aquí vuelve a ser inmediato por el **Principio Aditivo**. Finalmente, la expresión de $G(r,m)$ se obtiene por lo visto en la **Proposición 2.2.4**. □

La importancia que tiene el uso de códigos de Reed-Muller binarios radica en la cantidad de propiedades que verifican. Un ejemplo es la que se probará en el **Problema 3.2**. Para ello, debemos tener en cuenta que todo código lineal binario que admita una matriz generadora en la que todas sus filas tengan peso par verifica que toda palabra código también tiene peso par.

3.2. Construcción Recursiva de Plotkin

Tal y como ya se adelantó al comienzo del capítulo, nos basaremos ahora en la construcción de Plotkin dada en el **Problema 1.3** para obtener una construcción recursiva de los códigos de Reed-Muller binarios. Esta sólo es válida para cuando se tiene fijado un cierto orden para los elementos de $\mathbb{F}_2^m$. En efecto, dada la expansión binaria $i_0 + 2i_1 + 2^2 i_2 + \cdots + 2^{m-2} i_{m-2} + +2^{m-1} i_{m-1}$, con $i_0, i_1, ..., i_{m-2}, i_{m-1} \in \{0, 1\}$, de un cierto entero i, asociamos a $i+1$ el elemento $(i_0, i_1, i_2, ..., i_{m-2}, i_{m-1}) \in \mathbb{F}_2^m$, esto es:

$$\begin{array}{ccc} 1 & \longrightarrow & (0,0,0,...,0,0), \\ 2 & \longrightarrow & (1,0,0,...,0,0), \\ 3 & \longrightarrow & (0,1,0,...,0,0), \\ 4 & \longrightarrow & (1,1,0,...,0,0), \\ 5 & \longrightarrow & (0,0,1,...,0,0), \\ \vdots & \vdots & \vdots \\ 2^m - 2 & \longrightarrow & (1,0,1,...,1,1), \\ 2^m - 1 & \longrightarrow & (0,1,1,...,1,1), \\ 2^m & \longrightarrow & (1,1,1,...,1,1). \end{array}$$

A este le llamaremos *orden canónico* de $\mathbb{F}_2^m$. Supondremos a lo largo de toda esta sección que tenemos fijado este orden para los elementos de $\mathbb{F}_2^m$. Nuestro principal objetivo es poder obtener expresiones dependientes de r y m tanto para la distancia mínima de $\mathcal{RM}(r,m)$ como para una matriz generadora de $\mathcal{RM}(r,m)$. La gran parte de los resultados que aquí se recogen vienen en [3, Lección 7], aunque son necesarios [1, Chapter 9], [12, Sección 5.3] y [8, Sección 3.3] para completar el estudio adecuadamente.

Antes de continuar, es necesario resaltar las dos consecuencias siguientes que nos serán de mucha utilidad a lo largo de toda esta sección. Estas se deben a haber fijado el orden canónico en $\mathbb{F}_2^m$.

Lema 3.2.1. *La palabra característica asociada al polinomio Booleano x_i, como elemento de $\mathcal{P}_m$, es aquella que tiene en su k-ésima posición un* 1 *cuando la expansión binaria de k tiene un* 1 *en la i-ésima posición, para k recorriendo $\{1, ..., 2^m\}$. En términos de tablas de verdad, esto viene a decirnos que se tiene lo siguiente:*

$$\begin{array}{ccc} \psi(x_1) & = & 01010101...0101, \\ \psi(x_2) & = & 00110011...0011, \\ \vdots & \vdots & \vdots \\ \psi(x_m) & = & \underbrace{000...00}_{2^{m-1}}\underbrace{111...11}_{2^{m-1}}. \end{array}$$

Demostración. Basta construir las tablas de verdad para el orden canónico de $\mathbb{F}_2^m$ asociadas a los polinomios Booleanos x_i como elementos de $\mathcal{P}_m$.

$F(x_1, x_2, ..., x_m)$	F_1	F_2	$\cdots$	$F_{2^{m-1}-1}$	$F_{2^{m-1}}$	$\cdots$	F_{2^m-1}	F_{2^m}
x_1	0	1	$\cdots$	0	1	$\cdots$	0	1
x_2	0	0	$\cdots$	1	0	$\cdots$	1	1
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$
x_m	0	0	$\cdots$	0	1	$\cdots$	1	1

Así, por definición de la aplicación (3.1) bajo el orden canónico de $\mathbb{F}_2^m$, se sigue el resultado trivialmente. □

Lema 3.2.2. *Sea $F(x_1, ..., x_{m-1})$ un polinomio Booleano de $m-1$ indeterminadas que tiene como palabra binaria asociada a $\mathbf{x} = x_1...x_{2^{m-1}}$. Entonces, la palabra binaria asociada a F como polinomio Booleano de $\mathcal{P}_m$ es $\mathbf{x} * \mathbf{x} = x_1...x_{2^{m-1}}x_1...x_{2^{m-1}}$.*

Demostración. Construimos la tabla de verdad bajo el orden canónico de $\mathbb{F}_2^m$ asociada a nuestro polinomio Booleano de $m-1$ indeterminadas.

	F_1	$\cdots$	$F_{2^{m-1}}$
$F(x_1, ..., x_{m-1})$	x_1	$\cdots$	$x_{2^{m-1}}$

Si consideramos F como un polinomio de $\mathcal{P}_m$, dado que este no depende de la última indeterminada x_m, la correspondiente tabla de verdad vendrá determinada por los valores de la anterior.

	F_1	$\cdots$	$F_{2^{m-1}}$	$F_{2^{m-1}+1}$	$\cdots$	F_{2^m}
$F(x_1, ..., x_m)$	x_1	$\cdots$	$x_{2^{m-1}}$	x_1	$\cdots$	$x_{2^{m-1}}$

De esta manera, se tiene que $\mathbf{x} * \mathbf{x}$ es la palabra binaria asociada a F como polinomio Booleano de $\mathcal{P}_m$. □

Estos resultados nos permiten definir los códigos de Reed-Muller binarios como construcción de Plotkin para el orden canónico de $\mathbb{F}_2^m$. Para ello, es fundamental el teorema siguiente:

Teorema 3.2.3. *Dados dos números naturales r y m tales que $0 < r < m$, se cumple que*

$$\mathcal{RM}(r, m) = \mathcal{RM}(r, m-1) \circledast \mathcal{RM}(r-1, m-1).$$

Es decir, el código de Reed-Muller $\mathcal{RM}(r, m)$ es la construcción de Plotkin de los códigos de Reed-Muller $\mathcal{RM}(r, m-1)$ y $\mathcal{RM}(r-1, m-1)$.

Demostración. Veamos primero que $\mathcal{RM}(r,m) \subseteq \mathcal{RM}(r,m-1) \circledast \mathcal{RM}(r-1,m-1)$. Sea $\mathbf{x} \in \mathcal{RM}(r,m)$ una palabra código arbitraria, que está asociada al polinomio Booleano F de m indeterminadas de grado menor o igual que r. Es evidente que podemos expresar F en función de dos polinomios Booleanos de $m-1$ indeterminadas G y H como sigue:

$$F(x_1,...,x_m) = x_m G(x_1,...,x_{m-1}) + H(x_1,...,x_{m-1}), \tag{3.4}$$

donde G tiene grado menor o igual que $r-1$ y H grado menor o igual que r. Supongamos que $\mathbf{x}_G$ y $\mathbf{x}_H$ son las palabras binarias asociadas a estos polinomios G y H, respectivamente, como polinomios Booleanos de $m-1$ indeterminadas. Es evidente por definición que $\mathbf{x}_G \in \mathcal{RM}(r-1,m-1)$ y $\mathbf{x}_H \in \mathcal{RM}(r,m-1)$. Ahora, por el **Lema 3.2.2**, se tiene que $\mathbf{x}_G * \mathbf{x}_G$ y $\mathbf{x}_H * \mathbf{x}_H$ son las palabras binarias asociadas a los polinomios G y H, respectivamente, como polinomios Booleanos de m indeterminadas. Aplicando entonces la aplicación ψ_m dada en (3.1) a (3.4) (recordemos que ya se ha visto en el **Lema 3.2.1** que la palabra binaria asociada al polinomio Booleano $x_m \in \mathcal{P}_m$ era 000...0111...1), se tiene por linealidad que

$$\mathbf{x} = (000...0111...1)(\mathbf{x}_G * \mathbf{x}_G) + \mathbf{x}_H * \mathbf{x}_H = \mathbf{x}_H * \mathbf{x}_H + 000...0 * \mathbf{x}_G =$$

$$= (\mathbf{x}_H | \mathbf{x}_H + \mathbf{x}_G).$$

En consecuencia, $\mathbf{x} \in \mathcal{RM}(r,m-1) \circledast \mathcal{RM}(r-1,m-1)$.

Para obtener la igualdad basta ver que ambos códigos tienen la misma dimensión. En efecto, por (3.2) y la **Fórmula de Pascal**, podemos deducir de como viene dada la dimensión en la construcción de Plotkin de dos códigos lineales (véase el **Problema 1.3**) que

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

$$+ \sum_{k=1}^{r} \binom{m-1}{k} + \sum_{k=1}^{r} \binom{m-1}{k-1} = \sum_{k=0}^{r} \binom{m-1}{k} + \sum_{k=0}^{r-1} \binom{m-1}{k} =$$

$$= \dim(\mathcal{RM}(r,m-1)) + \dim(\mathcal{RM}(r-1,m-1)) =$$

$$= \dim(\mathcal{RM}(r,m-1) \circledast \mathcal{RM}(r-1,m-1))$$

por las propiedades de los coeficientes binomiales y haciendo el correspondiente cambio de variable. Se obtiene así la igualdad deseada. □

Hecho esto, podemos dar la siguiente definición recursiva de los códigos de Reed-Muller binarios para cuando se tenga fijado el orden canónico de $\mathbb{F}_2^m$. Es inmediato observar que esta es consistente con la **Definición 3.1.1**, en virtud del **Teorema 3.2.3** y el **Ejemplo 2.2.3**:

Definición 3.2.1. Dados r y m dos números naturales tales que $0 < r < m$, se define de manera recursiva el código de Reed-Muller binario de longitud 2^m y orden r ($\mathcal{RM}(r,m)$) a través de las reglas siguientes:

1) $\mathcal{RM}(0,n) = \{\underbrace{0\ldots0}_{2^n}, \underbrace{1\ldots1}_{2^n}\}, \qquad \forall n \in \{1,\ldots,m\}.$

2) $\mathcal{RM}(n,n) = \mathbb{F}_2^{2^n}, \qquad \forall n \in \{1,\ldots,m\}.$

3)
$$\mathcal{RM}(s,n) = \mathcal{RM}(s,n-1) \circledast \mathcal{RM}(s-1,n-1),$$
$$\forall s \in \{1,...,r\} \qquad \text{y} \qquad \forall n \in \{s,...,m\}.$$

Ejemplo 3.2.1. Dado m natural, se cumple para el orden canónico que

$$G(0,m) = \underbrace{(1\ 1\ \cdots\ 1)}_{2^m} \qquad \text{y} \qquad G(m,m) = \begin{pmatrix} G(m-1,m) \\ \underbrace{0\ \cdots\ 0}_{2^m-1}\ 1 \end{pmatrix}.$$

En efecto, ambas igualdades son consecuencia de (3.3). La primera se debe a que la aplicación ψ_m de (3.1) verifica que $\psi_m(1) = 1\ldots11$. La segunda es consecuencia de que ψ_m es, en particular, un homomorfismo de anillos, pues por el **Lema 3.2.1** tenemos que $\psi_m(x_1\cdots x_m) = \psi_m(x_1)\cdots\psi_m(x_m) = = 0\ldots01$ y el resto de polinomios que quedan tienen por palabras características a las pertenecientes a $\mathcal{RM}(m-1,m)$, cuya matriz generadora es $G(m-1,m)$.

Esta construcción nos permite dar los dos siguientes resultados.

Proposición 3.2.4. *Dados r y m naturales tales que $0 \leq r \leq m$, se tiene que la distancia mínima de $\mathcal{RM}(r,m)$ es 2^{m-r}.*

Demostración. Vamos a hacer uso de la **Definición 3.2.1**. Para ello, hay que tener en cuenta que, pese a que se tenga fijado el orden canónico de $\mathbb{F}_2^m$, podemos calcular la distancia mínima de nuestro código de Reed-Muller a partir de la construcción de Plotkin, puesto que cambiar el orden en $\mathbb{F}_2^m$ sólo hace que se obtenga un código equivalente, que sigue siendo un código de Reed-Muller con los mismos parámetros.

Argumentamos por inducción sobre m. Para $m = 1$ se tienen dos posibles códigos de Reed-Muller binarios. Como $\mathcal{RM}(0,1) = \{00,11\}$ y $\mathcal{RM}(1,1) = = \{00,11,01,10\}$, es evidente que $d(\mathcal{RM}(0,1)) = 2 = 2^{1-0}$ y $d(\mathcal{RM}(1,1)) = = 1 = 2^{1-1}$. Supongamos cierto el resultado para $m-1$ y probémoslo para m. Por hipótesis de inducción y lo visto en el **Problema 1.3**, se tiene que

$$d(\mathcal{RM}(r,m)) = \min\{2d(\mathcal{RM}(r,m-1)), d(\mathcal{RM}(r-1,m-1))\} =$$
$$= \min\{22^{m-r-1}, 2^{m-r}\} = 2^{m-r}.$$

□

Proposición 3.2.5. *Dados r y m naturales tales que $0 \leq r \leq m$, sólo para el orden canónico de $\mathbb{F}_2^m$, la matriz generadora de $\mathcal{RM}(r,m)$ viene dada por bloques de manera recursiva en función de las matrices generadoras de $\mathcal{RM}(r,m-1)$ y $\mathcal{RM}(r-1,m-1)$ como sigue:*

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

siendo

$$G(0,m) = \underbrace{(1\ 1\ \cdots\ 1)}_{2^m} \qquad y \qquad G(m,m) = \begin{pmatrix} G(m-1,m) \\ \underbrace{0\ \cdots\ 0}_{2^m-1}\ 1 \end{pmatrix}.$$

Demostración. Argumentamos por inducción sobre m. Si $m = 1$, en virtud del **Ejemplo 3.2.1**, tenemos que

$$G(0,1) = (1\ 1) \qquad \text{y} \qquad G(1,1) = \begin{pmatrix} G(0,1) \\ 0\ 1 \end{pmatrix} = \begin{pmatrix} 1\ 1 \\ 0\ 1 \end{pmatrix}.$$

Supongamos ahora cierto el resultado para $m-1$. Entonces, por el **Problema 1.3**, dado que estamos bajo el orden canónico de $\mathbb{F}_2^m$, aplicando la hipótesis de inducción se concluye inmediatamente el resultado para m. □

Ejemplo 3.2.2. Usando la **Proposición 3.2.5**, vamos a construir $G(1,3)$, esto es, una matriz generadora de $\mathcal{RM}(1,3)$ para el orden canónico de $\mathbb{F}_2^m$.

$$G(1,3) = \begin{pmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{pmatrix} = \begin{pmatrix} G(1,1) & G(1,1) & G(1,1) & G(1,1) \\ 0\ 0 & G(0,1) & 0\ 0 & G(0,1) \\ 0\ 0\ 0\ 0 & & 1\ 1\ 1\ 1 & \end{pmatrix} =$$

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

Nota 3.2.1. Una matriz de control de $\mathcal{RM}(r,m)$ también puede obtenerse aplicando la **Proposición 3.2.5** al correspondiente código de Reed-Muller dual (véase el **Problema 2.2**).

3.3. Construcción Geométrica

Para terminar, vamos a obtener información adicional acerca de los códigos de Reed-Muller binarios desde un punto de vista geométrico. Para ello, trabajaremos con el $\mathbb{F}_2$-espacio vectorial $\mathbb{F}_2^m$ de todos los vectores binarios de longitud m como geometría finita, que se denota por $EG(m,2)$ en términos geométricos y cuyos elementos llamaremos puntos en estas circunstancias. El objetivo es dar una caracterización geométrica de $\mathcal{RM}(r,m)$. En la redacción de esta sección usamos principalmente [11, Section 6.2]. Sin embargo, completaremos los resultados con [1, Chapter 9] y [6, Capítulo 12].

3.3.1. Geometría Finita $EG(m, 2)$

En primer lugar, es necesario hacer un breve estudio acerca de la geometría finita $EG(m, 2) = \{\mathbf{v}_1, ..., \mathbf{v}_{2^m}\}$. En concreto, vamos a introducir un tipo especial de subconjuntos de $EG(m, 2)$, que son las llamadas *variedades afines*.

Definición 3.3.1. Dados un subespacio vectorial V de $\mathbb{F}_2^m$ y un punto $\mathbf{a} \in EG(m, 2)$, se conoce por *variedad que pasa por* $\mathbf{a}$ *y tiene dirección* V a la clase de equivalencia

$$\mathbf{a} + V = \{\mathbf{a} + \mathbf{v} \mid \mathbf{v} \in V\}.$$

Llamaremos *dimensión* de la variedad $\mathbf{a} + V$ a la dimensión del subespacio vectorial V. Así, si esta es k, diremos que $\mathbf{a} + V$ es una *k-variedad*.

Veamos unos cuantos ejemplos.

Ejemplos 3.3.1. Sea $\mathbf{a} + V$ una variedad afín de $EG(m, 2)$.

(i) Si $V = \{\mathbf{0}\}$, tenemos que $\mathbf{a} + V = \{\mathbf{a}\}$. Las 0-variedades son por tanto los puntos de $EG(m, 2)$. El recíproco también es trivialmente cierto. En consecuencia, hay 2^m 0-variedades diferentes.

(ii) Si V tiene dimensión 1 (por lo que V es una recta vectorial), sabemos que existe $\mathbf{v} \in V$ no nulo tal que $V = \{\lambda\mathbf{v} \mid \lambda \in \mathbb{F}_2\} = \{\mathbf{0}, \mathbf{v}\}$. En este caso, a $\mathbf{a} + V = \{\mathbf{a}, \mathbf{a} + \mathbf{v}\}$ se le llama *recta afín*. Las rectas afines poseen dos puntos. Empleando un sencillo argumento de combinatoria, dado que 2 puntos distintos determinan una recta afín, se observa que hay $\binom{2^m}{2}$ rectas afines diferentes. He aquí un listado con las 28 rectas afines de $EG(3, 2) = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7, \mathbf{v}_8\}$.

$\{\mathbf{v}_1, \mathbf{v}_2\}$	$\{\mathbf{v}_2, \mathbf{v}_3\}$	$\{\mathbf{v}_3, \mathbf{v}_5\}$	$\{\mathbf{v}_4, \mathbf{v}_8\}$
$\{\mathbf{v}_1, \mathbf{v}_3\}$	$\{\mathbf{v}_2, \mathbf{v}_4\}$	$\{\mathbf{v}_3, \mathbf{v}_6\}$	$\{\mathbf{v}_5, \mathbf{v}_6\}$
$\{\mathbf{v}_1, \mathbf{v}_4\}$	$\{\mathbf{v}_2, \mathbf{v}_5\}$	$\{\mathbf{v}_3, \mathbf{v}_7\}$	$\{\mathbf{v}_5, \mathbf{v}_7\}$
$\{\mathbf{v}_1, \mathbf{v}_5\}$	$\{\mathbf{v}_2, \mathbf{v}_6\}$	$\{\mathbf{v}_3, \mathbf{v}_8\}$	$\{\mathbf{v}_5, \mathbf{v}_8\}$
$\{\mathbf{v}_1, \mathbf{v}_6\}$	$\{\mathbf{v}_2, \mathbf{v}_7\}$	$\{\mathbf{v}_4, \mathbf{v}_5\}$	$\{\mathbf{v}_6, \mathbf{v}_7\}$
$\{\mathbf{v}_1, \mathbf{v}_7\}$	$\{\mathbf{v}_2, \mathbf{v}_8\}$	$\{\mathbf{v}_4, \mathbf{v}_6\}$	$\{\mathbf{v}_6, \mathbf{v}_8\}$
$\{\mathbf{v}_1, \mathbf{v}_8\}$	$\{\mathbf{v}_3, \mathbf{v}_4\}$	$\{\mathbf{v}_4, \mathbf{v}_7\}$	$\{\mathbf{v}_7, \mathbf{v}_8\}$

Tabla 3.1: Rectas afines de $EG(3, 2)$.

(iii) Si V tiene dimensión 2 (por lo que V es un plano vectorial), sabemos que existen $\mathbf{v}, \mathbf{w} \in V$ no nulos y linealmente independientes tales que $V = \{\lambda\mathbf{v} + \mu\mathbf{w} \mid \lambda, \mu \in \mathbb{F}_2\} = \{\mathbf{0}, \mathbf{v}, \mathbf{w}, \mathbf{v} + \mathbf{w}\}$. En este caso, a $\mathbf{a} + V = \{\mathbf{a}, \mathbf{a} + \mathbf{v}, \mathbf{a} + \mathbf{w}, \mathbf{a} + \mathbf{v} + \mathbf{w}\}$ se le llama *plano afín*. Los planos afines poseen cuatro puntos. Se prueba que existen $4^{-1}\binom{2^m}{3}$ planos afines diferentes (véase el **Problema 3.3**).

(iv) Si V tiene dimensión $m-1$ (por lo que V es un hiperplano vectorial), dada una base $\mathfrak{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_{m-1}\}$ de V, se tiene que

$$\mathbf{a} + V = \{\mathbf{a} + \lambda_1\mathbf{v}_1 + \cdots + \lambda_{m-1}\mathbf{v}_{m-1} \mid \lambda_1, ..., \lambda_{m-1} \in \mathbb{F}_2\}.$$

En este caso, a $\mathbf{a}+V$ se le llama *hiperplano afín*. Se prueba que existen $2(2^m - 1)$ hiperplanos afínes diferentes (véase el **Problema 3.3**).

La siguiente caracterización determina cuando un subconjunto de $EG(m, 2)$ es una variedad afín.

Proposición 3.3.1. *Un subconjunto de $EG(m, 2)$ es una k-variedad si, y sólo si, este es el conjunto de soluciones de un sistema de $m-k$ ecuaciones lineales en m variables con rango $m-k$.*

Demostración. Sea V un $\mathbb{F}_2$-subespacio vectorial de $\mathbb{F}_2^m$ de dimensión k (lo que hemos llamado código lineal binario de longitud m y dimensión k). Tomamos $H \in \mathrm{Mat}_{(m-k)\times m}(\mathbb{F}_2)$ una matriz de control de V. Entonces, $\mathbf{x} \in V$ si, y sólo si, $\mathbf{x}H^T = \mathbf{0}$ (los vectores de V son las soluciones de un sistema de $m-k$ ecuaciones homogéneas en m variables con rango $m-k$). Sea $\mathbf{a} \in EG(m, 2)$. Por definición, $\mathbf{a}+V$ es una k-variedad. Ahora, $\mathbf{x} \in \mathbf{a}+V$ si, y sólo si, se tiene que $\mathbf{x} - \mathbf{a} \in V$. Por tanto, $\mathbf{x} \in \mathbf{a} + V$ si, y sólo si, se cumple que $\mathbf{x}H^T = \mathbf{a}H^T$. Tenemos así un sistema lineal de $m-k$ ecuaciones con m incógnitas, cuya solución son, precisamente, los puntos de $\mathbf{a}+V$. □

3.3.2. Interpretación Geométrica $\mathcal{RM}(r, m)$

Consideremos un polinomio Booleano de m indeterminadas F. Fijado un orden $EG(m, 2) = \mathbb{F}_2^m = \{\mathbf{v}_1, ..., \mathbf{v}_{2^m}\}$, asociamos a este polinomio, además de la correspondiente palabra binaria $\mathbf{F} = F_1F_2...F_{2^m}$, el subconjunto

$$S_F = \{\mathbf{v} \in \mathbb{F}_2^m \mid F(\mathbf{v}) = 1\} = \{\mathbf{v}_i \mid F_i = 1\} \subseteq EG(m, 2).$$

Además, como la aplicación ψ_m introducida en (3.1) es biyectiva, de esta forma, se obtienen todos los subconjuntos de $EG(m, 2)$. En efecto, dado $S \subseteq EG(m, 2)$, este nos determina de manera unívoca una determinada palabra $\mathbf{x} = x_1x_2 \ldots x_{2^m} \in \mathbb{F}_2^{2^m}$ como sigue:

$$\forall i \in \{1, 2, ..., 2^m\}, \qquad x_i = \begin{cases} 1, & \text{si} \quad \mathbf{v}_i \in S; \\ 0, & \text{si} \quad \mathbf{v}_i \notin S. \end{cases}$$

Ahora, por ser ψ_m biyectiva, obtenemos un único polinomio Booleano F tal que $\mathbf{F} = \mathbf{x}$. En otras palabras, para cada subconjunto $S \subseteq EG(m, 2)$, existe un único polinomio Booleano F tal que $S = S_F$. En estas condiciones, debido a la unicidad, diremos que F es el *polinomio Booleano asociado a S*, y $\mathbf{F}$ es la *palabra característica asociada a S*.

Esto que acabamos de explicar nos permite establecer la siguiente notación, que no debería resultar sorprendente, dado que es coherente con la que hemos estado empleando hasta ahora.

- Dada una palabra binaria $\mathbf{x} \in \mathbb{F}_2^{2^m}$, vamos a denotar por $F_{\mathbf{x}}$ al polinomio Booleano correspondiente, y por $S_{\mathbf{x}}$ al subconjunto de $EG(m,2)$ para el que $\mathbf{x}$ es palabra característica asociada.
- Dado un polinomio Booleano F, vamos a denotar por $\mathbf{x}_F$ a la correspondiente palabra binaria asociada, y por S_F al subconjunto de $EG(m,2)$ para el que F es polinomio Booleano asociado.
- Dado un subconjunto $S \subseteq EG(m,2)$, vamos a denotar por $\mathbf{x}_S$ a la palabra característica asociada a S, y por F_S al polinomio Booleano asociado a S.

Nuestro objetivo es describir los códigos de Reed-Muller binarios en términos de las variedades afines de $EG(m,2)$ (que no son más que un tipo especial de subconjuntos de $EG(m,2)$). Para ello, es necesario hallar una correspondencia entre los polinomios Booleanos de un cierto grado y las variedades afines de cierta dimensión dada.

Proposición 3.3.2. *Si S es una k-variedad, entonces el correspondiente polinomio Booleano asociado tiene grado $m-k$.*

Demostración. Sea $S = \mathbf{a} + V$ una k-variedad. Según lo visto en la **Proposición 3.3.1**, sabemos que S es el conjunto de soluciones de un sistema de $m-k$ ecuaciones lineales en m variables con rango $m-k$. Supongamos, sin pérdida de generalidad, que este sistema viene dado como sigue:

$$\begin{cases} l_1(x_1,...,x_m) &= 1, \\ l_2(x_1,...,x_m) &= 1, \\ \vdots & \vdots \ \vdots \\ l_{m-k}(x_1,...,x_m) &= 1. \end{cases} \tag{3.5}$$

Ahora bien, es obvio que $(x_1,...,x_m)$ es solución de (3.5) si, y sólo si, es también solución de la ecuación

$$\prod_{i=1}^{m-k} l_i(x_1,...,x_m) = 1, \tag{3.6}$$

donde, como cada ecuación de (3.5) es lineal, el polinomio a la izquierda de (3.6) tiene grado $m-k$. En resumen, se ha probado que

$$S = \{(x_1,...,x_m) \mid \prod_{i=1}^{m-k} l_i(x_1,...,x_m) = 1\},$$

de donde se sigue que el polinomio asociado a S, que denotamos por F_S, es precisamente $F_S = \prod_{i=1}^{m-k} l_i(x_1,...,x_m)$, que tiene grado $m-k$. □

Nota 3.3.1. El recíproco a este resultado es falso en general, ya que se pueden encontrar polinomios Booleanos F cuyos correspondientes subconjuntos $S_F \subseteq EG(m,2)$ no son variedades afines (véase el **Problema 3.4**). Sin embargo, el recíproco sí que es cierto para el caso particular de los monomios Booleanos. En efecto, el subconjunto S_F que tiene asociado al monomio Booleano $F = x_{i_1} \cdots x_{i_s}$ de grado s es una $(m-s)$-variedad, pues se trata del conjunto de soluciones del sistema de s ecuaciones lineales

$$x_{i_1} = 1, \ldots, x_{i_s} = 1.$$

En particular, los subconjuntos S_{x_i} son hiperplanos afines.

Ya estamos en condiciones de dar la caracterización geométrica de $\mathcal{RM}(r,m)$ buscada.

Teorema 3.3.3. *El código de Reed-Muller binario $\mathcal{RM}(r,m)$ es el subespacio vectorial generado por las palabras características asociadas a todas las variedades afines de $EG(m,2)$, con dimensión al menos $m-r$.*

Demostración. Sea $\mathbf{x}$ la palabra característica asociada a una variedad afín de dimensión al menos $m-r$ (la cual denotaremos por $S_{\mathbf{x}}$). Supongamos que $F_{\mathbf{x}}$ es el polinomio Booleano que tiene asociada esta palabra característica $\mathbf{x}$. Entonces, en virtud de la **Proposición 3.3.2**, se tiene que este polinomio Booleano tiene grado menor o igual que r. Así, por como se definen los códigos de Reed-Muller binarios, se tiene que $\mathbf{x} \in \mathcal{RM}(r,m)$. Recíprocamente, sea F el polinomio Booleano asociado a una palabra $\mathbf{x}_F$ de $\mathcal{RM}(r,m)$. Sabemos que este tiene grado $s \leq r$. Supongamos que $F = \sum_{i=1}^{l} P_i$, siendo estos los monomios Booleanos en los que se descompone F (los cuales tienen grado $\deg(P_i) \leq s$, para todo $i \in \{1, ..., l\}$). Por linealidad de (3.1), se tiene que $\mathbf{x}_F = \sum_{i=1}^{l} \mathbf{x}_{P_i}$ es la palabra asociada a F. Ahora bien, según lo visto en la **Nota 3.3.1**, cada $\mathbf{x}_{P_i}$ es la palabra característica asociada a una variedad afín de dimensión $m - \deg(P_i) \geq m - s$. Por tanto, $\mathbf{x}_F$ es suma de palabras características de variedades afines de dimensión al menos $m - s \geq m - r$, de donde se concluye el resultado. □

Una consecuencia inmediata de este teorema, que necesitaremos cuando tratemos la decodificación en los códigos de Reed-Muller binarios, es la siguiente:

Corolario 3.3.4. *Todas las palabras características asociadas a conjuntos que sean $(r+1)$-variedades de $EG(m,2)$ son elementos de $\mathcal{RM}(r,m)^{\perp}$.*

Demostración. El resultado es consecuencia inmediata del **Teorema 3.3.3** y del **Problema 2.2**. En efecto, basta aplicar este teorema al código de Reed-Muller binario $\mathcal{RM}(m-r-1,m) = \mathcal{RM}(r,m)^{\perp}$. □

3.4. Problemas Resueltos

Problema 3.1. Describir el código de Reed-Muller $\mathcal{RM}(1,5)$: calcular una matriz generadora, su dimensión y su distancia mínima.

Solución. Para obtener una matriz generadora, basta usar la **Subrutina A.1**. Esta nos permite calcular la matriz generadora de $\mathcal{RM}(1,5)$ que vimos en la **Proposición 3.2.5**. Así, escribiendo en *Mathematica* la instrucción

```
matgeniter[1,5]//MatrixForm
```

obtenemos la matriz siguiente:

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

Ahora bien, como esta matriz generadora tiene rango máximo 6 (que coincide con el número de filas de la misma), la dimensión del código $\mathcal{RM}(1,5)$ es, precisamente, 6. Finalmente, la distancia mínima se obtiene a partir de la fórmula dada en la **Proposición 3.2.4**. Por tanto, como $m = 5$ y $r = 1$, la distancia mínima del código dado es 16. □

Observación 3.4.1. El código estudiado en el **Problema 3.1** es el código de Reed-Muller que llevaban equipado las naves espaciales de la NASA en la década de los años 50. Ya hablamos de este en la Sección 2.1.

Problema 3.2. Probar que las palabras características de todo monomio Booleano de grado exactamente $t \geq 0$ tienen peso 2^{m-t}. Deducir de este hecho que todas las palabras de $\mathcal{RM}(r,m)$, con $r < m$, tienen peso par. Concluir que $\mathcal{RM}(m-1,m)$ se corresponde con el conjunto de todas las palabras binarias de $\mathbb{F}_2^{2^m}$ de peso par.

Solución. Sea $F \in \mathbb{F}_2[x_1,...,x_m]$ un monomio de grado t, y vamos a suponer que se tiene fijado un orden $\mathbb{F}_2^m = \{\mathbf{v}_1,...,\mathbf{v}_{2^m}\}$. Por hipótesis, como F es de grado t, se tiene que $F = x_{i_1}\cdots x_{i_t}$, con $i_1,...,i_t \in \{1,...,m\}$. Queremos probar que $\mathbf{F}$ tiene peso 2^{m-t}. Por (1.2), como estamos en el caso binario, sabemos que $\omega(\mathbf{F}) = \sum_{i=1}^{2^m} F_i$, pues $F_i \in \{0,1\}$, para todo $i \in \{1,...,2^m\}$. Además, dado el vector $\mathbf{v}_j$ que ocupa la posición j-ésima en el orden establecido, tenemos la siguiente caracterización para las letras de $\mathbf{F}$:

$$F_j = 1 \Longleftrightarrow v_{ji_1} = \cdots = v_{ji_t} = 1, \qquad \forall j \in \{1,...,2^m\}.$$

Si conseguimos probar que hay 2^{m-t} letras F_j que verifican esta equivalencia, habremos terminado. Pero esto es inmediato, pues fijadas estas t coordenadas $\{i_1,...,i_t\}$ en cada vector $\mathbf{v}_j \in \mathbb{F}_2^m$, quedan libres las $m-t$ restantes,

que pueden tomar 2 valores distintos. A partir de aquí, con un sencillo argumento combinatorio, se concluye el resultado.

Ahora, como hemos visto en la **Proposición 3.1.2** que una matriz generadora de este código tiene por filas las palabras características de algunos monomios Booleanos, que acabamos de ver que tienen en particular peso par cuando su grado es menor estrictamente que m, se sigue del comentario hecho al final de la Sección 3.1 que toda palabra de $\mathcal{RM}(r,m)$, para $r<m$, tiene también peso par. Además, como $\mathcal{RM}(m-1,m)$ está formado por la mitad de las palabras de $\mathbb{F}_2^{2^m}$, pues

$$\dim(\mathcal{RM}(m-1,m)) = \sum_{k=0}^{m-1} \binom{m}{k} = 2^m - 1,$$

por lo que acabamos de probar, necesariamente $\mathcal{RM}(m-1,m)$ tiene que ser el conjunto de todas las palabras de $\mathbb{F}_2^{2^m}$ con peso par. □

Problema 3.3. Determinar el número de planos e hiperplanos afines en $EG(m,2)$. Calcularlos en el caso de $EG(3,2)$, determinando sus palabras características asociadas para el orden canónico de $\mathbb{F}_2^3$.

Solución. Empecemos calculando el número de planos afines en $EG(m,2)$, que no es más que un problema de combinatoria. Ya hemos visto que se tienen 2^m puntos distintos, y que los planos afines son de la forma siguiente:

$$\{\mathbf{a}+\lambda_1\mathbf{v}+\lambda_2\mathbf{w} \mid \lambda_1,\lambda_2 \in \{0,1\}\} = \{\mathbf{a}, \mathbf{a}+\mathbf{v}, \mathbf{a}+\mathbf{w}, \mathbf{a}+\mathbf{v}+\mathbf{w}\},$$

donde $\mathbf{v}$ y $\mathbf{w}$ son vectores no nulos y linealmente independientes de $\mathbb{F}_2^m$. Obsérvese que fijados $\mathbf{a}$,$\mathbf{v}$ y $\mathbf{w}$, el último punto del plano viene siempre determinado. En otras palabras, se tiene que tres puntos nos determinan un plano afín, de donde en un principio se sigue que hay $\binom{2^m}{3}$ plano afines. Sin embargo, como a su vez cada uno de estos planos viene determinado por 3 cualesquiera de sus 4 puntos, en esta cuenta estamos contando planos de más. Concretamente, se cuenta $\binom{4}{3} = 4$ veces cada plano. En conclusión, se tienen $4^{-1}\binom{2^m}{3}$ planos afines diferentes en $EG(m,2)$.

Veamos ahora el número de hiperplanos afines. En esta ocasión, vamos a seguir una estrategia de conteo distinta. Para empezar, vamos a determinar el número de hiperplanos vectoriales de $\mathbb{F}_2^m$. Por Álgebra Lineal, por como viene dada la dimensión de los subespacios ortogonales, basta calcular el número de subconjuntos $<\mathbf{v}>\subseteq \mathbb{F}_2^m$ en los que $\mathbf{v}\neq\mathbf{0}$, puesto que estos coinciden. Es obvio que hay 2^m-1 subconjuntos de este tipo. Hecho esto, pasemos a calcular el número de variedades afines $\mathbf{a}+V$, con V hiperplano vectorial fijo (que ya hemos visto que hay 2^m-1 distintos). Pero, dado que el número de clases de equivalencia de este tipo coincide con el cociente entre

el número de puntos de $EG(m,2)$ (que es 2^m) y el número de vectores que hay en V (que es fácil ver, con un argumento análogo al empleado con los planos afines, que es 2^{m-1}), se tiene que hay un total de 2 clases de equivalencia distintas para cada hiperplano vectorial V fijado. En definitiva, por el **Principio Multiplicativo**, podemos concluir que se tienen $2(2^m-1)$ hiperplanos afines distintos en $EG(m,2)$.

Fijado el orden canónico $EG(3,2) = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7, \mathbf{v}_8\}$, he aquí la lista con sus 14 planos afines junto con sus correspondientes palabras características asociadas para dicho orden:

plano	palabra	plano	palabra
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$	11110000	$\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_8\}$	01101001
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_5, \mathbf{v}_6\}$	11001100	$\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_6, \mathbf{v}_7\}$	01100110
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_7, \mathbf{v}_8\}$	11000011	$\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_7\}$	01011010
$\{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_7\}$	10101010	$\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_6, \mathbf{v}_8\}$	01010101
$\{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_6, \mathbf{v}_8\}$	10100101	$\{\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6\}$	00111100
$\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_8\}$	10011001	$\{\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_7, \mathbf{v}_8\}$	00110011
$\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_6, \mathbf{v}_7\}$	10010110	$\{\mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7, \mathbf{v}_8\}$	00001111

Tabla 3.2: Planos afines de $EG(3,2)$.

Es obvio que estos coinciden con los hiperplanos afines de $EG(3,2)$. □

Problema 3.4. Demostrar que el recíproco de la **Proposición 3.3.2** es falso en general.

Solución. Basta con dar un contraejemplo, esto es, hay que hallar un polinomio Booleano F de grado k tal que el subconjunto $S_F \subseteq EG(m,2)$, asociado a F, no sea una $(m-k)$-variedad. De hecho, es inmediato observar que en tal caso este no sería si quiera una variedad afín. En efecto, pues si este fuese una variedad afín de dimensión distinta a $m-k$, llegaríamos a un absurdo debido a la **Proposición 3.3.2** por tener F grado k.

Sea $F = x_1x_2 + x_3$ un polinomio Booleano de 3 variables, que tiene grado 2. Veamos que $S_F \subseteq EG(3,2)$ no es una variedad afín argumentando por reducción al absurdo. Supongamos que S_F es una variedad afín. Por lo que hemos mencionado antes, necesariamente, por tener F grado 2, esta tendría que ser una recta afín. Pero esto es absurdo, ya que

$$S_F = \{(x_1,x_2,x_3) \in \mathbb{F}_2^3 \mid x_1x_2 + x_3 = 1\} =$$
$$= \{(1,1,0),(0,0,1),(1,0,1),(0,1,1)\}$$

y las rectas afines tienen exactamente 2 puntos. En resumen, queda probado que el recíproco de la **Proposición 3.3.2** es falso en general. □

Capítulo 4

Codificación y Decodificación

En este último capítulo, se presentan los métodos de codificación y decodificación para los códigos de Reed-Muller binarios.

4.1. Generalidades

Antes de empezar, conviene repasar algunas generalidades acerca de codificación y decodificación en códigos lineales y cíclicos. Vamos a recuperar, por tanto, resultados de la asignatura optativa de Cuarto del Grado en Matemáticas de la UPV/EHU *Códigos y Criptografía*.

4.1.1. Codificación en Códigos Lineales y Cíclicos

Ya hemos dicho que para dar un código lineal $\mathcal{C}$ es suficiente dar una matriz generadora. Nos preguntamos ahora: ¿se puede obtener una matriz generadora de expresión lo más sencilla posible? La respuesta a esta pregunta nos la da el resultado del Álgebra Lineal que nos dice que toda matriz $G \in \mathrm{Mat}_{s\times n}(\mathbb{F}_q)$ (con $s \leq n$) de rango máximo s puede llevarse, realizando operaciones elementales en filas y columnas, a una matriz de la forma $(I_s|B)$. A esta expresión se la conoce por *forma estándar*. Sin embargo, para que el código con matriz generadora $(I_s|B)$ sea el mismo que aquel con matriz generadora G, deben realizarse estas transformaciones elementales sólo por filas. En consecuencia, no todo código lineal admite una matriz generadora dada en forma estándar. La importancia de las matrices generadoras dadas en forma estándar radica en que es fácil codificar con ellas ya que, dada una palabra $\mathbf{x} \in \mathbb{F}_q^s$, esta se codifica como

$$\mathbf{x}(I_s|B) = (x_1 \dots x_s \underbrace{c_{s+1} \dots c_n}_{\text{redundancias}}), \tag{4.1}$$

donde es evidente que esta se corresponde con una palabra código en la que las s primeras letras son, precisamente, las de la palabra original $\mathbf{x}$. Cabe

observar que si $(I_s|B)$ es una matriz generadora de un cierto código lineal, entonces podemos dar una matriz de control por:

$$H = (-B^\top | I_{n-s}) \in \mathrm{Mat}_{(n-s)\times n}(\mathbb{F}_q). \tag{4.2}$$

En el caso de los códigos cíclicos siempre es posible obtener una codificación donde la palabra a emitir lleve en las últimas posiciones a las letras de la palabra original que se desea codificar. Para ello, dado el código cíclico $\mathcal{C}$, suponiendo que tenemos la palabra original $\mathbf{y} \in \mathbb{F}_q^k$ ($\dim(\mathcal{C}) = k$), se genera el polinomio $b(x) = \sum_{i=0}^{k-1} y_i x^{n-1-i}$. Tomando ahora el resto $r(x) = \sum_{i=0}^{l} r_i x^i$ de dividir este polinomio $b(x)$ entre el polinomio generador de nuestro código $\mathcal{C}$ (el cual, por ser el grado del polinomio generador $n-k$, tendrá que tener, por el algoritmo de la división, grado menor que $n-k$, esto es, $l < n-k$), se tiene que $b(x) - r(x) \in \mathcal{C}(x)$. Consecuentemente, por como vienen dados $b(x)$ y $r(x)$, tenemos la palabra código $-r_0 \ldots - r_l y_{k-1} \ldots y_0$ que tomamos como codificación de nuestra palabra original.

4.1.2. Métodos Generales de Decodificación

Se tienen tres métodos de decodificación generales.

El primero, válido para todo código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$, es el llamado *método de decodificación basado en líderes*. Este se basa en la relación de equivalencia sobre $\mathbb{F}_q^n$ siguiente:

$$\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n,\ \mathbf{x}\mathfrak{R}\mathbf{y} \Longleftrightarrow \mathbf{x} - \mathbf{y} \in \mathcal{C}.$$

Supongamos que se desea decodificar $\mathbf{z} \in \mathbb{F}_q^n$. Se buscan en $[\mathbf{z}]$ (clase representada por $\mathbf{z}$) las palabras de menor peso posible (estas se conocen por líderes de $[\mathbf{z}]$). Sea una de estas $\mathbf{e_z}$. Entonces, se decodifica $\mathbf{z}$ por $\mathbf{z} - \mathbf{e_z}$, que es una palabra código (se toma por tanto como error cometido en la transmisión al líder elegido). Esta palabra $\mathbf{z}$ admitirá decodificación única en el caso de que $\omega(\mathbf{e_z}) \leq \lfloor \frac{d-1}{2} \rfloor$, siendo d la distancia mínima de $\mathcal{C}$. Este método es útil cuando se conocen todas las palabras del código o no es muy difícil calcularlas.

Otro método de decodificación alternativo válido para todo código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$ con matriz de control H conocida es el llamado *método de decodificación basado en síndromes*. Este se basa en la relación de equivalencia sobre $\mathbb{F}_q^n$ siguiente:

$$\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n,\ \mathbf{x} \sim \mathbf{y} \Longleftrightarrow S(\mathbf{x}) = S(\mathbf{y}),$$

donde $S(\mathbf{x}) = \mathbf{x}H^T$ es lo que se conoce por *síndrome* de $\mathbf{x}$ *respecto de* H. Supongamos que se desea decodificar $\mathbf{z} \in \mathbb{F}_q^n$. Si $S(\mathbf{z}) = \mathbf{0}$, se tiene que $\mathbf{z}$

es una palabra código y se decodifica tal cual. En caso contrario, hay que buscar en $\bar{\mathbf{z}}$ (clase representada por $\mathbf{z}$) una palabra $\mathbf{e_z}$ de peso lo mínimo posible, para decodificar $\mathbf{z}$ como $\mathbf{z} - \mathbf{e_z}$, que es claramente una palabra código. Para obtener $\mathbf{e_z}$, en la práctica construimos una tabla con los síndromes de todas las palabras de $\mathbb{F}_q^n$, ordenadas por pesos de menor a mayor. Normalmente, se construye una tabla con los síndromes de las palabras con peso hasta $\lfloor \frac{d-1}{2} \rfloor$, siendo d la distancia mínima de $\mathcal{C}$. A esta tabla se la conoce por **tabla de síndromes**. Si el síndrome de nuestra palabra coincide con alguno de la tabla, podremos asegurar que la decodificación será única. Sin embargo, no podemos garantizar que esta decodificación vaya a ser única si el peso de la palabra líder es mayor que $\lfloor \frac{d-1}{2} \rfloor$. Este método es útil cuando conocemos una matriz de control del código o esta es fácil de calcular (como sucede por ejemplo en los códigos cíclicos).

Por último, se tiene el llamado *método de decodificación cíclica*, el cual es sólo válido para códigos cíclicos $\mathcal{C} \subseteq \mathbb{F}_q^n$ con matriz de control H conocida. Este es un caso particular del método de decodificación basado en síndromes. El objetivo es construir lo que se conoce como **tabla reducida de síndromes**, que no es más que la tabla formada por los síndromes de las palabras líder que tengan la última (esta posición se elige sin pérdidad de generalidad) componente no nula. Supongamos que se busca decodificar la palabra $\mathbf{y}$. Se calcula $S(\mathbf{y}^{(i)})$ (recordemos que esta notación fue introducida al comienzo de la Sección 1.3), para todo $i \in \{0, 1, ..., n-1\}$, hasta que este valor coincida con alguno de los síndromes $S(\mathbf{e})$ de la tabla reducida de síndromes. Suponiendo que se da la coincidencia en el paso i-ésimo, se decodifica $\mathbf{y}$ como la palabra $\mathbf{x}$ tal que $\mathbf{x}^{(i)} = \mathbf{y}^{(i)} - \mathbf{e}$. Si no ha sido posible calcular $\mathbf{x}$ a través del proceso anterior, significa que no podemos asegurar que nuestra palabra tenga decodificación única. En estos casos, tal y como se hace en el método de decodificación basado en síndromes, hay que ampliar esta tabla hasta dar con una decodificación.

4.2. Codificación en Códigos de Reed-Muller

El objetivo de esta sección es establecer un procedimiento de codificación para los códigos de Reed-Muller binarios. Este se basa en que es posible obtener un orden para los elementos de $\mathbb{F}_2^m$ tal que $\mathcal{RM}(r, m)$ admite una matriz generadora dada en forma estándar. Para ello, vamos a aplicar el resultado del Álgebra Lineal antes mencionado, cuya demostración en el caso binario nos servirá para diseñar la **Subrutina A.2**.

Proposición 4.2.1. *Toda matriz binaria $G \in Mat_{s\times n}(\mathbb{F}_2)$ de rango máximo $s \leq n$ puede llevarse, realizando operaciones elementales por filas y permutaciones en las columnas, a una matriz dada en forma estándar.*

Demostración. Sea $G = (g_{ij})_{(i,j)\in\{1,...,s\}\times\{1,...,n\}} \in \mathrm{Mat}_{s\times n}(\mathbb{F}_2)$. Aplicamos inducción sobre n. Si $n = 1$, la demostración es trivial. Supongamos cierto el resultado para $n-1$. Como el rango de G coincide con el número de filas, necesariamente en cada una de estas ha de existir al menos un elemento no nulo. Bajo estas circunstancias, pueden darse los dos casos siguientes:

a) Si $g_{11} = 1$, para cada $i \in \{2, ..., s\}$, sustituimos cada fila i-ésima de G por la fila i-ésima de G menos la primera fila de G. De esta forma, a través de operaciones elementales por filas, transformamos G en la matriz

$$\left(\begin{array}{c|c} 1 & \\ 0 & \\ \vdots & B \\ 0 & \end{array}\right),$$

donde $B \in Mat_{s\times(n-1)}(\mathbb{F}_2)$. Aplicando la hipótesis de inducción a B se concluye el resultado.

b) Si $g_{11} = 0$, ha de existir una columna j de G tal que $g_{1j} = 1$. Permutamos las columnas 1 y j de G entre sí, de forma que ahora en la posición $(1, 1)$ de la nueva matriz tengamos un 1. Esta nueva matriz está en las condiciones de a). Aplicando entonces dicho proceso, se obtiene el resultado.

En resumen, queda probada la propiedad deseada. □

Corolario 4.2.2. *Dado el código de Reed-Muller binario $\mathcal{RM}(r, m)$, es posible hallar un orden para los elementos de $\mathbb{F}_2^m$ tal que $\mathcal{RM}(r, m)$ admita una matriz generadora dada en forma estándar.*

Demostración. Supongamos que tenemos fijado el *orden canónico* para el código de Reed-Muller binario $\mathcal{RM}(r, m)$. Entonces, la **Proposición 3.2.5** nos da una matriz generadora de $\mathcal{RM}(r, m)$, la cual se encuentra bajo las hipótesis de la **Proposición 4.2.1**. Por consiguiente, podemos llevar esta matriz a una dada en forma estándar a través de operaciones elementales por filas y permutando columnas entre sí. Pero esto último es equivalente a intercambiar la posición de dos letras en todas las palabras código de $\mathcal{RM}(r, m)$, lo cual significa que se han intercambiado de posición dos vectores en $\mathbb{F}_2^m$. Se concluye así el resultado. □

Llamaremos al orden de $\mathbb{F}_2^m$ que se obtiene con el **Corolario 4.2.2**, siguiendo los pasos de la demostración de la **Proposición 4.2.1**, *orden estándar* de $\mathbb{F}_2^m$.

Estos resultados nos permiten establecer un procedimiento de codificación en los códigos de Reed-Muller binarios. En efecto, dado el código $\mathcal{RM}(r, m)$, basta fijar un orden estándar de $\mathbb{F}_2^m$ para realizar el proceso de codificación tal y como se explica en (4.1).

4.3. Decodificación en Códigos de Reed-Muller: Algoritmo de Reed

Una de las mayores ventajas que tiene el uso de los códigos de Reed-Muller binarios es su fácil decodificación por el llamado *algoritmo de Reed*. Este toma como base un método muy práctico y eficiente de decodificación para cierto tipo de códigos lineales, que se conoce por *método de decodificación por mayoría*. La principal característica de este método es que no emplea síndromes, sino que detecta directamente las posiciones donde se han producido los errores a partir de las propiedades de la palabra recibida. Así, si el código lineal dado es binario, seremos capaces de llevar a cabo la decodificación trivialmente. No entraremos a explicar en detalle este método general para evitar alargarnos. Pueden encontrarse breves resúmenes del mismo en [6, Problema 6.6] y [2, Section 4.14]. Para explicar el algoritmo de Reed, tomaremos como referencias [1, Chapter 9] y [6, Capítulo 12].

Hay muchas formas de presentar el algoritmo de Reed, pero la mejor manera de hacerlo es en términos de la geometría finita $EG(m,2)$. La idea es la siguiente: supongamos que fijado un orden $\mathbb{F}_2^m = EG(m,2) = \{\mathbf{v}_1, ..., \mathbf{v}_{2^m}\}$, se ha enviado una palabra código $\mathbf{c} \in \mathcal{RM}(r,m)$, a partir de la cual recibimos $\mathbf{y} = \mathbf{c} + \mathbf{e}$. Asumiendo que $\omega(\mathbf{e}) \leq 2^{m-r-1}$, se trata de determinar las posiciones $i \in \{1, 2, ..., 2^m\}$ en las que se hayan cometido errores durante la transmisión. Para ello, reformularemos el problema empleando las 0-variedades de $EG(m,2)$. Necesitamos el siguiente concepto de *paridad*.

Definición 4.3.1. Dadas una k-variedad $S \subseteq EG(m,2)$ y una palabra $\mathbf{y} = \mathbf{c} + \mathbf{e}$, recibida durante la transimisión de información ($\mathbf{c}$ palabra código enviada y $\mathbf{e}$ error dado en la transmisión), diremos que S es *par respecto de* $\mathbf{y}$ si esta palabra $\mathbf{y}$ contiene un número par de errores en las posiciones del soporte de la palabra característica asociada a S. En caso contrario, diremos que S *es impar respecto de* $\mathbf{y}$.

Recordemos que el *soporte* de una palabra $\mathbf{x}$ de longitud n, que se denota por $\text{sop}(\mathbf{x})$, se define por:

$$\text{sop}(\mathbf{x}) = \{i \in \{1, ..., n\} \mid x_i \neq 0\}. \tag{4.3}$$

Sea S una k-variedad. Si denotamos por $\mathbf{x}_S$ a la palabra característica asociada a S, por la **Definición 4.3.1** y (4.3), la paridad de S respecto de $\mathbf{y}$ viene determinada por la del producto escalar $< \mathbf{x}_S, \mathbf{e} >$. Como además en el caso binario este valor coincide con el peso de la palabra producto $\mathbf{x}_S\mathbf{e}$, podemos definir alternativamente la paridad de S respecto de $\mathbf{y}$ como la paridad de $\omega(\mathbf{x}_S\mathbf{e})$.

Así, por como vienen dadas las palabras características de las 0-variedades,

determinar si la i-ésima coordenada de $\mathbf{y}$ es correcta o no equivale a calcular la paridad de $\{\mathbf{v}_i\} \subseteq EG(m,2)$. En efecto, denotando por $\mathbf{x}_{\{\mathbf{v}_i\}}$ a la palabra característica asociada a $\{\mathbf{v}_i\}$, se tiene que $e_i = 1$ si, y sólo si, $\omega(\mathbf{x}_{\{\mathbf{v}_i\}}\mathbf{e}) = 1$ (pues $\mathbf{x}_{\{\mathbf{v}_i\}}$ tiene todas sus coordenadas nulas, salvo aquella que ocupa la posición i-ésima). Desafortunadamente, la paridad de las 0-variedades no puede ser evaluada directamente (salvo que se conozca el error). Sin embargo, sí que podemos obtener esta para el caso de las $(r+1)$-variedades.

Proposición 4.3.1. *Recibida $\mathbf{y} = \mathbf{c} + \mathbf{e}$, donde $\boldsymbol{c} \in \mathcal{RM}(r,m)$ es la palabra código enviada y $\boldsymbol{e}$ el error dado en la transmisión, se tiene que la paridad respecto de $\mathbf{y}$ de las $(r+1)$-variedades coincide con la de $\omega(\mathbf{xy})$, siendo $\mathbf{x}$ la palabra característica asociada a la correspondiente variedad afín.*

Demostración. Sea S una $(r+1)$-variedad con palabra característica asociada $\mathbf{x}_S$. Por el **Corolario 3.3.4**, sabemos que $\mathbf{x}_S \in \mathcal{RM}(r,m)^{\perp}$. Así,

$$< \mathbf{x}_S, \mathbf{y} > \underset{def.}{=} < \mathbf{x}_S, \mathbf{c} + \mathbf{e} > \underset{lin.}{=} < \mathbf{x}_S, \mathbf{c} > + < \mathbf{x}_S, \mathbf{e} > \underset{def.}{=} < \mathbf{x}_S, \mathbf{e} > .$$

De aquí se sigue que la paridad de S respecto de $\mathbf{y}$ coincide con la de $\omega(\mathbf{x}_S\mathbf{y})$ en el caso binario. □

La idea es utilizar el conocimiento de las paridades respecto de $\mathbf{y}$ de las $(r+1)$-variedades para determinar la del resto de k-variedades, con $k \leq \leq r$. Para ello, vamos a proceder mediante lógica mayoritaria: dada una k-variedad S, suponiendo conocidas las paridades respecto de $\mathbf{y}$ de todas las $(k+1)$-variedades que contienen a S, diremos que su paridad respecto de $\mathbf{y}$ coincide con la de la mayoría de estas variedades afines.

Para probar el resultado que demuestra la veracidad de este mecanismo, se requieren primero dos resultados técnicos.

Lema 4.3.2. *Para cada k-variedad $S = \mathbf{a} + V$ de $EG(m,2)$ y cada punto $\mathbf{b} \in EG(m,2) - S$, existe una única variedad de dimensión $k+1$ que contiene a S y a $\mathbf{b}$.*

Demostración. Este es un resultado de existencia y unicidad. La prueba de existencia es inmediata, pues no hay más que comprobar que $\mathbf{a} + W$, donde $W = V \oplus \mathbb{F}_2(\mathbf{b} - \mathbf{a})$, es una $(k+1)$-variedad que contiene a S y a $\mathbf{b}$. Pasemos ahora a ver la unicidad. Supongamos sin pérdida de generalidad que $\mathbf{a} + W'$ es cualquier $(k+1)$-variedad que contiene a S y a $\mathbf{b}$. Es obvio que $V \subseteq W'$ y $\mathbf{b} \in \mathbf{a} + W'$. De esto último, se sigue que $\mathbf{b} - \mathbf{a} \in W'$, donde $\mathbf{b} - \mathbf{a} \notin V$. En consecuencia, necesariamente $W' = V \oplus \mathbb{F}_2(\mathbf{b} - \mathbf{a}) = W$ por ser ambos espacios vectoriales finitos de igual dimensión. Así, se tiene que $\mathbf{a} + W' = \mathbf{a} + W$, quedando probada la unicidad. □

Lema 4.3.3. *Cada k-variedad S de $EG(m,2)$, con $k < m$, está contenida en $2^{m-k} - 1$ variedades afines de dimensión $k+1$.*

Demostración. Según el **Lema 4.3.2**, para cada punto $\mathbf{b} \in EG(m,2) - -S$ existe una única $(k+1)$-variedad que contiene a S y a $\mathbf{b}$. Como cada k-variedad contiene 2^k puntos, existen $2^m - 2^k$ puntos en $EG(m,2) - S$, de los cuales exactamente $2^{k+1} - 2^k = 2^k$ generan la misma $(k+1)$-variedad que contiene a S. Así, el número total de $(k+1)$-variedades que contienen a S es

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

Queda por tanto probado el resultado. □

Hecho esto, ya podemos dar el resultado fundamental antes mencionado. Este suele conocerse como **Criterio de la lógica mayoritaria**.

Teorema 4.3.4. *Sean* $\mathbf{y}$ *una palabra recibida a partir de* $\mathcal{RM}(r,m)$ *y* S *una* k*-variedad, con* $0 \leq k \leq r$*, de* $EG(m,2)$*. Si el número de errores en* $\mathbf{y}$ *no supera los* $2^{m-r-1} - 1$*, entonces la paridad de* S *respecto de* $\mathbf{y}$ *coincide con la de la mayoría de las* $(k+1)$*-variedades que contienen a* S*.*

Demostración. Por el **Lema 4.3.3**, S está contenido en $2^{m-k} - 1$ variedades afines de dimensión $k+1$, donde cada una de estas viene determinada de forma unívoca dando un punto exterior a S en virtud del **Lema 4.3.2**. Por hipótesis, han de existir a lo más $2^{m-r-1} - 1$ variedades afines de dimensión $k+1$ que contengan a S determinadas por puntos exteriores a S correspondientes a una coordenada de $\mathbf{y}$ incorrecta. El resto de las $(k+1)$-variedades tienen la propiedad de que no contienen puntos exteriores a S correspondientes a coordenadas erróneas de $\mathbf{y}$. Así, por la **Definición 4.3.1**, estas tienen la misma paridad respecto de $\mathbf{y}$ que S. Entonces, por todo lo mencionado, el número de $(k+1)$-variedades con la misma paridad respecto de $\mathbf{y}$ que S es al menos de $(2^{m-k} - 1) - (2^{m-r-1} - 1)$. El resultado a partir de aquí se debe a que $2^{m-k} - 2^{m-r-1} \geq 2^{m-r-1}$, pues $k \leq r$. □

Tras todos estos resultados, podemos describir el algoritmo de Reed.

Algoritmo. Fijado el orden $\mathbb{F}_2^m = EG(m,2) = \{\mathbf{v}_1, ..., \mathbf{v}_{2^m}\}$ con el cual se ha construido $\mathcal{RM}(r,m)$, los pasos a seguir son los siguientes:

1) Recibida una palabra $\mathbf{y}$, asumiendo que esta contiene a lo más $2^{m-r-1} - 1$ errores, calculamos, empleando la **Proposición 4.3.1**, la paridad respecto de $\mathbf{y}$ de todas las $(r+1)$-variedades de $EG(m,2)$.

2) Empleando el **Criterio de la lógica mayoritaria** visto en el **Teorema 4.3.4**, se calculan las paridades respecto de $\mathbf{y}$ de todas las k-variedades de $EG(m,2)$, para $k \in \{r, r-1, ..., 0\}$.

3) Se corrigen las coordenadas de $\mathbf{y}$ correspondientes a todas las 0-variedades impares respecto de $\mathbf{y}$.

Ejemplo 4.3.1. Supongamos recibida la palabra 01100001, codificada mediante el orden canónico de $\mathbb{F}_2^3$ en $\mathcal{RM}(1,3)$, donde se ha producido un error. Vamos a decodificarla mediante el algoritmo de Reed. Primero calculamos la paridad de los planos afines de $EG(3,2) = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7, \mathbf{v}_8\}$ empleando la **Proposición 4.3.1**. Por la Tabla 3.2, estas son:

plano	paridad	plano	paridad
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$	par	$\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_8\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_5, \mathbf{v}_6\}$	impar	$\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_6, \mathbf{v}_7\}$	par
$\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_7, \mathbf{v}_8\}$	par	$\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_7\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_7\}$	impar	$\{\mathbf{v}_2, \mathbf{v}_4, \mathbf{v}_6, \mathbf{v}_8\}$	par
$\{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_6, \mathbf{v}_8\}$	par	$\{\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_8\}$	impar	$\{\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_7, \mathbf{v}_8\}$	par
$\{\mathbf{v}_1, \mathbf{v}_4, \mathbf{v}_6, \mathbf{v}_7\}$	par	$\{\mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7, \mathbf{v}_8\}$	impar

Ahora, por el **Criterio de la lógica mayoritaria** (**Teorema 4.3.4**), se calculan las paridades de las rectas afines (ver Tabla 3.1). Estas son:

recta	paridad	recta	paridad	recta	paridad	recta	paridad
$\{\mathbf{v}_1, \mathbf{v}_2\}$	par	$\{\mathbf{v}_2, \mathbf{v}_3\}$	par	$\{\mathbf{v}_3, \mathbf{v}_5\}$	impar	$\{\mathbf{v}_4, \mathbf{v}_8\}$	par
$\{\mathbf{v}_1, \mathbf{v}_3\}$	par	$\{\mathbf{v}_2, \mathbf{v}_4\}$	par	$\{\mathbf{v}_3, \mathbf{v}_6\}$	par	$\{\mathbf{v}_5, \mathbf{v}_6\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_4\}$	par	$\{\mathbf{v}_2, \mathbf{v}_5\}$	impar	$\{\mathbf{v}_3, \mathbf{v}_7\}$	par	$\{\mathbf{v}_5, \mathbf{v}_7\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_5\}$	impar	$\{\mathbf{v}_2, \mathbf{v}_6\}$	par	$\{\mathbf{v}_3, \mathbf{v}_8\}$	par	$\{\mathbf{v}_5, \mathbf{v}_8\}$	impar
$\{\mathbf{v}_1, \mathbf{v}_6\}$	par	$\{\mathbf{v}_2, \mathbf{v}_7\}$	par	$\{\mathbf{v}_4, \mathbf{v}_5\}$	impar	$\{\mathbf{v}_6, \mathbf{v}_7\}$	par
$\{\mathbf{v}_1, \mathbf{v}_7\}$	par	$\{\mathbf{v}_2, \mathbf{v}_8\}$	par	$\{\mathbf{v}_4, \mathbf{v}_6\}$	par	$\{\mathbf{v}_6, \mathbf{v}_8\}$	par
$\{\mathbf{v}_1, \mathbf{v}_8\}$	par	$\{\mathbf{v}_3, \mathbf{v}_4\}$	par	$\{\mathbf{v}_4, \mathbf{v}_7\}$	par	$\{\mathbf{v}_7, \mathbf{v}_8\}$	par

De la misma forma, si obtenemos la paridad de cada punto, se observa que el único punto impar es $\mathbf{v}_5$, luego el error se haya en la quinta posición. Por tanto, decodificamos la palabra recibida como 01101001.

4.4. Problemas Resueltos

Problema 4.1. Sabiendo que se está enviando información codificada en $\mathcal{RM}(1,5)$ mediante el orden estándar de $\mathbb{F}_2^5$, obtenido mediante la **Subrutina A.2**, decodificar 10011101010001101110010010001001 empleando el algoritmo de Reed sabiendo que no se han dado más de 7 errores.

Solución. Basta emplear el **Programa A.1**. En efecto, escribiendo la siguiente instrucción en *Mathematica* para $m = 5$

```
decodificarReed[{1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1,
1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1},
formordstandar[1, 5][[2]], variedades]
```

obtenemos la palabra 10010001111001100110011010011001. Como esta ha sido codificada mediante una matriz dada en forma estándar y nuestro código tiene dimensión 6 (ver **Problema 3.1**), la palabra original es 100100. □

Apéndice A

Programación

Para terminar, se incluyen subrutinas y programas diseñados en *Mathematica* útiles para llevar a cabo la codificación y decodificación en los códigos de Reed-Muller binarios.

Cabe resaltar que en este caso, por el funcionamiento interno del comando *Tuples*, nos conviene tomar de manera "dual" el orden canónico de $\mathbb{F}_2^m$. Esto es, dada la expansión binaria $i_0+2i_1+2^2i_2+\cdots+2^{m-2}i_{m-2}+2^{m-1}i_{m-1}$, con $i_0, i_1, ..., i_{m-2}, i_{m-1} \in \{0,1\}$, de un cierto entero i, asociaremos a $i+1$ el elemento $(i_{m-1}, i_{m-2}, ..., i_2, i_1, i_0) \in \mathbb{F}_2^m$, de manera que

$$\begin{array}{ccc} 1 & \longrightarrow & (0,0,...,0,0,0), \\ 2 & \longrightarrow & (0,0,...,0,0,1), \\ 3 & \longrightarrow & (0,0,...,0,1,0), \\ 4 & \longrightarrow & (0,0,...,0,1,1), \\ 5 & \longrightarrow & (0,0,...,1,0,0), \\ \vdots & \vdots & \vdots \\ 2^m-2 & \longrightarrow & (1,1,...,1,0,1), \\ 2^m-1 & \longrightarrow & (1,1,...,1,1,0), \\ 2^m & \longrightarrow & (1,1,...,1,1,1). \end{array}$$

Se puede probar que todas las propiedades estudiadas funcionan exactamente igual que con el orden que se estableció al comienzo de la Sección 3.2. Por tanto, sin pérdida de generalidad, consideraremos este como el orden canónico de $\mathbb{F}_2^m$ a la hora de diseñar los programas y las subrutinas.

Subrutina A.1. Función $matgeniter(r, m)$. Dados enteros r y m tales que $0 \leq r \leq m$, devuelve la matriz generadora de $\mathcal{RM}(r, m)$ calculada a través de la **Proposición 3.2.5**. Pese a que el orden canónico que se emplea no es el mismo que se estableció en la teoría, las matrices generadoras sí que coinciden.

```
matgeniter[r_, m_] := Module[{lista = {}, i, j},
```

```
For[i = 0, i <= m, i++, For[j = 0, j <= i, j++,
If[j == 0, lista = AppendTo[lista, Tuples[{1}, 2^i]],
If[i == j, lista = AppendTo[lista,
Join[lista[[-1]], Join[Tuples[{0}, 2^i - 1], {{1}}, 2]]];
lista = Delete[lista, 1], lista = AppendTo[lista,
Join[Join[lista[[2]], ConstantArray[
0, {Length[lista[[1]]], Length[lista[[2]][[1]]]}]],
Join[lista[[2]], lista[[1]]], 2]]; lista = Delete[lista, 1]]];
If[i == m && j == r, Return[lista[[-1]]]]]]]
```

Subrutina A.2. Función $formastandar(r, m)$. Dados enteros r y m tales que $0 \leq r \leq m$, devuelve, tanto la forma estándar de la matriz obtenida para estos mismos valores con la **Subrutina A.1**, siguiendo los pasos de la demostración dada para la **Proposición 4.2.1**, como el orden estándar correspondiente de $\mathbb{F}_2^m$ para el cual esta es matriz generadora de $\mathcal{RM}(r, m)$.

```
formordstandar[r_, m_] :=
Module[{G = matgencaniter[r, m], n, s, i = 1, j, k, H, aux, A,
lista}, n = Length[G[[1]]]; s = Length[G]; A = G;
lista = Tuples[{0, 1}, Log[2, n]];
While[i <= s, If[A[[i, i]] == 1, For[j = 1, j <= s, j++,
If[A[[j, i]] == 1 && i != j,
A[[j]] = Mod[A[[j]] - A[[i]], 2]]]; i++, H = Transpose[A];
For[k = i, k <= n , k++, If[A[[i, k]] == 1,
aux = H[[k]]; H[[k]] = H[[i]]; H[[i]] = aux;
aux = lista[[k]]; lista[[k]] = lista[[i]]; lista[[i]] = aux;
A = Transpose[H]; k = n + 1]]]; Return[{A, lista}]]
```

Subrutina A.3. Función $codificar(\mathbf{x}, r, m)$. Dados enteros r y m tales que $0 \leq r \leq m$, y la palabra binaria $\mathbf{x}$ a codificar mediante $\mathcal{RM}(r, m)$, de longitud $\dim(\mathcal{RM}(r, m)) = \sum_{k=0}^{r} \binom{m}{k}$, devuelve la codificación de $\mathbf{x}$ usando una matriz generadora dada en forma estándar de $\mathcal{RM}(r, m)$, tal y como se explica en la Sección 4.2.

```
codificar[x_, r_, m_] :=
Module[{G = formordstandar[r, m][[1]]}, Return[Dot[x, G]]]
```

Subrutina A.4. Función $pesopalabra(\mathbf{x})$. Dada la palabra $\mathbf{x}$, devuelve su peso.

```
pesopalabra[palabra_] := Module[{cont = 0, i,
longitud = Length[palabra]}, For[i = 0, i < longitud, i++;
If[palabra[[i]] != 0, cont++]]; Return[cont]]
```

Subrutina A.5. Función $palabrascodigo(G)$. Dada la matriz generadora G de un código lineal binario, devuelve las palabras de este.

```
palabrascodigo[G_] := Module[{C = {}, longitud, escalares, i,
palabra}, longitud = Length[G]; escalares = Tuples[{0, 1},
longitud]; For[i = 0, i < Length[escalares], i++;
palabra = Mod[Dot[escalares[[i]], G], 2];
C = Append[C, palabra]]; Return[C]]
```

Subrutina A.6. Función $decodificarlideres(\mathbf{x}, \mathcal{C})$. Dados un código lineal binario $\mathcal{C}$ de longitud m y una palabra binaria $\mathbf{x}$ a decodificar mediante $\mathcal{C}$, devuelve su decodificación, advirtiendo que esta no es única cuando corresponda, empleando el método de decodificación basado en líderes.

```
decodificarlideres[x_, C_] := Module[{minimo, pesoclase = {},
pesosord, decodificacion, comprobar = 0, longitud = Length[C],
i, clase = {}}, longitud = Length[C]; For[i = 1, i <= longitud,
i++, If[x == C[[i]], comprobar = 1; Break]]; If[comprobar == 1,
decodificacion = x, For[i = 1, i <= longitud, i++,
clase = AppendTo[clase, Mod[x + C[[i]], 2]];
pesoclase = AppendTo[pesoclase, pesopalabra[clase[[i]]]]];
pesosord = Sort[pesoclase]; minimo = pesosord[[1]];
For[i = 1, i <= longitud, i++, If[minimo == pesoclase[[i]],
decodificacion = Mod[x - clase[[i]], 2]; Break]];
If[minimo == pesosord[[2]],
Print["La decodificaci\'on no es \'unica"]]]; decodificacion]
```

Subrutina A.7. Función $matconstandar(r, m)$. Dados enteros r y m tales que $0 \leq r \leq m$, devuelve la matriz de control correspondiente al orden estándar de $\mathbb{F}_2^m$ para $\mathcal{RM}(r, m)$ obtenido empleando la **Subrutina A.2**. Esta se calcula mediante la propiedad marcada por (4.2).

```
matcontstandar[r_, m_] := Module[{G = matgenstandar[r, m], n, s,
H, B}, s = Length[G]; n = Length[G[[1]]]; B = Take[G, {1, s},
{s + 1, n}]; H = Join[Mod[-Transpose[B], 2],
IdentityMatrix[n - s], 2]; Return[H]]
```

Subrutina A.8. Función $decosinmatcon(H, \mathbf{x})$. Dadas una matriz de control H de un código lineal binario $\mathcal{C}$ de longitud m y la palabra binaria $\mathbf{x}$ a decodificar mediante $\mathcal{C}$, devuelve su decodificación, advirtiendo que esta no es única cuando corresponda, empleando el método de decodificación basado en síndromes.

```
decosinmatcon[H_, palabra_] := Module[{n = Length[palabra],
minimo, cont, min, k = Length[H], longitud, s, i, j, escalares,
sindromes, ciclo, matcero}, s = Mod[Dot[palabra, Transpose[H]]
, 2]; matcero = Table[0, {j, k}]; If[s == matcero,
Print["La palabra est\'a en el c\'odigo"]; palabra,
escalares = Tuples[{0, 1}, n]; sindromes = {};
```

```
ciclo = Length[escalares]; For[i = 1, i <= ciclo, i++,
If[Mod[Dot[escalares[[i]], Transpose[H]], 2] == s,
sindromes = AppendTo[sindromes, escalares[[i]]]]];
min = pesopalabra[sindromes[[1]]]; minimo = 1;
longitud = Length[sindromes]; For[i = 2, i <= longitud, i++,
If[pesopalabra[sindromes[[i]]] < min,
min = pesopalabra[sindromes[[i]]]; minimo = i]]; cont = 0;
For[i = 1, i <= longitud, i++,
If[min == pesopalabra[sindromes[[i]]], cont = cont + 1]];
If[cont >= 2, Print["La decodificaci\'on no es \'unica"]];
Mod[palabra - sindromes[[minimo]], 2]]]
```

Programa A.1. *Algoritmo de Reed.* Dado un orden para los vectores de $\mathbb{F}_2^m$, se trata de realizar un programa que devuelva la decodificación de una palabra binaria $\mathbf{x}$ mediante el algoritmo de Reed para el código $\mathcal{RM}(1, m)$, dado un valor m. Esta palabra tiene que tener a lo sumo $2^{m-2} - 1$ errores.

Para ello, son necesarias las 5 subrutinas siguientes:

- Función *palabrasociada*$(orden, S)$. Dados un orden para los vectores de $\mathbb{F}_2^m$ y una variedad afín S, devuelve la palabra asociada a S para el orden dado.

  ```
  palabrasociada[orden_, S_] :=
  Module[{n = Length[S], l = Length[orden], i, j, palabra = {},
  verificar = 0}, For[j = 1, j <= l, j++, For[i = 1, i <= n,
  i++, If[orden[[j]] == S[[i]], palabra = AppendTo[palabra, 1];
  i = n + 1; verificar = 1]];
  If[verificar == 0, palabra = AppendTo[palabra, 0],
  verificar = 0]]; Return[palabra]]
  ```

- Función *subvariedad*(S, T). Dadas dos variedades afines S y T, determina si S es una subvariedad afín para T.

  ```
  subvariedad[S_, T_] :=
  Module[{n = Length[S], s = Length[T], i, j, verificar = 0},
  For[i = 1, i <= n, i++, For[j = 1, j <= s, j++,
  If[S[[i]] == T[[j]], j = s + 1; verificar = 1]];
  If[verificar == 0, Return[False], verificar = 0]];
  Return[True]]
  ```

- Función *paridadbase*$(\mathbf{x}, orden, S)$. Dadas la palabra $\mathbf{x}$ a decodificar, un orden para los vectores de $\mathbb{F}_2^m$ y una variedad afín S, devuelve la paridad de S respecto de $\mathbf{x}$ para el orden dado, calculada en las condiciones de la **Proposición 4.3.1**.

```
paridadbase[x_, S_, orden_] :=
Module[{palabra = palabrasociada[orden, S], peso},
peso = pesopalabra[x*palabra];
If[Mod[peso, 2] == 0, Return["par"], Return["impar"]]]
```

- Función *casobase*($\mathbf{x}, orden, variedadesmaximas$). Dadas la palabra $\mathbf{x}$ a decodificar, un orden para los vectores de $\mathbb{F}_2^m$ y un conjunto de variedades afines, devuelve un listado con las paridades de todas las variedades afines del conjunto dado obtenidas mediante la subrutina anterior.

```
casobase[x_, orden_, variedadesmaximas_] :=
Module[{n, i, P = {}}, n = Length[variedadesmaximas];
For[i = 1, i <= n, i++,
P = AppendTo[P, {variedadesmaximas[[i]],
paridadbase[x, variedadesmaximas[[i]], orden]}]]; Return[P]]
```

- Función *casogeneral*($\mathbf{x}, orden, variedades, variedadesparidad$). Dadas la palabra $\mathbf{x}$ a decodificar, un orden para los vectores de $\mathbb{F}_2^m$ y dos conjuntos, uno con todos las variedades afines de $EG(m, 2)$ de una cierta dimensión, y otro con todas las variedades afines que tengan dimensión una unidad más con sus respectivas paridades respecto de $\mathbf{x}$ para el orden dado, devuelve las paridades del primero de estos conjuntos respecto de $\mathbf{x}$ para el orden dado calculadas mediante el **Criterio de la lógica mayoritaria** explicado en el **Teorema 4.3.4**.

```
casogeneral[x_, orden_, variedades_, variedadesparidad_] :=
Module[{n = Length[variedades], s = Length[variedadesparidad],
i, j, T, P = {}},
For[i = 1, i <= n, i++, T = {}; For[j = 1, j <= s, j++,
If[subvariedad[variedades[[i]], variedadesparidad[[j, 1]]],
T = AppendTo[T, variedadesparidad[[j, 2]]]]];
If[Count[T, "par"] > Count[T, "impar"],
P = AppendTo[P, {variedades[[i]], "par"}],
P = AppendTo[P, {variedades[[i]], "impar"}]]]; Return[P]]
```

Ahora, necesitamos determinar todos los planos y rectas afines de $EG(m, 2)$ (además de los puntos como variedades afines). Para ello, se definen las siguientes funciones que determinan, para ciertos parámetros, las correspondientes variedades afines.

```
puntos := Tuples[{0, 1}, m]

puntosvar[i_] := {Mod[puntos[[i]], 2]}
```

```
recta[i_, j_] := Union[Mod[Table[puntos[[i]]
+ l (puntos[[j]] - puntos[[i]]), {l, 0, 1}], 2]]

plano[i_, j_, h_] := Union[Flatten[Mod[Table[
puntos[[i]] + l (puntos[[j]] - puntos[[i]]) +
k (puntos[[h]] - puntos[[i]]), {k, 0, 1}, {l, 0, 1}], 2], 1]]
```

Así, podemos generar el siguiente conjunto que posee todos los planos, rectas y puntos (como 0-variedades) afines de $EG(m, 2)$, en dicho orden.

```
variedades ={Union[Select[Flatten[Table[
plano[i, j, h], {i, 2^m - 2}, {j, i + 1, 2^m - 1}, {h, i + 2,
2^m}], 2], Length[#] == 2^2 &]],
Union[Select[
Flatten[Table[recta[i, j], {i, 2^m - 1}, {j, i + 1, 2^m}], 1],
Length[#] == 2 &]], Union[
Select[Table[puntosvar[i], {i, 2^m}], Length[#] == 1 &]]};
```

Hecho todo esto, ya estamos en condiciones de dar la subrutina clave de este algoritmo, que llamaremos $decodificarReed(\mathbf{x}, orden, var)$. Esta, recibiendo la palabra $\mathbf{x}$ a decodificar, un orden para los vectores de $\mathbb{F}_2^m$ (que en general será el orden estándar de $\mathbb{F}_2^m$ obtenido mediante la **Subrutina A.2**) y un conjunto con todas las variedades necesarias para realizar la decodificación empleando el algoritmo de Reed (que es precisamente el conjunto de variedades que acabamos de construir), devuelve la decodificación de $\mathbf{x}$ a través del código de Reed-Muller $\mathcal{RM}(1, m)$ mediante el algoritmo de Reed.

```
decodificarReed[x_, orden_, var_] :=
Module[{n = Length[var], S = casobase[x, orden, var[[1]]],
s = 2, l = Length[x], i, y = {}, j},
While[s != n + 1, S = casogeneral[x, orden, var[[s]], S]; s++];
For[i = 1, i <= l, i++,
j = Position[Union[orden], orden[[i]]][[1, 1]];
If[S[[j, 2]] == "impar", y = AppendTo[y, Mod[x[[i]] + 1, 2]],
y = AppendTo[y, x[[i]]]]]; Return[y]]
```

Nota A.0.1. El **Programa A.1** puede generalizarse trivialmente a cualquier r si se definen las correspondientes funciones para determinar todas las variedades afines de $EG(m, 2)$ con dimensión superior a 2. Estas tendrían que incluirse, por delante, en el conjunto que hemos definido para que guarde todas las variedades afines según su dimensión.

Bibliografía

[1] J. Adámek. Foundations Of Coding. 1991. John Wiley & Sons, Inc. United States of America.

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann. Error-Correcting Linear Codes Classification by Isometry and Applications (**Volume 18 of Algorithms and Computation in Mathematics**). 2006. Springer-Verlag. Berlin.

[3] M. J. Iranzo, F. Pérez. LECCIONES de Elementos de Álgebra. Aplicaciones. Facultad de Matemáticas. Universidad de Valencia. Cursos 2000/2001-2008/2009.

(http://www.uv.es/iranzo/lecciones_de_codigos.pdf).

[4] T. Kasami, S. Lin, W. W. Peterson. New Generalizations of the Reed-Muller Codes Part I: Primitive Codes. IEEE Transactions on Information Theory. Volume 14, pages 189-199. 1968.

[5] D. E. Muller. Application of Boolean Algebra to Switching Circuit Design and to Error Detection. IEEE Transactions Comp. Volume 3, pages 6-12. 1954.

[6] C. Munera, J. Tena. Codificación de la Información. 1997. Universidad de Valladolid. Salamanca.

[7] M. Plotkin. Binary Codes With Specified Minimum Distances. IEEE Transactions on Information Theory. Volume 6, pages 445-450. 1960.

[8] R. A. Podestá. Introducción a la Teoría de Códigos Autocorrectores. CONICET y SecytUNC. 2006.

(http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat35−3.pdf).

[9] S. Raaphorst. Reed-Muller Codes. Carleton University. 2003.

[10] I. S. Reed. A Class of Multiple-Error Codes and Decoding Scheme. IEEE Transactions on Information Theory. Volume 4, pages 38-49. 1954.

[11] S. Roman. Coding and Information Theory. 1992. Springer-Verlag. Berlin.

[12] J. J. Simón. Apuntes de Códigos Correctores de Errores. Máster Universidad de Murcia. Curso 2011-2012.

(http://www.um.es/docencia/jsimon/depmat/2011−2012/Codigos/ApuntesCodigosMasterCompleto.pdf).

[13] E. J. Weldon. New Generalizations of the Reed-Muller Codes Part II: Nonprimitive Codes. IEEE Transactions on Information Theory. Volume 14, pages 199-205. 1968.