Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Códigos correctores óptimos mediante técnicas elementales

Autora: Cristina Martínez de Ilarduya Alcaide

Tutor: José Enrique Marcos Naveira

"Do not go where the path may lead, go instead where there is no path and leave a trail."

Ralph Waldo Emerson

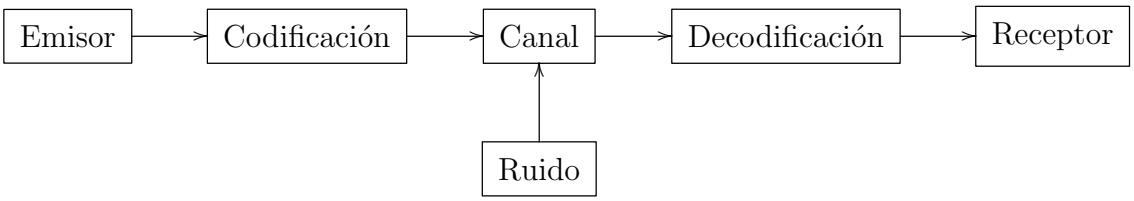
Agradecimientos:
Me gustaría mostrar mi más sincero agradecimiento a José Enrique,
mi tutor, por su implicación y su atención constante.

Índice general

Introducción

La teoría de los códigos correctores de errores tiene su origen en el artículo [Sha] de C.E. Shannon publicado en 1948. Los códigos correctores de errores se utilizan en la industria cuando se quiere enviar una información a través de un canal sujeto a ruido. Un código corrector añade información extra al mensaje que se quiere transmitir con el fin de recuperar la información enviada.

El siguiente diagrama proporciona una representación visual de un sistema de transmisión de información general:



Los denominados códigos en bloque transmiten la información en palabras de la misma longitud. Dentro de los códigos en bloque, los códigos lineales son los más estudiados debido a que su estructura permite utilizar las herramientas del álgebra lineal tanto para obtener resultados teóricos como para su manejo práctico.

El objetivo del presente Trabajo de Fin de Grado es el estudio de los códigos lineales sobre cuerpos finitos con el propósito de hallar técnicas elementales que nos permitan construir códigos óptimos, pues no hay un método explícito para construir una familia de estos códigos.

En el primer capítulo, de carácter introductorio, mostramos las nociones básicas de cuerpos finitos necesarias para cualquier curso de teoría de códigos. En un primer momento, nuestra intención fue profundizar más en estas ideas. Sin embargo, hemos acabado centrándonos en códigos sobre los cuerpos $\mathbb{F}_2$ y $\mathbb{F}_3$. No obstante, por su interés, hemos decidido no eliminar gran parte del contenido de este capítulo.

En el capítulo 2 exponemos los códigos lineales. Tratamos el concepto de matriz generadora, matriz de control y diferentes propiedades de los códigos. Además, se muestran diversas cotas de códigos y la decodificación general propia de códigos lineales.

En los siguientes tres capítulos se presentan los códigos lineales binarios, algunos de ellos óptimos, que hemos conseguido hallar con diferentes técnicas, tras multitud de ensayos fallidos. La mayoría de estos códigos me han sido sugeridos por mi tutor [Mar]. Hemos utilizado también otros métodos como, por ejemplo, el que sugiere [Til].

El interés principal de estos códigos es la cualidad de ser óptimos, si bien también hemos valorado los códigos con pocos pesos, dos o tres pesos no nulos, y la propiedad de autoortogonalidad. Asimismo, destaca el hecho de poder calcular a mano la distribución de pesos del código. Nos hemos limitado a longitudes de los códigos pequeñas, $n \leq 256$, para poder cotejarlos con las tablas de [Grassl] y así

saber si nos acercábamos a códigos óptimos. No obstante es obvio que técnicas tan elementales no tienen límite y fácilmente pueden proporcionar códigos análogos de parámetros mucho mayores.

Posteriormente, aplicando estas técnicas a códigos lineales ternarios, hemos obtenido resultados muy pobres. Para estos códigos ha sido necesario el uso de ordenador, nosotros hemos utilizado el software MAPLE. A pesar de ello, describimos otros procedimientos que resultan más interesantes, como el código simplex ternario y la construcción $(u+v+w \mid 2u+v \mid u)$. A continuación se expone cómo, a partir de este último método, se han construido los códigos Reed-Muller ternarios de la forma que dicta [KsPa].

Es posible que códigos similares con mayor longitud valgan para ser utilizados en técnicas criptográficas. Un ejemplo es el uso de códigos en el criptosistema McEliece.

Los códigos también tienen aplicación en combinatoria y teoría de grafos, así como en esquemas de compartición de secretos, protocolos seguros (multi-party computation) y autenticación, entre muchas otras.

Capítulo 1

Cuerpos finitos

Este capítulo está dedicado a la presentación de algunas de las ideas y resultados básicos de la teoría de cuerpos finitos que se utilizan en la teoría de códigos correctores de errores.

Las demostraciones de estos enunciados pueden encontrarse en [LiPi], capítulo 3 y en [MuTe], capítulos 5 y 9.

Sea p un número primo, q una potencia de un primo, es decir $q = p^n$. Se dan por conocidos los cuerpos finitos primos $\mathbb{F}_p = (\mathbb{Z}/(p), +, \cdot)$ y se sabe que existe un único cuerpo finito primo para cada primo p, salvo isomorfismos. Un cuerpo finito de q elementos se denota por $\mathbb{F}_q = GF(q)$.

Sea A un anillo o cuerpo de característica p, entonces para todo $a, b \in A$ y todo $n \in \mathbb{N}$ se cumple

$$(a+b)^p = a^p + b^p \qquad (a+b)^{p^n} = a^{p^n} + b^{p^n}$$

Teorema 1 *Sea K un cuerpo finito, entonces su característica es un primo p, el cuerpo tiene p^n elementos y es una extensión de grado n del cuerpo primo $\mathbb{F}_p$.*

Sea $P(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado $n \geq 2$, entonces $\mathbb{F}_p[X]/(P(X))$ es un cuerpo con p^n elementos.

Teorema 2 *Sea $q = p^n$. El cuerpo finito $\mathbb{F}_q$ es exactamente el conjunto de raíces del polinomio $X^q - X \in \mathbb{F}_p[X]$. En consecuencia, $\mathbb{F}_q$ es el cuerpo de descomposición de dicho polinomio sobre $\mathbb{F}_p$. Luego dos cuerpos con p^n elementos son isomorfos. Para cada potencia de un primo p^n existe un único cuerpo con p^n elementos, salvo isomorfismo.*

Teorema 3 *El cuerpo $GF(p^n)$ tiene exactamente un subcuerpo con p^d elementos para cada divisor $d|n$. No hay otros subcuerpos de $GF(p^n)$.*

Teorema 4 *Sea $q = p^n$ y el cuerpo $\mathbb{F}_q$. Su grupo aditivo es isomorfo a*

$$(\mathbb{F}_q, +) \cong (\overbrace{\mathbb{Z}/(p) \times \cdots \times \mathbb{Z}/(p)}^{n \text{ veces}}, +)$$

Su grupo multiplicativo $(\mathbb{F}_q \setminus \{0\}, \cdot)$ es cíclico de orden $p^n - 1$.

Luego, $\mathbb{F}_q$ tiene exactamente $\varphi(p^n - 1)$ elementos cuyo orden multiplicativo es $q - 1 = p^n - 1$. Considerando la correspondiente propiedad de los grupos cíclicos finitos, para cada $d \in \mathbb{N}$ que divide a $q - 1 = p^n - 1$, el cuerpo $\mathbb{F}_q$ tiene exactamente $\varphi(d)$ elementos de orden multiplicativo d. Además, todo elemento no nulo de $\mathbb{F}_q$ es una raíz de la unidad.

Un elemento de $\mathbb{F}_q$ cuyo orden multiplicativo es $q - 1$ se denomina elemento primitivo del cuerpo, o raíz primitiva.

Proposición 5 *Sea $q = p^n$, la extensión $\mathbb{F}_p \subseteq \mathbb{F}_q$ es simple.*

Lema 6 *Sea p primo, para cada $n \in \mathbb{N}$ existe algún $f(X) \in \mathbb{F}_p[X]$ polinomio irreducible de grado n.*

Lema 7 *Sea p primo, sea $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado n. Entonces $f(X)$ divide al polinomio $X^{p^n} - X$.*

Proposición 8 *Sea p primo, sea $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado d. Entonces $f(X)$ divide al polinomio $X^{p^n} - X$ si y solo si $d|n$.*

Proposición 9 *El polinomio $X^{p^n} - X$ es el producto de todos los polinomios mónicos irreducibles de $\mathbb{F}_p[X]$ cuyo grado divide a n.*

Sea K un cuerpo de característica p. La aplicación

$$\begin{aligned} \sigma : K &\to K \\ a &\mapsto a^p \end{aligned}$$

es un homomorfismo de cuerpos. La imagen de σ es un subcuerpo de K.

$$Im(\sigma) = \{a^p : a \in K\} = K^p \subseteq K$$

El homomorfismo σ es un automorfismo si y solo si $K^p = K$. Si lo es, se denomina automorfismo de Frobenius.

Lema 10 *Todo polinomio irreducible $P(X) \in \mathbb{F}_p[X]$ tiene derivada $P'(X) \neq 0$. Y por lo tanto, tiene todas sus raíces distintas y de multiplicidad uno, donde las tenga.*

Lema 11 *Sea $q = p^n$, la extensión de cuerpos $\mathbb{F}_p \subseteq \mathbb{F}_q$ es normal y separable, luego es una extensión de Galois.*

Teorema 12 *Sea $q = p^n$, el grupo de Galois de la extensión $\mathbb{F}_p \subseteq \mathbb{F}_q$ es cíclico de grado n, está generado por el automorfismo de Frobenius.*

Si $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ es el automorfismo de Frobenius, tenemos que

$$Gal(\mathbb{F}_q/\mathbb{F}_p) = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}.$$

Nótese que

$$\begin{aligned} \sigma^i : \mathbb{F}_q &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha^{p^i} \end{aligned}$$

Es claro que $\sigma^n = id$. Debido a que $\sigma^n(\alpha) = \alpha^{p^n} = \alpha$, ya que $\alpha \in \mathbb{F}_q = \mathbb{F}_{p^n}$.

Lema 13 *Sea $f(X) \in \mathbb{F}_p[X]$ un polinomio irreducible de grado n, entonces $f(X)$ tiene una raíz α en $\mathbb{F}_{p^n}$. Además, el conjunto de las raíces de $f(X)$ es*

$$\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}\} \subseteq \mathbb{F}_{p^n}$$

Luego $\mathbb{F}_{p^n}$ es el cuerpo de descomposición de $f(X)$.

Los elementos $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}} \subseteq \mathbb{F}_{p^n}$ se denominan los conjugados de α respecto $\mathbb{F}_p$.

Lema 14 *Sea $\alpha \in \mathbb{F}_q \setminus \{0\}$, sus conjugados respecto $\mathbb{F}_p$ tienen el mismo orden en el grupo $\mathbb{F}_q \setminus \{0\}$.*

Es decir, las raíces de un mismo polinomio irreducible $f(X) \in \mathbb{F}_p[X]$ tienen el mismo orden multiplicativo.

Sea el polinomio irreducible $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{F}_p[X]$ y sean $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}} \in \mathbb{F}_{p^n}$ sus raíces. Nótese que:

$Traza(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-2}} + \alpha^{p^{n-1}} = -a_{n-1} \in \mathbb{F}_p$

$Norma(\alpha) = \alpha \cdot \alpha^p \cdot \alpha^{p^2} \cdots \alpha^{p^{n-2}} \cdot \alpha^{p^{n-1}} = \alpha^{1+p+p^2+\cdots+p^{n-2}+p^{n-1}} = (-1)^n a_0 \in \mathbb{F}_p$

La última igualdad podría ser útil para calcular potencias de α^k, y una ayuda para determinar el orden multiplicativo de α.

Lema 15 *Dos polinomios irreducibles del mismo grado en $\mathbb{F}_p[X]$ tienen cuerpos de descomposición isomorfos.*

Teorema 16 (Teorema de Wedderburn) *Todo cuerpo finito es conmutativo.*

Proposición 17 *Sea p un primo impar. La mitad de los elementos de $\mathbb{F}_{p^n} \setminus \{0\}$ son cuadrados, y la otra mitad no son cuadrados.*
Todos los elementos de $\mathbb{F}_{2^n}$ son cuadrados.

Veamos algunos resultados relativos a polinomios irreducibles sobre el cuerpo $\mathbb{F}_p$.

Lema 18 *Sea $P(X) \in \mathbb{F}_p[X]$ un polinomio mónico de grado dos o tres, entonces $P(X)$ es irreducible si y solo si no tiene raíces en $\mathbb{F}_p$.*
Ningún polinomio irreducible de $\mathbb{F}_p[X]$ de grado mayor o igual que dos tiene raíces.

Teorema 19 *El polinomio $X^p - X - a \in \mathbb{F}_p[X]$ es irreducible si y solo si $a \neq 0$ en $\mathbb{F}_p$.*

Proposición 20 *Sea p primo y t otro primo tal que $t \mid (p-1)$ y $t^2 \nmid (p-1)$. Sea $a \in \mathbb{F}_p$ un elemento cuyo orden multiplicativo es t. Entonces el polinomio $X^t - a \in \mathbb{F}_p[X]$ es irreducible.*

Seguidamente daremos la definición de orden multiplicativo.

Definición 21 *Sea un polinomio irreducible $f(X) \in \mathbb{F}_p[X]$ de grado n, $f(X) \neq X$. Su orden se define como el orden de cualquier raíz suya en $\mathbb{F}_{p^n}$.*

Hemos visto en el Lema 14 que todas las raíces de un mismo polinomio irreducible tienen el mismo orden multiplicativo.

Lema 22 *Sea un polinomio irreducible $f(X) \in \mathbb{F}_p[X]$ de grado n, $f(X) \neq X$. Su orden es un divisor de $p^n - 1$. Ese orden es el menor natural d tal que $f(X)$ divide a $X^d - 1$.*

Definición 23 *Sea un polinomio irreducible $f(X) \in \mathbb{F}_p[X]$ de grado n, $f(X) \neq X$. Se denomina polinomio primitivo si su orden es $p^n - 1$. En este caso cualquier raíz suya genera el grupo $\mathbb{F}_{p^n} \setminus \{0\}$.*

Sea $\alpha \in GF(p^n)$ un elemento de orden $p^n - 1$, que también se llama elemento primitivo ó raíz primitiva de $GF(p^n)$. Sea su polinomio mínimo irreducible $Irre(\alpha, \mathbb{F}_p) \in \mathbb{F}_p[X]$. Obviamente este polinomio es primitivo.

Un cuerpo finito $GF(p^n)$ tiene $\varphi(p^n - 1)$ elementos de orden $p^n - 1$, es decir, elementos primitivos. Cada polinomio primitivo de grado n tiene n raíces distintas, que son elementos primitivos. En consecuencia, en $\mathbb{F}_p[X]$ hay exactamente $\dfrac{\varphi(p^n - 1)}{n}$ polinomios primitivos mónicos de grado n.

Se denomina polinomio ciclotómico de orden n, y se denota por Φ_n, al polinomio mónico cuyas raíces son todas las raíces primitivas de orden n de la unidad.

Sea $\Phi_n(X) \in \mathbb{Z}[X]$ el polinomio ciclotómico n-ésimo. Recordemos que, para cada $n \in \mathbb{N}$, este es un polinomio irreducible en $\mathbb{Z}[X]$. Por el contrario, considerando $\Phi_n(X) \in \mathbb{F}_p[X]$, es irreducible en solo algunos casos. Recordemos:

$$X^m - 1 = \prod_{n|m} \Phi_n(X); \qquad deg(\Phi_n(X)) = \varphi(n)$$

Teorema 24 *Asumimos que $p \nmid n$. Sea el polinomio ciclotómico $\Phi_n(X)$. Sea d el menor natural que cumple $p^d \equiv 1\, mod\,(n)$. Entonces el polinomio $\Phi_n(X)$ factoriza en el producto de $\varphi(n)/d$ polinomios mónicos irreducibles distintos, cada uno de ellos de grado d.*

Corolario 25 *Asumimos que $p \nmid n$. El polinomio ciclotómico $\Phi_n(X)$ es irreducible en $\mathbb{F}_p[X]$ si y solo si el menor natural d que cumple $p^d \equiv 1\, mod\,(n)$ es justamente $d = \varphi(n)$.*

Recordemos la **congruencia de Euler**:

Si $a, m \in \mathbb{N} \setminus \{0, 1\}$ y $mcd(a, m) = 1$, entonces

$$a^{\varphi(m)} \equiv 1\, mod\,(m)$$

Además, el menor $d \in \mathbb{N}$ que satisface $a^d \equiv 1\, mod\,(m)$ debe ser un divisor de $\varphi(m)$, es decir, $d \mid \varphi(m)$.

Capítulo 2

Códigos lineales en bloque

Este capítulo proporciona los conceptos fundamentales de códigos lineales en bloque.

Los códigos usados para detección y corrección de errores son típicamente códigos en bloque. Los códigos en bloque transmiten la información en palabras de la misma longitud. La idea principal en que se basan es la introducción de información redundante que, una vez recibido el mensaje, puede utilizarse para detectar y eventualmente recuperar la parte corrompida durante la transmisión.

Definición 26 *Un código $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$.*

Sus elementos se denominan palabras y $\mathbb{F}_q$ alfabeto del código. Estas palabras son los únicos elementos de $\mathbb{F}_q^n$ que transmite el emisor. Si el receptor recibe una palabra de longitud n que está en $\mathbb{F}_q^n$ pero no en $\mathcal{C}$, sabe que se ha producido algún error en la transmisión y, mediante el método de decodificación y corrección de errores, determinará cuál era la palabra de $\mathcal{C}$ que se le transmitió.

Para la medida del error cometido en la transmisión de una palabra del código $\mathcal{C} \subseteq \mathbb{F}_q^n$ y de lo próxima que se encuentra una palabra de otra disponemos de la siguiente idea sencilla de R.W.Hamming.

Definición 27 (Distancia de Hamming) *Dados dos elementos $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, se define la distancia de Hamming entre x e y como el número de coordenadas en que difieren, es decir,*

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

Esta es efectivamente una distancia en $\mathbb{F}_q^n$, pues cumple las propiedades correspondientes.

Dada esta definición, llamaremos **distancia mínima** de un código $\mathcal{C} \subseteq \mathbb{F}_q^n$ a

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

El proceso de decodificación y corrección de errores aplicado por el receptor es el siguiente: recibida $y \in \mathbb{F}_q^n$, el receptor verifica si $y \in \mathcal{C}$; en cuyo caso se interpreta que la palabra ha sido transmitida correctamente. Si $y \notin \mathcal{C}$, se han producido errores en la transmisión. Entonces y se decodifica aplicando el *principio de distancia mínima*, se halla la palabra-código $z \in \mathcal{C}$ tal que la distancia entre y y z sea mínima y se considera que z es la palabra que transmitió el emisor. Este algoritmo falla si hay más de una palabra-código que satisfaga esa distancia mínima. En cualquier otro caso proporciona una, no necesariamente correcta, decodificación de y.

Como veremos en la proposición siguiente, el parámetro que permite medir exactamente la capacidad de corrección de errores de un código es la distancia mínima.

Proposición 28 *Sea $\mathcal{C}$ un código en bloque de longitud n y distancia mínima d sobre $\mathbb{F}_q$, el proceso anterior, aplicado a una n-upla recibida, permite*

(I) *detectar cualquier configuración de t errores si $t < d$.*

(II) *corregir cualquier configuración de t errores si $2t < d$.*

(III) *corregir cualquier configuración de s borrones si $s < d$.*

(IV) *corregir cualquier configuración de t errores y s borrones si $2t + s < d$.*

Demostración: Sea $c \in \mathcal{C}$ la palabra enviada e y el mensaje recibido.

(I) Si y contiene $t < d$ errores y $t > 0$, entonces $y \notin \mathcal{C}$ ya que cualquier palabra de $\mathcal{C}$ está a distancia al menos d de c. Por tanto, basta evaluar la condición $y \in \mathcal{C}$ para detectar si han ocurrido errores.

Para probar las restantes afirmaciones, recordemos que el algoritmo anterior decodifica correctamente y cuando c es la única palabra de $\mathcal{C}$ más próxima a y.

(II) Si y contiene t errores y $2t < d$, entonces $d(y, c) < d(y, x)$ para todo $x \in \mathcal{C}$. En efecto, por definición de distancia mínima, las bolas con centro en las palabras-código y radio $(d-1)/2$, siempre para la métrica de Hamming, son disjuntas. Por tanto, si $2t < d$, entonces y estará en una y solo una de tales bolas, que tendrá por centro la palabra-código más cercana, ya que en otro caso existiría $x \in \mathcal{C}$, $x \neq c$ tal que $d(y, x) \leq d(y, c) \leq (d-1)/2$, con lo que, al ser d una distancia, $d(c, x) \leq d-1$, lo que contradice la definición de d.

(III) Si y contiene s borrones, $s < d$, podemos suponer, salvo reordenación y para simplificar la notación, que están en las posiciones $y_1, \ldots, y_s$. Entonces c es el único elemento de $\mathcal{C}$ que coincide con y en las últimas $n - s$ posiciones. En efecto, si $x \in \mathcal{C}$ también coincide con y en las últimas $n - s$ posiciones, entonces $d(c, x) \leq s < d$, luego $c = x$.

(IV) Si y contiene t errores y s borrones, $2t + s < d$, como en el apartado anterior, podemos suponer que los borrones están en las posiciones $y_1, \ldots, y_s$. Sea $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-s}$ la proyección en las últimas $n - s$ coordenadas. Entonces $d(\pi(y), \pi(c)) < d(\pi(y), \pi(x))$ para todo $x \in \mathcal{C}$. En efecto, en otro caso existiría $x \in \mathcal{C}$, $x \neq c$ tal que $d(\pi(y), \pi(x)) \leq d(\pi(y), \pi(c)) \leq (d - s - 1)/2$, con lo que al ser d una distancia, $d(c, x) \leq d - 1$, en contradicción con la definición de d. Como en el caso (III), $\pi(c)$ determina unívocamente c ya que $s < d$. □

Como consecuencia de la Proposición 28, un código $\mathcal{C}$ con distancia mínima d corrige $t = \left\lfloor \dfrac{d-1}{2} \right\rfloor$ errores.

Interesa, por tanto, que la distancia mínima del código sea la mayor posible, condicionada por otros parámetros.

Definición 29 *Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$.*

Todo código lineal $\mathcal{C}$ de longitud n es también un código en bloque de longitud n. Además, como espacio vectorial, $\mathcal{C}$ posee dimensión k, luego el número de palabras-código es q^k. Llamaremos d a su distancia mínima. Un código lineal con estos parámetros se denota por $[n, k, d]_q$.

A continuación se presentan algunas definiciones que otorgan información sobre las propiedades de un $[n, k, d]_q$-código lineal $\mathcal{C}$.

- La **redundancia** del código es $r = n - k$.
- Su **tasa de transmisión de información** es $R(\mathcal{C}) = k/n$.

- Dado un elemento del código, $x \in \mathcal{C}$, se define su **peso** $w(x)$ como el número de coordenadas no nulas de x y se define el **peso mínimo** del código $w(\mathcal{C})$ como el mínimo de los pesos de sus elementos excluido el vector 0_n.

Teorema 30 *En un código lineal, el peso mínimo es igual a la distancia mínima.*

Demostración: Sea w el peso mínimo y sea d la distancia mínima del código. Se toma v vector del código de peso mínimo. El peso de v es igual a la distancia de Hamming de v con el vector 0. Luego $w = peso(v) = d(v, 0) \geq d$.

Por otro lado, se toman u, z vectores del código tal que cumplan que la distancia de Hamming entre ellos es la mínima. La distancia entre ellos es igual al peso de su resta. Entonces $d = d(u, z) = w(u - z) \geq w$. Como se quería demostrar, $w = d$. □

Todo subespacio de $\mathbb{F}_q^n$ de dimensión k puede ser interpretado como imagen de una (no única) aplicación lineal inyectiva $f : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$. Podemos entender que esta f es la aplicación de codificación y, por tanto, que $\mathbb{F}_q^k$ es la fuente de información que estamos codificando con $\mathcal{C}$. Esta interpretación motiva la siguiente definición.

Definición 31 *Llamaremos matriz generadora G del código $\mathcal{C}$ a la matriz de una aplicación lineal inyectiva $f : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subseteq \mathbb{F}_q^n$, es decir, a una matriz de orden $k \times n$ cuyas filas son una base de $\mathcal{C}$.*

El rango de G es k y un mismo código tiene varias matrices generadoras así como no es única la base de $\mathcal{C}$ como subespacio vectorial de $\mathbb{F}_q^n$.

Una matriz generadora G proporciona un código y una codificación. En efecto,

$$\mathcal{C} = \{vG : v \in \mathbb{F}_q^k\}$$

La forma de codificar un mensaje original v, que identificamos con un elemento de $\mathbb{F}_q^k$, es realizar el producto $vG = w$. Obtenemos un mensaje codificado $w \in \mathcal{C} \subseteq \mathbb{F}_q^n$, con la correspondiente redundancia de información, que permitirá corregir posibles errores.

Así, la codificación para códigos lineales es simple y requiere el almacenamiento en memoria de una matriz G, es decir, de nk elementos de $\mathbb{F}_q$ y no de nq^k, como sería el caso de un código en bloque no lineal con el mismo cardinal.

Un subespacio vectorial de $\mathbb{F}_q^n$ puede describirse no solo mediante un sistema de generadores, lo que da lugar al concepto anterior de matriz generadora, sino también mediante unas ecuaciones implícitas. Esta forma de caracterización origina la siguiente definición.

Definición 32 *Diremos que una matriz H es una matriz de control del código $\mathcal{C}$ si para todo vector $x \in \mathbb{F}_q^n$, se verifica que $x \in \mathcal{C}$ si y solo si $Hx^t = 0$.*

Es decir,

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : Hx^t = 0\}$$

La matriz H está definida sobre $\mathbb{F}_q$, tiene orden $(n - k) \times n$ y rango $n - k$. Al igual que ocurre con la matriz generadora, no existe una única matriz de control de un código.

La relación entre las matrices generadora y de control de un código es la dada en la siguiente proposición, cuya demostración es inmediata.

Proposición 33 *Si G y H son las matrices generadora y de control de un código $\mathcal{C}$, entonces se cumple que $GH^t = 0$.*

Precisamos lo que se entiende por códigos equivalentes y código sistemático.

Dos códigos lineales $\mathcal{C}_1, \mathcal{C}_2$ son **equivalentes** si se puede obtener uno del otro realizando las operaciones siguientes:

- Existe una permutación σ del conjunto $\{1, 2, \ldots, n\}$ tal que

$$\mathcal{C}_2 = \left\{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) : (x_1, x_2, \ldots, x_n) \in \mathcal{C}_1\right\}$$

- Multiplicando la componente en una posición fija de todos los elementos de $\mathcal{C}_1$ por una constante no nula de $\mathbb{F}_q$.

Dos códigos equivalentes tienen los mismos parámetros, $[n, k, d]_q$.

Un $[n, k, d]_q$-código $\mathcal{C}$ se denomina **sistemático** si una de sus matrices generadoras es de la forma $G = [I_k, A]$, donde I_k es la matriz identidad de orden k y A es una matriz de orden $k \times (n - k)$. Si esto ocurre, decimos que la matriz generadora está en la forma estándar.

En este caso, la operación de codificación de un mensaje original proporciona un mensaje donde las k primeras coordenadas del vector codificado es el propio mensaje original y las $(n - k)$ restantes coordenadas son los llamados símbolos de control.

Si la matriz generadora $G = [I_k, A]$ está en la forma estándar, entonces la matriz $H = [-A^t, I_{n-k}]$ es una matriz de control del código. En este caso decimos que la matriz de control está en la forma estándar.

Proposición 34 *Todo código lineal es equivalente a uno sistemático.*

Demostración: Sea el código $\mathcal{C}$ de parámetros $[n, k, d]$ sobre $\mathbb{F}_q$. La dimensión de $\mathcal{C}$ es k, entonces una matriz generadora G de $\mathcal{C}$ tiene orden $k \times n$ y rango k, luego posee k columnas linealmente independientes. Mediante una permutación σ del conjunto $\{1, 2, \ldots, n\}$ podemos conseguir que estas columnas sean las k primeras. Así, se obtiene una matriz $G' = [A, B]$ con A regular, de tamaño $k \times k$. Ahora, mediante una sucesión de operaciones elementales (método de Gauss) puede transformarse A en la matriz identidad I_k. Si estas operaciones se realizan en la matriz G', obtenemos una matriz en forma estándar cuyas filas generan el mismo espacio que las de G' y que es, por tanto, un código sistemático equivalente al que tiene a G por matriz generadora. □

El siguiente resultado permite calcular la distancia mínima a partir de la matriz de control del código, en lugar de calcular el peso de todas sus palabras.

Teorema 35 *Sea un código lineal con matriz de control H. La distancia mínima d del código es el valor que cumple lo siguiente:*
Todo subconjunto de $d - 1$ columnas de H es linealmente independiente;
existe un subconjunto de d columnas linealmente dependientes.

Demostración: Sea d la distancia mínima y a su vez el peso mínimo del código. Sea H la matriz de control con columnas $u_1, \ldots, u_n$. Si se toma un vector $v = (a_1, \ldots, a_n)$ no nulo de peso menor que el peso mínimo del código d, v no está en el código. Entonces, $0 \neq Hv^t = a_1u_1 + \cdots + a_nu_n$, es decir, cada $d - 1$ columnas de H son linealmente independientes.

Ahora, si se toma un vector x, que pertenezca al código, de peso exactamente el peso mínimo d, sabemos que $0 = Hx^t$, luego en H hay d columnas linealmente independientes. □

Sabemos que todo subespacio vectorial es un subgrupo. Es curioso el hecho de que sobre los cuerpos finitos primos $\mathbb{F}_p$ se satisface la implicación recíproca.

Proposición 36 *Sea p primo. Sea $\mathbb{F}_p^n$ considerado espacio vectorial sobre $\mathbb{F}_p$. Sea V un subgrupo de $\mathbb{F}_p^n$, entonces V es un subespacio vectorial de $\mathbb{F}_p^n$.*

Definimos ahora lo que se entiende por código óptimo.

Definición 37 *Un código lineal de parámetros $[n,k,d]_q$ se dice óptimo si no existe ningún otro código con parámetros $[n,k,d_2]_q$ tal que $d_2 > d$.*

Hay otros dos conceptos de código óptimo referidos a los parámetros n y k. Para la longitud n tenemos el siguiente:

Definición 38 *Un código lineal de parámetros $[n,k,d]_q$ se dice óptimo si no existe ningún otro código con parámetros $[n_2,k,d]_q$ tal que $n_2 < n$.*

2.1. Códigos divisibles

Seguidamente señalaremos una serie de propiedades que serán útiles más adelante.

Una de las características de algunos de los códigos que hemos construido en capítulos posteriores es que los pesos de todas las palabras-código son divisibles entre un número entero. Examinando [HuPl], hemos reparado en el interés de esta característica, pues está relacionada con la propiedad de autoortogonalidad. A continuación se dan las nociones de código divisible, código dual, código autodual y código autoortogonal y los teoremas que las relacionan.

Decimos que un código $\mathcal{C}$ es *divisible* si todas las palabras-código tienen peso divisible por un entero $\triangle > 1$. Se dice que el código es divisible por $\triangle$; $\triangle$ es un divisor de $\mathcal{C}$ y el divisor de $\mathcal{C}$ será el mayor de los divisores.

Sea $\mathcal{C}$ un código lineal y sea H una matriz de control de $\mathcal{C}$. Podemos considerar H como la matriz generadora de otro código sobre $\mathbb{F}_q$. Este código es el denominado **código dual** de $\mathcal{C}$, y se denota por $\mathcal{C}^\perp$.

De hecho, $\mathcal{C}^\perp$ es el código que consiste en el subespacio ortogonal de $\mathcal{C}$ respecto de la forma bilineal simétrica $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ dada por $B(x,y) = \sum_{i=1}^n x_i y_i$. Como dicha forma es no degenerada, se tiene que $\mathcal{C}^\perp$ tiene dimensión $n-k$ si $\mathcal{C}$ tiene dimensión k. Además, si G es una matriz generadora de $\mathcal{C}$, la igualdad $GH^t = 0$ implica que G es una matriz de control de $\mathcal{C}^\perp$.

Un código $\mathcal{C}$ es **autoortogonal** si $\mathcal{C} \subseteq \mathcal{C}^\perp$.

Un código $\mathcal{C}$ es **autodual** si $\mathcal{C} = \mathcal{C}^\perp$.

En el siguiente teorema, veremos algunos resultados elementales sobre el peso de palabras-código cuando trabajamos con códigos sobre $\mathbb{F}_2$, que resultarán útiles más adelante.

Teorema 39 *Se cumple lo siguiente:*

(I) *Si $x, y \in \mathbb{F}_2^n$, entonces $w(x+y) = w(x) + w(y) - 2 \cdot w(x \cap y)$, donde $x \cap y$ es el vector de $\mathbb{F}_2^n$, que tiene unos exactamente en aquellas posiciones donde ambos x, y tengan unos.*

(II) *Si $x, y \in \mathbb{F}_2^n$, entonces $w(x \cap y) \equiv x \cdot y$ (mod 2).*

(III) *Si $x \in \mathbb{F}_2^n$, entonces $w(x) \equiv x \cdot x$ (mod 2).*

Veamos, pues, la relación entre los códigos lineales binarios divisibles entre cuatro y los códigos autoortogonales.

Teorema 40 *Sea $\mathcal{C}$ un código lineal binario.*

(I) *Si $\mathcal{C}$ es autoortogonal y cada fila de una matriz generadora suya tiene peso divisible entre cuatro, entonces todas las palabras del código $\mathcal{C}$ tienen peso divisible entre cuatro.*

(II) *Si todas las palabras del código $\mathcal{C}$ tienen peso divisible entre cuatro, entonces $\mathcal{C}$ es autoortogonal.*

Demostración: Para (I), sean x, y filas de la matriz generadora. Por el Teorema 39, $w(x+y) = w(x) + w(y) - 2 \cdot w(x \cap y) \equiv 0 + 0 - 2 \cdot w(x \cap y) \equiv 0 \pmod 4$. Ahora procedemos por inducción sabiendo que cada palabra-código es la suma de ciertas filas de la matriz generadora.

Para (II), sean $x, y \in \mathcal{C}$. De nuevo por el Teorema 39, $2(x \cdot y) \equiv 2 \cdot w(x \cap y) \equiv 2 \cdot w(x \cap y) - w(x) - w(y) \equiv -w(x+y) \equiv 0 \pmod 4$. Luego $x \cdot y \equiv 0 \pmod 2$. □

Es natural preguntarse si el Teorema 40 puede generalizarse a códigos cuyas palabras-código tienen pesos divisibles entre otros números aparte del cuatro. El Teorema 40 afirma que los códigos binarios divisibles entre cuatro son autoortogonales. Esto no es cierto si consideramos códigos binarios divisibles entre dos.

2.2. Cotas de códigos lineales

A continuación se describen las cotas de códigos lineales más comunes.

Teorema 41 (Cota de Hamming) *Sea $\mathcal{C}$ un código lineal q-ario de longitud n que corrige t errores, entonces se cumple*

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t \leq q^{n-k} \tag{2.1}$$

Demostración: Como $\mathcal{C}$ corrige t errores, las bolas de radio t centradas en las palabras del código $\mathcal{C}$ son disjuntas. El cardinal de una bola de radio t es

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t$$

Tenemos q^k bolas disjuntas, cada una del cardinal anterior, todas ellas contenidas en $\mathbb{F}_q^n$, que tiene cardinal q^n, con lo que la desigualdad (2.1) queda probada. □

Se dice que un código es perfecto si en la desigualdad (2.1) se da la igualdad.

Teorema 42 (Cota de Singleton) *Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un $[n,k,d]_q$ código lineal, entonces*

$$k + d \leq n + 1 \tag{2.2}$$

Demostración: Para toda palabra $(x_1, \ldots, x_n)$ del código, suprimimos las $d-1$ últimas coordenadas. Obtenemos palabras $(x_1, \ldots, x_{n-d+1})$ que son todas distintas. Luego $q^k \leq q^{n-d+1}$ y queda probada la desigualdad (2.2). □

Se dice que un código es de Máxima Distancia de Separación (MDS) si se da la igualdad en (2.2).

Seguidamente, daremos la noción de código residual, que nos permite obtener otra cota para códigos lineales.

Proposición 43 *Sea $\mathcal{C}$ un código lineal con parámetros $[n, k, d]$ sobre $\mathbb{F}_q$, entonces existe un código de parámetros $[n-d, k-1, \lceil d/q \rceil]$ sobre $\mathbb{F}_q$. Se denomina código residual.*

Demostración: Sea $c \in \mathcal{C}$ una palabra-código de peso exactamente d y sea G una matriz generadora del código en la que la palabra c sea la primera fila.

Permutando las columnas de G y multiplicándolas por constantes no nulas, de forma que las d coordenadas no nulas de c sean exactamente las d primeras y sean todas unos, se obtiene un código equivalente a $\mathcal{C}$ que llamaremos $\mathcal{C}$ asimismo.

La nueva matriz generadora de $\mathcal{C}$ de orden $k \times n$ y rango k tiene la forma siguiente. En la primera fila se encuentra el vector c es decir, hay d unos y $(n-d)$ ceros.

$$B = \left[\begin{array}{ccccccc|ccccc} 1 & 1 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline & & & & & & & & & & \\ & & & & & & & G_2 & & & \\ & & & & & & & & & & \end{array}\right]$$

La submatriz G_2 es de orden $(k-1) \times (n-d)$. El rango de G_2 es $(k-1)$, puesto que, si no fuese así y el rango fuese menor que $(k-1)$, con transformaciones elementales de las filas de G_2 (y de B), podríamos lograr que la primera fila de G_2 fuese toda de ceros. Fijándonos en la matriz grande B y haciendo una combinación lineal de esta segunda fila y también de su primera fila, conseguiríamos una palabra-código de $\mathcal{C}$ no nula de peso menor que d, en contra de la hipótesis.

Ahora, sea $\mathcal{C}_2$ el código lineal sobre $\mathbb{F}_q$ cuya matriz generadora es G_2, sabemos que tiene parámetros $[n-d, k-1, d_2]_q$.

Veamos cual es el peso mínimo del código.

Sea $x \in \mathcal{C}$ no nula combinación lineal de las $k-1$ últimas filas de B, de forma que la correspondiente combinación lineal de las $k-1$ filas de G_2 tenga peso w. Sea δ_i el número de coordenadas en la primera sección de x que tiene valor i para cada $i \in \mathbb{F}_q$. La palabra código $x - ic \in \mathcal{C}$ y tiene peso $w + d - \delta_i$ y, como este peso debe ser mayor o igual que d concluimos que $w \geq \delta_i$ para cada $i \in \mathbb{F}_q$. Nótese que $\sum_{i=1}^{q} \delta_i = d$. Por lo cual, algún $\delta_i \geq d/q$ luego $w \geq d/q$. Como todos los valores son enteros, tenemos que $w \geq \lceil d/q \rceil$, es decir, $d_2 \geq \lceil d/q \rceil$. □

Aplicando la Proposición 43 reiteradamente mientras se pueda, se obtiene el siguiente resultado.

Teorema 44 (Cota de Griesmer) *Sea $\mathcal{C}$ un $[n, k, d]$-código lineal sobre $\mathbb{F}_q$, entonces*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \tag{2.3}$$

Los códigos que alcanzan la cota de Griesmer (2.3) con igualdad tienen la propiedad de ser óptimos.

2.3. Decodificación de códigos lineales

En esta sección se expone un método general de decodificación de códigos lineales.

Sea $\mathcal{C}$ un código lineal de parámetros $[n, k, d]$ sobre $\mathbb{F}_q$. Como sabemos $\mathcal{C}$ corrige $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errores.

Si se envía una palabra-código $c \in \mathcal{C}$ y se recibe $y \in \mathbb{F}_q^n$, el error cometido durante la transmisión ha sido $e = y - c$. La estrategia que seguiremos para decodificar y es la siguiente: calculamos la distancia de y a todas las palabras de $\mathcal{C}$ y la decodificamos por la más próxima, si existe. Si durante la transmisión se han cometido a lo más t errores, es decir, $w(e) \leq t$, entonces $d(c, y) = w(e) \leq t$ y c es la única palabra del código con tal propiedad; la decodificación es, por tanto, correcta. Si $t < w(e) < d$, podemos detectar que se han producido errores, puesto que $y \notin \mathcal{C}$, pero no corregirlos en general. Si $w(e) \geq d$ la decodificación fallará eventualmente.

La mayor información acerca del error cometido la da el llamado *síndrome*. Supongamos, como antes, que se ha enviado c y recibido $y = c + e$. Sea H una matriz de control del código $\mathcal{C}$.

Definición 45 *Se denomina síndrome de y al vector*

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

Se verifica

$$y \in \mathcal{C} \text{ si y solo si } s(y) = 0$$

en cuyo caso la palabra y se supone transmitida correctamente. Como el síndrome es una aplicación lineal, se cumple

$$s(y) = s(c + e) = s(c) + s(e) = s(e)$$

y, por lo tanto, conocemos el síndrome del error cometido.

Proposición 46 *El síndrome del vector recibido $s(y)$ es una combinación lineal de las columnas de la matriz H correspondientes a las posiciones en las que se han producido los errores.*

Consideremos en $\mathbb{F}_q^n$ la relación de equivalencia

$$u \sim v \text{ si y solo si } u - v \in \mathcal{C}$$

El espacio vectorial cociente obtenido, módulo dicha relación, se denota por $\mathbb{F}_q^n/\mathcal{C}$. Los elementos de $\mathbb{F}_q^n/\mathcal{C}$ son clases de equivalencia

$$u + \mathcal{C} = \Big\{ u + x : x \in \mathcal{C} \Big\}$$

Como cada clase posee $\#\mathcal{C} = q^k$ elementos (ó representantes), el cardinal de $\mathbb{F}_q^n/\mathcal{C}$ es q^{n-k} y su dimensión es $n - k$.

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

Definición 47 *Si en una clase de equivalencia existe un único elemento de peso mínimo, este elemento se denomina el líder de la clase.*

En general, no toda clase tendrá líder, ya que el elemento de peso mínimo no será, en general, único. Sin embargo, si una clase contiene un elemento de peso $\leq t$, este es el líder de la clase, como asegura la siguiente proposición.

Proposición 48 *Cada clase de $\mathbb{F}_q^n/\mathcal{C}$ posee a lo sumo un elemento de peso $\leq t$.*

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

Recibido un vector y, decodificar y significa encontrar la palabra de $\mathcal{C}$ más próxima a y, y la decodificación será posible si y solo si esta palabra existe, es decir, si es única. Como todos los vectores $y - x$, $x \in \mathcal{C}$, están en la misma clase de equivalencia de $\mathbb{F}_q^n/\mathcal{C}$, que es la clase de y, el mínimo de $d(y, x) = w(y - x)$ se obtiene cuando $y - x$ es el líder de la clase. Por consiguiente, la decodificación es posible si y solo si la clase del vector recibido posee líder y el error es asumido como el líder de la clase. La Proposición 48 garantiza que si el número de errores no supera la capacidad correctora del código, entonces la decodificación es correcta.

Para realizar este proceso, se construye una tabla (Standard Decoding Array, SDA) con dos columnas y tantas filas como clases hay en $\mathbb{F}_q^n/\mathcal{C}$, es decir, q^{n-k} filas. En la primera columna escribimos el síndrome de un elemento cualquiera de cada una de las clases; en la segunda el líder de la clase correspondiente, si existe. Esta tabla se construye una vez y sirve para la decodificación de cualquier vector.

Algoritmo 49 *Recibido un vector y*

1. *Calcular $s(y)$ y buscarlo en la columna de síndromes.*
2. *Si la clase correspondiente no posee líder, la decodificación falla. Fin.*
3. *Si la clase posee líder, e, se decide que e es el error cometido.*
   La palabra decodificada es $y - e$. Fin.

Este es un algoritmo genérico de decodificación válido para cualquier código lineal, impracticable si el tamaño de la tabla es muy grande. Casi todo código lineal particular tiene un algoritmo propio de decodificiación mucho más eficiente, siendo la sencillez del algoritmo de decodificación uno de los criterios para preferir un código en una aplicación real.

Capítulo 3

Códigos lineales binarios con técnicas elementales

El objetivo de este capítulo es la obtención de códigos lineales binarios óptimos utilizando construcciones muy simples basadas meramente en sumas.

Entendemos por código óptimo aquel código que, fijada su longitud y dimensión, tenga la máxima distancia mínima posible.

Llamaremos código *casi óptimo* a un código con parámetros $[n, k, d-1]_2$, siendo d la distancia mínima del código óptimo para dicha longitud y dimensión, n y k.

En las páginas [Grassl] y [SchSch] podemos ver tablas en las que se muestran códigos que tienen la máxima distancia mínima en función de los parámetros de longitud y dimensión, y, en los casos en los que no se sabe con exactitud dicha distancia mínima óptima, se expone la cota de esta y el código con la máxima distancia mínima encontrado hasta el momento, pudiendo ser esta distancia mínima efectivamente la máxima.

Siendo los métodos utilizados tan sencillos, no esperábamos encontrar nada revelador. A pesar de ello, hemos obtenido en algunos casos códigos óptimos, códigos *casi óptimos* y otros ejemplos cautivadores. El principal valor de este hecho es la posibilidad de realizar a mano los cálculos de los pesos, el número de palabras que hay para cada peso y otros datos del código, lo cual es posible gracias a la notable simetría de los códigos. Además, hemos hallado códigos en los que el número de pesos no nulos es pequeño y, en algun caso, hemos obtenido códigos de gran longitud.

Algunas características que hemos observado en los códigos que hemos construido han suscitado nuestro interés. Hay códigos con solo dos o tres pesos no nulos. Si se desea profundizar en ello, pueden consultarse los artículos [WaDiXu] y [Ding], que tratan sobre códigos con dos y tres pesos no nulos, respectivamente. Otra propiedad de algunos códigos es que los pesos de todas sus palabras son *divisibles entre cuatro* y, por tanto, son códigos autoortogonales.

Sin embargo, estos códigos son poco susceptibles de ser utilizados en aplicaciones reales debido a su baja dimensión, puesto que esto conlleva una baja tasa de transmisión de información.

Los códigos lineales binarios que hemos obtenido tienen los siguientes parámetros:

- Códigos óptimos

$$[15, 5, 7]_2,\ \ [20, 5, 9]_2,\ \ [20, 6, 8]_2,\ \ [21, 5, 10]_2,\ \ [28, 7, 12]_2,\ \ [77, 7, 36]_2,$$

$$[93, 8, 44]_2,\ \ [120, 9, 56]_2,\ \ [121, 8, 58]_2,\ \ [136, 9, 64]_2$$

- Códigos *casi óptimos*

$$[26, 6, 11]_2, \ [120, 8, 57]_2, \ [135, 9, 63]_2$$

- Otros códigos interesantes

$$[130, 9, 58]_2, \ [171, 9, 72]_2, \ [240, 10, 112]_2, \ [262, 10, 120]_2$$

Los códigos lineales binarios con solo tres pesos no nulos tienen los siguientes parámetros:

$$[15, 5, 7]_2, \ [21, 5, 10]_2, \ [28, 7, 12]_2, \ [93, 8, 44]_2, \ [120, 9, 56]_2, \ [136, 9, 64]_2$$

Hemos obtenido los siguientes parámetros correspondientes a códigos *divisibles entre cuatro* y, por consiguiente, a códigos autoortogonales:

$$[28, 7, 12]_2, \ [93, 8, 44]_2, \ [120, 9, 56]_2, \ [136, 9, 64]_2, \ [240, 10, 112]_2$$

Como ya hemos comentado, los códigos que hemos construido poseen dimensión baja. Quien desee profundizar en este tema, puede examinar los siguientes artículos: [BoJaf] y [Til] tratan sobre códigos con dimensión a lo sumo 7 y dimensión 7, respectivamente; [BoJaVe] se ocupa de los códigos de dimensión ocho y [DoGuSi] de los códigos de dimensión nueve. Finalmente, el artículo [GuBh], además de ocuparse de los códigos de dimensión nueve, se refiere a los códigos de dimensión diez.

Compararemos nuestros códigos con los códigos de [Grassl], cuyas construcciones son en muchos casos automatizadas utilizando el sistema algebraico computacional MAGMA y, en consecuencia, más laboriosas.

3.1. Código lineal binario óptimo de parámetros $[15, 5, 7]_2$

A modo de introducción, para describir las técnicas que usaremos en este capítulo, comenzaremos dando un ejemplo bastante simple para obtener un código de parámetros bien conocidos $[15, 5, 7]_2$.

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{15}$, de parámetros $[15, 5, d]_2$ siguiente:

LLamamos cabecera a los elementos $a_i \in \mathbb{F}_2$ que se encuentran en las primeras componentes de las palabras-código; y llamamos cola al resto de elementos que dependen linealmente de los elementos de la cabecera.

Dicho esto, en la cabecera de las palabras del código, cinco coordenadas, se colocan los elementos $a_1, \ldots, a_5 \in \mathbb{F}_2$ libres; y en la cola, todas las sumas posibles de tres elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_1 = \Big\{ (a_1, a_2, a_3, a_4, a_5, \ a_i + a_j + a_k \ ) \ : \ \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, \ldots, 5\}, \text{ distintos} \Big\} \subset \mathbb{F}_2^{15}$$

De esta manera, tal como se indicó previamente, la longitud del código es

$$n = 5 + \binom{5}{3} = 5 + 10 = 15$$

es decir, 5 elementos en la cabecera y $\binom{5}{3}$ elementos en la cola, que es el número de subconjuntos de tres elementos elegidos del conjuntos de cinco elementos de la cabecera, los cuales se sumarán para obtener los elementos correspondientes.

La dimensión es $k = 5$ y, por lo tanto, el número de palabras que hay en el código es $2^5 = 32$.

Describiremos una matriz generadora G_1 dividiéndola en bloques. En el primer bloque se tiene la matriz identidad 5×5, que nos dará la información que hemos codificado, $v \in \mathbb{F}_2^5$, al realizar el producto $v \cdot G_1 = [v|w]$. El segundo bloque estará formado por todas las columnas en las que hay tres unos y el resto ceros, que, en el producto anterior, nos dará $w \in \mathbb{F}_2^{10}$ y nos permitirá corregir errores en el proceso de decodificación. El orden de estas columnas es irrelevante pues dará lugar a códigos equivalentes. Esta matriz tendrá orden 5×15 y rango 5.

$$G_1 = \left[\begin{array}{ccccc|ccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 1 \end{array}\right]$$

De esta forma, el código $\mathcal{C}_1$ es sistemático.

Sabemos que, en un código lineal, el peso mínimo es igual a la distancia mínima. Por consiguiente, para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código; para ello usaremos métodos combinatorios.

Recordemos que, dado un elemento de un código $\mathcal{C}$, $x \in \mathcal{C}$, se define su **peso** $w(x)$ como el número de coordenadas no nulas de x.

Los resultados se muestran en la siguiente tabla.

n_i	$\sum_3$	**peso**
1	6	7
2	6	8
3	4	7
4	4	8
5	10	15

Cuadro 3.1: Pesos del código

En la primera columna aparece el número exacto de a_i que son distintos de cero, n_i, lo que dará el peso de la cabecera. En la segunda columna, se muestra el peso de la cola, cuántas sumas de tres elementos son distintas de cero dependiendo del número n_i. En la última columna, los elementos de la fila correspondiente se suman, dando como resultado el peso total de las palabras-código con dicha propiedad.

Los cálculos se detallan a continuación:

- Si en la cabecera hay exactamente **un** $a_i \neq 0$, el peso de la cabecera será igual a 1. El peso de la cola será $\binom{4}{2}$, pues las únicas sumas que resultan distintas de cero son las sumas que contienen al a_i distinto de cero; los otros dos elementos de la suma podrán ser cualesquiera entre los cuatro elementos de la cabecera que son distintos de cero.

$$1 + \binom{4}{2} = 1 + 6 = 7$$

- Si en la cabecera hay exactamente **dos** $a_i \neq 0$, el peso de la cabecera será 2. Hallemos el peso de la cola. Fijémonos en que la única manera de que un elemento de la cola sume uno es que

en la suma esté uno y solo uno de los dos elementos de la cabecera distintos de cero; si no hubiese ninguno, obviamente la suma sería cero; y si estuviesen los dos sumaría $2 = 0$ en $\mathbb{F}_2$. Luego para cada a_i distinto de cero elegimos subconjuntos de dos elementos en el conjunto de elementos de la cabecera que sean cero, esto es, $2 \cdot \binom{3}{2}$.

$$2 + 2 \cdot \binom{3}{2} = 2 + 2 \cdot 3 = 8$$

- Si en la cabecera hay exactamente **tres** $a_i \neq 0$, el peso de la cabecera será 3. El peso de la cola será $1 + 3$, el elemento formado por la suma de los tres elementos de la cabecera que son uno; y tres elementos formados por las sumas en las que hay un elemento de la cabecera distinto de cero y los dos elementos iguales a cero que quedan.

$$3 + (1 + 3) = 7$$

- Si en la cabecera hay exactamente **cuatro** $a_i \neq 0$, el peso de esta será 4. El peso de la cola será $\binom{4}{3}$, pues, las sumas de tres elementos de la cabecera que son distintas de cero son las posibles maneras de elegir tres elementos entre los cuatro que son distintos de cero; si en alguna suma estuviese el único elemento de la cabecera que es cero, la suma sería $2 = 0$ en $\mathbb{F}_2$.

$$4 + \binom{4}{3} = 4 + 4 = 8$$

- Si en la cabecera hay exactamente **cinco** $a_i \neq 0$, el peso de la cabecera será 5 y el peso de la cola $\binom{5}{3}$, todas las posibles maneras de escoger subconjuntos de tres elementos entre los cinco elementos de la cabecera.

$$5 + \binom{5}{3} = 5 + 10 = 15$$

Veamos ahora cuántas palabras hay para cada uno de los pesos.

En todo código lineal está la palabra que tiene todas sus componentes nulas.

(I) Hemos visto que, si hay un solo $a_i \neq 0$, entonces el peso es 7. Luego hay 5 palabras de peso 7, una para cada $i \in \{1, 2, 3, 4, 5\}$.

(II) Si hay exactamente dos $a_i \neq 0$, el número de palabras con esta propiedad es $\binom{5}{2} = 10$. Hay 10 palabras con peso 8.

(III) El número de palabras con exactamente tres $a_i \neq 0$ es $\binom{5}{3} = 10$. Hay 10 palabras con peso 7.

(IV) El número de palabras con exactamente cuatro $a_i \neq 0$ es $\binom{5}{4} = 5$. Hay 5 palabras con peso 8.

(V) Y, por último, hay una palabra con todos los elementos de la cabecera distintos de cero. Hay una palabra con peso 15.

El número total de palabras es $1+5+10+10+5+1=32=2^5$, como cabía esperar.

Se define A_i como el número exacto de palabras que tienen peso i. Tenemos lo siguiente:

$$\begin{array}{rcl} A_0 & = & 1 \\ A_7 & = & 15 \\ A_8 & = & 15 \\ A_{15} & = & 1 \end{array}$$

Observamos que en el código $\mathcal{C}_1$ está la palabra cuyas componentes son todas uno, $[1,\ldots,1]$. Esto quiere decir que si en el código está una palabra x, entonces también está su palabra complementaria $x+[1,\ldots,1]$ y sus pesos suman 15. Teniendo en cuenta este razonamiento, fijémonos en la tabla anterior. Notemos que se trata de un código con solo tres pesos no nulos; estos pesos tienen un peso complementario: 0 y 15, 7 y 8, y hay la misma cantidad de palabras de un peso y su complementario. Es un código *autocomplementario* con solo **tres pesos** no nulos.

En conclusión, la distancia mínima del código es $d=7$ y se tiene un código de parámetros $[15,5,7]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código óptimo.

n/k	**3**	**4**	**5**	**6**	**7**
13	7	6	5	4	4
14	8	7	6	5	4
15	8	8	7	6	5
16	8	8	8	6	6
17	9	8	8	7	6

Cuadro 3.2: Bounds on the minimum distance of linear codes over $GF(2)$

Advertimos que el $[15,5,7]_2$ código lineal binario se trata de un código óptimo pues cumple la cota de Griesmer (2.3) con igualdad.

$$\sum_{i=0}^{4}\left\lceil\frac{7}{2^i}\right\rceil = 7+4+2+1+1=15$$

Puesto que el código consta solamente de 32 palabras, no es necesario idear un algoritmo de decodificación; por tanto se sigue el método general. Recibida una palabra, el receptor comprueba si dicha palabra está en el código; en caso afirmativo, interpreta que la palabra ha sido transmitida correctamente. Si la palabra no está en el código, entonces se compara la distancia de dicha palabra con el resto de palabras hasta que esta sea menor que 3, que es la capacidad correctora del código.

A continuación daremos otras construcciones comunes de un código de parámetros $[15,5,7]_2$:

- Sea un código simplex lineal binario de parámetros $[2^4-1,4,2^{4-1}]_2=[15,4,8]_2$. Todas las palabras no nulas tienen peso ocho. Añadimos al código la palabra cuyas componentes son todas uno, $[1,1,\ldots,1]$, la cual no está en el código. El código aumentado que obtenemos tiene parámetros $[15,5,7]_2$.
- Existe un código binario BCH en sentido estricto primitivo de parámetros $[15,5,7]_2$. Este código de longitud $15=2^4-1$ está formado por todos los polinomios de $\mathbb{F}_2[X]/(X^{15}-1)$ que

se anulan en $\alpha, \alpha^3, \alpha^5$. El polinomio generador es

$$\begin{aligned} g(x) &= f_1(x)f_3(x)f_5(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1) \\ &= x^{10}+x^8+x^5+x^4+x^2+x+1 \end{aligned}$$

La matriz de control H tiene orden 3×15 sobre $GF(2^4)$ u orden 12×15 sobre $GF(2)$.

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{42} \\ 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{70} \end{bmatrix} = \left[\begin{array}{cccccccccccccc} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ \hline 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \\ \hline 1&0&1&1&0&1&1&0&1&1&0&1&1&0&1 \\ 0&1&1&0&1&1&0&1&1&0&1&1&0&1&1 \\ 0&1&1&0&1&1&0&1&1&0&1&1&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right]$$

Las dos últimas filas son linealmente redundantes. Hay 10 filas linealmente independientes, luego $k = 5$.

- La construcción dada en [Grassl] es la siguiente:

  Construction of a linear code $[15, 5, 7]$ over $GF(2)$:

  [1]: $[8, 1, 8]$ Cyclic Linear Code over $GF(2)$
  Repetition Code of length 8

  [2]: $[4, 1, 4]$ Cyclic Linear Code over $GF(2)$
  Repetition Code of length 4

  [3]: $[4, 3, 2]$ Cyclic Linear Code over $GF(2)$
  Dual of the Repetition Code of length 4

  [4]: $[8, 4, 4]$ Quasicyclic of degree 2 Linear Code over $GF(2)$
  PlotkinSum of [3] and [2]

  [5]: $[16, 5, 8]$ Linear Code over $GF(2)$
  PlotkinSum of [4] and [1]

  [6]: $[15, 5, 7]$ Linear Code over $GF(2)$
  Puncturing of [5] at $\{16\}$

3.2. Código lineal binario óptimo de parámetros $[20, 5, 9]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{20}$, de parámetros $[20, 5, d]_2$ definido de la siguiente forma.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_5 \in \mathbb{F}_2$ y, en la cola, todas las sumas posibles de tres y cuatro elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_2 = \left\{ (a_1, a_2, a_3, a_4, a_5, \sum_3 a_j, \sum_4 a_k) \ : \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, 2, 3, 4, 5\} \right\} \subset \mathbb{F}_2^{20}$$

La longitud del código es

$$n = 5 + \binom{5}{3} + \binom{5}{4} = 5 + 10 + 5 = 20$$

i.e. 5 elementos en la cabecera y $\binom{5}{3} + \binom{5}{4}$ elementos en la cola, que son el número de subconjuntos de tres y cuatro elementos, respectivamente, escogidos del conjunto de cinco elementos de la cabecera, los cuales se sumarán para obtener los elementos de la cola.

La dimensión es $k = 5$, luego el número de palabras que hay en el código es $2^5 = 32$.

Una matriz generadora G_2 tendrá orden 5×20 y rango 5. Podemos describirla, como en el caso previo, dividiéndola en bloques. En primer lugar, tendremos la matriz identidad 5×5. El siguiente bloque, 5×10, estará compuesto por todas las posibles columnas en las que hay tres unos y dos ceros, sin repetirse ninguna; y, por último, un bloque 5×5, donde las columnas son todos los vectores posibles que tienen cuatro unos y un cero, sin repetición. Por supuesto, el orden de estas columnas no es de gran importancia puesto que dará códigos equivalentes.

$$G_2 = \left[\begin{array}{ccccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & \cdots & 0 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 & 1 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 & 0 & 1 & \cdots & 1 \end{array}\right]$$

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla.

$\boldsymbol{n_i}$	$\sum_{\mathbf{3}}$	$\sum_{\mathbf{4}}$	**peso**
1	6	4	11
2	6	2	10
3	4	2	9
4	4	4	12
5	10	0	15

Cuadro 3.3: Pesos del código

En la primera columna aparece el número exacto de a_i que son distintos de cero, n_i, lo que dará el peso de la cabecera. Las segunda y tercera columnas muestran el peso de la cola, dependiendo del número de a_i distintos de cero, separada en dos bloques: en el primer caso, para las posiciones correspondientes a las sumas de tres elementos; y en el segundo, para todas las sumas de cuatro elementos; por último, en la cuarta columna aparece el peso total como suma de los pesos de la cabecera, primera columna, y de la cola, segunda y tercera columna.

Seguidamente se concretan los cálculos realizados:

- Primeramente, si en la cabecera hay exactamente **un** $a_i \neq 0$, el peso de la cabecera será 1. El peso del primer bloque de la cola, es decir, el peso de las posiciones correspondientes a sumas de tres elementos, será 6, puesto que, en este caso, para que la suma de tres elementos elegidos de la cabecera sea distinto de cero, tiene que contener al a_i que era distinto de cero entre sus tres elementos sumados. De este modo, el número de componentes distintas de cero de

la palabra-código será el número de subconjuntos de dos elementos escogidos en el conjunto formado por los cuatro elementos de la cabecera que son cero, esto es, $\binom{4}{2}$. De igual manera, el peso del segundo bloque de la cola, el que corresponde a las sumas de cuatro elementos, será igual al número de posibles maneras de tomar subconjuntos de tres elementos en el conjunto anterior, $\binom{4}{3}$.

$$1 + \binom{4}{2} + \binom{4}{3} = 1 + 6 + 4 = 11$$

- Si en la cabecera hay exactamente **dos** $a_i \neq 0$, el peso de la cabecera será 2. Para calcular el peso de la cola, la dividimos en dos bloques. Para el primero, veremos cuántas sumas de tres elementos son distintas de cero en $\mathbb{F}_2$. Las sumas en las que están ambos elementos son cero, luego solo las sumas en las que esté uno y solo uno de ellos resultarán 1. Esto es, para cada $a_i \neq 0$, elegir todos los posibles subconjuntos de dos elementos entre los tres elementos que son cero, i.e. $\binom{3}{2}$, por lo tanto el resultado será $2 \cdot \binom{3}{2}$. Igualmente, para el segundo bloque, las sumas de cuatro elementos en las que estén los dos a_i distintos de cero sumaran cero. De esta forma, las sumas cuyo resultado es distinto de cero son las sumas en las que está un elemento de los dos distintos de cero sumado a los tres elementos iguales a cero que quedan. Es decir, el peso total en el segundo bloque es 2.

$$2 + 2 \cdot \binom{3}{2} + 2 = 2 + 6 + 2 = 10$$

- Si en la cabecera hay exactamente **tres** $a_i \neq 0$. En la cabecera tendremos peso 3. En el primer bloque de la cola, las únicas sumas de tres elementos que darán como resultado distinto de cero serán, en primer lugar, las sumas de los tres elementos distintos de cero y, además, las sumas de cada uno de estos elementos con los otros dos elementos que son cero, esto es $1 + 3$. En el segundo bloque de la cola, el peso es 2 ya que solo hay dos sumas de cuatro elementos de la cabecera que resultan 1, los tres elementos que son distintos de cero con cada uno de los elementos que son cero.

$$3 + (1 + 3) + 2 = 9$$

- Si en la cabecera hay exactamente **cuatro** $a_i \neq 0$, en la cabecera el peso será 4. Las sumas de tres elementos de la cabecera que son distintas de cero son las posibles maneras de elegir tres elementos entre los cuatro que son distintos de cero, puesto que si en alguna suma estuviese el único elemento de la cabecera que es cero, la suma sería $2 = 0$ en $\mathbb{F}_2$. Luego el peso del primer bloque de la cola es $\binom{4}{3}$. Las sumas de cuatro elementos de la cabecera que son distintas de cero serán las sumas que incluyen al elemento de la cabecera que es cero y los otros tres sumandos elegidos de todas las maneras posibles entre los cuatro elementos de la cabecera que son distintos de cero, esto es, igual que en el primer bloque, $\binom{4}{3}$.

$$4 + \binom{4}{3} + \binom{4}{3} = 4 + 4 + 4 = 12$$

- Finalmente, si en la cabecera hay exactamente **cinco** $a_i \neq 0$, es decir, todos los elementos de la cabecera son distintos de cero, entonces el peso de esta será 5. En la cola el peso será 10. En el primer bloque tendremos que, al ser todos los elementos de la cabecera distintos de cero,

todas las sumas posibles de tres elementos elegidos entre esos cinco siempre serán distintas de cero, luego el peso es $\binom{5}{3}$. Sin embargo, en el segundo bloque de la cola, las sumas de cuatro elementos, siendo estos cuatro elementos siempre unos, serán 0 en $\mathbb{F}_2$.

$$5 + \binom{5}{3} + 0 = 5 + 10 + 0 = 15$$

Calculamos cuántas palabras hay para cada uno de los pesos y mostramos los resultados en una tabla.

En todo código lineal está la palabra cuyas componentes son todas nulas.

(I) Si hay un solo $a_i \neq 0$, entonces el peso es 11. Luego hay 5 palabras de peso 11, una para cada $i \in \{1, 2, 3, 4, 5\}$.

(II) Si hay exactamente dos $a_i \neq 0$, el número de palabras con esta propiedad es $\binom{5}{2} = 10$. Hay 10 palabras con peso 10.

(III) El número de palabras con exactamente tres $a_i \neq 0$ es $\binom{5}{3} = 10$. Hay 10 palabras con peso 9.

(IV) El número de palabras con exactamente cuatro $a_i \neq 0$ es $\binom{5}{4} = 5$. Hay 5 palabras con peso 12.

(V) Y, por último, hay una palabra con todos los elementos de la cabecera distintos de cero. Hay una palabra con peso 15.

El número total de palabras es $1 + 5 + 10 + 10 + 5 + 1 = 32 = 2^5$, como ya sabíamos.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_9 & = & 10 \\ A_{10} & = & 10 \\ A_{11} & = & 5 \\ A_{12} & = & 5 \\ A_{15} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 9$ y se tiene un código de parámetros $[20, 5, 9]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código óptimo.

n/k	**3**	**4**	**5**	**6**	**7**
18	10	8	8	8	7
19	10	9	8	8	8
20	11	10	9	8	8
21	12	10	10	8	8
22	12	11	10	9	8

Cuadro 3.4: Bounds on the minimum distance of linear codes over $GF(2)$

Observamos que la construcción del código lineal dada en [Grassl] es más compleja que en nuestro caso.

Construction of a linear code $[20, 5, 9]$ over $GF(2)$:

[1]: $[8, 7, 2]$ Cyclic Linear Code over $GF(2)$
Dual of the Repetition Code of length 8

[2]: $[135, 8, 65]$ Linear Code over $GF(2)$
Let $C1$ be the BCH Code over $GF(2)$ of parameters 127 63. Let $C2$ the Subcode Between Code of dimension 8 between $C1$ and the BCH Code with parameters 127 64. Return Construction X using $C1, C2$ and [1]

[3]: $[70, 7, 33]$ Linear Code over $GF(2)$
Puncturing of [2] at

$$\{2, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 24, 25, 26, 27, 29, 31, 32, 33, 38, 39, 41, 42,$$

$$43, 45, 48, 49, 53, 55, 57, 58, 64, 66, 67, 68, 69, 73, 74, 75, 77, 78, 80, 81, 84, 87, 89, 92,$$

$$97, 100, 101, 102, 105, 107, 108, 110, 114, 118, 119, 122, 123, 125, 127, 128, 135\}$$

[4]: $[37, 6, 17]$ Linear Code over $GF(2)$
Puncturing of [3] at

$$\{2, 8, 10, 11, 14, 17, 20, 21, 22, 24, 27, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 48, 49, 50, 51,$$

$$52, 55, 57, 58, 60, 61, 62, 65\}$$

[5]: $[20, 5, 9]$ Linear Code over $GF(2)$
Puncturing of [4] at

$$\{2, 7, 8, 10, 12, 13, 14, 17, 21, 22, 23, 25, 28, 29, 30, 31, 33\}$$

El $[20, 5, 9]_2$ código lineal binario se trata de un código óptimo pues cumple la cota de Griesmer (2.3) con igualdad.

$$\sum_{i=0}^{4} \left\lceil \frac{9}{2^i} \right\rceil = 9 + 5 + 3 + 2 + 1 = 20$$

Igual que en el caso anterior, se sigue el método general de decodificación debido a la pequeña cantidad de palabras que tiene el código. Recibida una palabra, el receptor comprueba si dicha palabra está en el código; en el caso de que la palabra esté en el código, interpreta que la palabra ha sido transmitida de forma correcta. Si la palabra no está en el código, se compara la distancia de dicha palabra con el resto de palabras hasta que esta sea menor que 4, que es la capacidad correctora del código.

El código de parámetros $[20, 5, 9]_2$ extendido da lugar a un código lineal binario de parámetros $[21, 5, 10]_2$, el cual también es óptimo.

Veamos a continuación la relación entre sus pesos y el número de palabras del código con dichos pesos y observemos que se trata de un código con solo **tres pesos** no nulos.

$$\begin{aligned} A_0 &= 1 \\ A_{10} &= 20 \\ A_{12} &= 10 \\ A_{16} &= 1 \end{aligned}$$

3.3. Código lineal binario óptimo de parámetros $[28, 7, 12]_2$

Siguiendo el mismo procedimiento que en los ejemplos anteriores, se considera el siguiente código lineal incluido en $\mathbb{F}_2^{28}$.

$$\mathcal{C}_3 = \left\{(a_1, a_2, a_3, a_4, a_5, a_6, a_7, \sum_5 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 7\}\right\} \subset \mathbb{F}_2^{28}$$

Se trata de un código lineal binario cuyas palabras están constituidas por una cabecera, en la que se colocan los elementos que definen la dimensión del código, y por una cola, formada por todas las posibles sumas de cinco elementos que se pueden formar con los elementos de la cabecera y subíndices distintos.

Así pues, la longitud del código es

$$n = 7 + \binom{7}{5} = 28$$

esto es, 7 elementos en la cabecera y $\binom{7}{5}$ elementos en la cola, resultado de tomar todos los posibles subconjuntos de cinco elementos del conjunto de siete elementos de la cabecera para formar todas las sumas requeridas.

La dimensión del subespacio vectorial $\mathcal{C}_3$ es $k = 7$ y, en consecuencia, el número de palabras en $\mathcal{C}_3$ es $2^7 = 128$.

Una matriz generadora G_3 tendrá orden 7×28, rango 7 y la siguiente forma.

$$G_3 = \left[\begin{array}{ccccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 1 \end{array}\right]$$

De la misma manera que en los ejemplos anteriores, vamos a describir G_3 dividiéndola en bloques. Primero, tendremos la matriz identidad 7×7. El siguiente bloque, 7×21, estará compuesto por todas las posibles columnas en las que hay cinco unos y el resto ceros sin repetirse ninguna. El orden de estas columnas no es importante ya que dará códigos equivalentes.

Los resultados de los pesos de las palabras se muestran en la tabla.

$\boldsymbol{n_i}$	$\sum_{\mathbf{5}}$	**peso**
1	15	16
2	10	12
3	6+3	12
4	12	16
5	1+10	16
6	6	12
7	21	28

Cuadro 3.5: Pesos del código

A continuación se desarrollan los cálculos realizados.

- Si en la cabecera hay exactamente **un** $a_i \neq 0$, el peso de la cabecera es 1. Hallemos el peso de la cola. Es claro que las únicas componentes que serán distintas de cero serán las que contengan al a_i que es distinto de cero en la suma. Puesto que en la cola están (sumados) todos los subconjuntos de cinco elementos elegidos entre los siete de la cabecera, el número de elementos de la cola que contiene a un determinado a_i es $\binom{6}{4}$, todos los posibles subconjuntos de cuatro elementos elegidos entre los seis restantes.

$$1 + \binom{6}{4} = 1 + 15 = 16$$

- Si en la cabecera hay exactamente **dos** $a_i \neq 0$, el peso de la cabecera es 2. Para hallar el peso de la cola, nos damos cuenta de que la componente correspondiente a las sumas de cinco elementos en los que estén ambos a_i distinto de cero será cero, al igual que las componentes en las que no esté ninguno de ellos. Entonces, para cada uno de los a_i distinto de cero, el número de sumas que serán distintas de cero, será $\binom{5}{4}$, todos los posibles subconjuntos de cuatro elementos tomados entre los cinco que quedan. Como hay dos a_i, el número total de componentes que serán distintas de cero y aportarán al peso serán $2 \cdot \binom{5}{4}$.

$$2 + 2 \cdot \binom{5}{4} = 2 + 10 = 12$$

- Si en la cabecera hay exactamente **tres** $a_i \neq 0$, el peso de la cabecera es 3. El peso de la cola es $6 + 3$. Las componentes que serán distintas de cero pueden ser de dos tipos. En primer lugar, serán distintas de cero las componentes en las que aparezcan los tres a_i que son distintos de cero. Hay $\binom{4}{2}$ componentes con esta propiedad, el número de subconjuntos de dos elementos que se pueden tomar entre los cuatro elementos de la cabecera que son cero, para que la suma tenga cinco elementos. El otro tipo de componentes que serán distintas de cero son las que contienen a uno y solo uno de los a_i distintos de cero, puesto que si contuviesen a dos de ellos, la suma en $\mathbb{F}_2$ sería cero. Como hay cuatro elementos de la cabecera iguales a cero y tres distintos de cero, solo hay una componente de este tipo para cada a_i, es decir, en total 3.

$$3 + \left(\binom{4}{2} + 3\right) = 3 + 6 + 3 = 12$$

- Si en la cabecera hay exactamente **cuatro** $a_i \neq 0$, el peso de la cabecera es 4. Las únicas sumas de cinco elementos elegidos entre siete, de los cuales cuatro son distintos de cero, serán las sumas en las que hay tres elementos distintos de cero y dos iguales a cero. El número de subconjuntos que podemos tomar de tres elementos en un conjunto de cuatro es $\binom{4}{3}$ y el número de subconjuntos que podemos tomar de dos elementos en un conjunto de tres es $\binom{3}{2}$. Luego, en total, el peso de la cola es el producto $\binom{4}{3} \cdot \binom{3}{2}$

$$4 + \binom{4}{3} \cdot \binom{3}{2} = 4 + 12 = 16$$

- Si en la cabecera hay exactamente **cinco** $a_i \neq 0$, el peso de la cabecera es 5. En la cola, las componentes que son distintas de cero contendrán en sus elementos sumados o a los cinco elementos distintos de cero, o a tres de ellos. En el caso de contener a tres de ellos, hay en total el número de subconjuntos que podemos tomar de tres elementos en el conjunto de los cinco que son distintos de cero; los otros dos elementos que completan la suma serán los dos elementos de la cabecera que son distintos de ellos. En conclusión, el peso de la cola será $1 + \binom{5}{3}$.

$$5 + \left(1 + \binom{5}{3}\right) = 5 + 1 + 10 = 16$$

- Si en la cabecera hay exactamente **seis** $a_i \neq 0$, el peso de la cabecera es 6. En la cabecera solo hay un elemento distinto de cero; las componentes que tengan a este elemento como parte de la suma, sumarán $4 = 0$ en $\mathbb{F}_2$. El resto de las sumas sumarán $5 = 1$ en $\mathbb{F}_2$, luego el peso de la cola es igual a $\binom{6}{5}$, todos los subconjuntos que se pueden tomar de cinco elementos elegidos en un conjunto de seis.

$$6 + \binom{6}{5} = 6 + 6 = 12$$

- Si en la cabecera hay exactamente **siete** $a_i \neq 0$, el peso de la cabecera es 7. Todas las componentes de la cabecera son unos y, por consiguiente, todas las sumas de cinco elementos escogidos de la cabecera serán igual a uno en $\mathbb{F}_2$.

$$7 + \binom{7}{5} = 7 + 21 = 28$$

Calculamos cuántas palabras hay para cada uno de los pesos y mostramos los resultados en una tabla.

En todo código lineal está la palabra que tiene todas sus componentes nulas.

(I) Si hay exactamente un $a_i \neq 0$, entonces el peso es 16. Luego hay 7 palabras de peso 16, una para cada $i \in \{1, 2, 3, 4, 5, 6, 7\}$.

(II) Si hay exactamente dos $a_i \neq 0$, el número de palabras con esta propiedad es $\binom{7}{2} = 21$ y, como hemos visto, el peso de cada una de ellas es 12.

(III) El número de palabras con exactamente tres $a_i \neq 0$ es $\binom{7}{3} = 35$. Cada una de ellas tiene peso 12.

(IV) El número de palabras con exactamente cuatro $a_i \neq 0$ es $\binom{7}{4} = 35$. Cada una de ellas tiene peso 16.

(V) El número de palabras con exactamente cinco $a_i \neq 0$ es $\binom{7}{5} = 21$. Cada una de ellas tiene peso 16.

(VI) El número de palabras con exactamente seis $a_i \neq 0$ es $\binom{7}{6} = 7$. Cada una de ellas tiene peso 12.

(VII) Y, por último, hay una palabra con todos los elementos de la cabecera distintos de cero. Tiene peso 28.

El número total de palabras es $1 + 7 + 21 + 35 + 35 + 21 + 7 + 1 = 128 = 2^7$, como ya sabíamos.

El código $\mathcal{C}_3$ se trata de un código *autocomplementario* puesto que la palabra cuyas componentes son todas uno está en el código. Esto quiere decir que si una palabra $x \in \mathcal{C}_3$, entonces la palabra $x + [1, \ldots, 1] \in \mathcal{C}_3$, la cual se trata de su palabra complementaria.

Observamos esta característica, junto con el hecho de que el código tiene solamente **tres pesos** no nulos. Notemos, además, que el peso de cada palabra es *divisible entre cuatro* y, por ese motivo, se trata de un código **autoortogonal**.

$$\begin{aligned} A_0 &= 1 \\ A_{12} &= 63 \\ A_{16} &= 63 \\ A_{28} &= 1 \end{aligned}$$

En conclusión, la distancia mínima del código es $d = 12$ y se tiene un código de parámetros $[28, 7, 12]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código óptimo.

n/k	**5**	**6**	**7**	**8**	**9**
26	12	12	11	10	9
27	13	12	12	10	10
28	14	12	12	11	10
29	14	13	12	12	11
30	15	14	12	12	12

Cuadro 3.6: Bounds on the minimum distance of linear codes over $GF(2)$

Sin embargo, observando dicha tabla, notemos que existe un código con parámetros $[27, 7, 12]_2$. Esto quiere decir que nuestro código de parámetros $[28, 7, 12]_2$ no es óptimo con respecto a la Definición 38 que dimos en la página 9 porque existe otro con menor longitud pero con igual dimensión y distancia mínima.

La construcción de dicho código dada en [Grassl] se realiza recortando un código BCH extendido.

Construction of a linear code $[28, 7, 12]$ over $GF(2)$:

[1]: $[32, 11, 12]$ Linear Code over $GF(2)$
Extended BCH Code with parameters 31 11

[2]: $[28, 7, 12]$ Linear Code over $GF(2)$
Shortening of [1] at $\{29 \ldots 32\}$

3.4. Código lineal binario óptimo de parámetros $[77, 7, 36]_2$

Tomamos un código lineal binario de parámetros $[77, 7, d]_2$ definido como sigue: en la cabecera de las palabras-código se colocan siete elementos $a_i \in \mathbb{F}_2$; y, en la cola, todas las posibles sumas de

tres y cuatro elementos escogidos entre los a_i que hemos colocado en la cabecera con subíndices distintos.

$$\mathcal{C}_4 = \left\{(a_1, \ldots, a_7, \sum_3 a_j, \sum_4 a_k) \ : \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, \ldots, 7\}\right\} \subset \mathbb{F}_2^{77}$$

La longitud del código es

$$n = 7 + \binom{7}{3} + \binom{7}{4} = 7 + 35 + 35 = 77$$

y la dimensión de $\mathcal{C}_4$ como subespacio vectorial de $\mathbb{F}_2^{77}$ es $k = 7$. El número de palabras que hay en el código es $2^7 = 128$.

Para hallar la distancia mínima del código, calcularemos los pesos de todas las palabras con métodos combinatorios, como hemos hecho en otros casos. A continuación se muestran los resultados en una tabla, así como los cálculos detallados. A partir de ahora añadiremos como última columna el número de palabras que hay en el código dependiendo de la cantidad de a_i distintos de cero en la cabecera y lo denotaremos por nº. El número de palabras que hay en el código con exactamente j coordenadas de la cabecera distintas de cero para cada $j \in \{0, \ldots, k\}$ es $\binom{k}{j} = \binom{7}{j}$.

$\boldsymbol{n_i}$	$\sum_{\mathbf{3}}$	$\sum_{\mathbf{4}}$	**peso**	**nº**
1	15	20	36	7
2	20	20	42	21
3	19	16	38	35
4	16	16	36	35
5	15	20	40	21
6	20	20	46	7
7	35	0	42	1

Cuadro 3.7: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{6}{2} + \binom{6}{3} = 1 + 15 + 20 = 36$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{5}{2} + 2 \cdot \binom{5}{3} = 2 + 2 \cdot 10 + 2 \cdot 10 = 42$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(1 + 3 \cdot \binom{4}{2}\right) + \left(4 + 3 \cdot \binom{4}{3}\right) = 3 + (1 + 3 \cdot 6) + (4 + 3 \cdot 4) = 38$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} + 4 \cdot \binom{3}{2}\right) + \left(\binom{4}{3} \cdot 3 + 4\right) = 4 + (4 + 4 \cdot 3) + (4 \cdot 3 + 4) = 36$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \left(\binom{5}{3} + 5\right) + \binom{5}{3} \cdot 2 = 5 + (10 + 5) + 10 \cdot 2 = 40$$

- Exactamente seis $a_i \neq 0$:

$$6 + \binom{6}{3} + \binom{6}{3} = 6 + 20 + 20 = 46$$

- Exactamente siete $a_i \neq 0$:

$$7 + \binom{7}{3} + 0 = 7 + 35 + 0 = 42$$

Veamos de manera concisa cuántas palabras hay con cada uno de los pesos. Reparemos, además, en la curiosa distribución de estos.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{36} & = & 42 \\ A_{38} & = & 35 \\ A_{40} & = & 21 \\ A_{42} & = & 22 \\ A_{46} & = & 7 \end{array}$$

Por ende, la distancia mínima del código es $d = 36$. El código que hemos construido tiene parámetros $[77, 7, 36]_2$, que, como observamos en la tabla correspondiente de [Grassl], es un código óptimo. Reparemos en dicha tabla.

n/k	5	6	7	8	9
75	38	36	36	34	33-34
76	38	37	36	35	34
77	39	38	36	36	34-35
78	40	38	37	36	35-36
79	40	39	38	36	36

Cuadro 3.8: Bounds on the minimum distance of linear codes over $GF(2)$

Observemos que, no obstante, existen códigos de parámetros $[77, 8, 36]_2$, $[76, 7, 36]_2$ y $[75, 7, 36]_2$, este último es el código óptimo si tomamos la acepción de código óptimo dada en la Definición 38.

3.5. Código lineal binario óptimo de parámetros $[93, 8, 44]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{93}$, de parámetros $[93, 8, d]_2$ siguiente.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_9 \in \mathbb{F}_2$, con el detalle de que $a_9 = a_1 + \cdots + a_8$; y, en la cola, todas las sumas posibles de seis elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_5 = \left\{(a_1, \ldots, a_8, a_9 = a_1 + \cdots + a_8, \sum_6 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 9\}\right\} \subset \mathbb{F}_2^{93}$$

La longitud del código es

$$n = 9 + \binom{9}{6} = 9 + 84 = 93$$

La dimensión es $k = 8$ y, por lo tanto, el número de palabras que hay en el código es $2^8 = 256$.

Nota 50 *Si hubiese nueve a_i linealmente independientes en la cabecera y tomásemos la palabra en la que los nueve a_i fuesen iguales a uno, el peso de dicha palabra sería nueve, puesto que todas las sumas de seis elementos resultarían cero. En dicho caso, la distancia mínima sería a lo sumo $d = 9$.*

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

En este caso solo hay una cantidad par de a_i distintos de cero en la cabecera, por la condición $a_9 = a_1 + \cdots + a_8$, lo cual es una ventaja a la hora de calcular los pesos de todas las palabras del código.

Los resultados se muestran en la siguiente tabla y a continuación se detallan las cuentas.

$\boldsymbol{n_i}$	$\sum_{\boldsymbol{6}}$	**peso**	**nº**
2	42	44	36
4	44	48	126
6	38	44	84
8	56	64	9

Cuadro 3.9: Pesos del código y número de palabras

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{7}{5} = 2 + 2 \cdot 21 = 44$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} \cdot \binom{5}{3} + 4\right) = 4 + (4 \cdot 10 + 4) = 48$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(3 \cdot \binom{6}{5} + \binom{6}{3}\right) = 6 + (3 \cdot 6 + 20) = 44$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \binom{8}{5} = 8 + 56 = 64$$

En este caso, puesto que $a_9 = a_1 + \cdots + a_8$, el número de palabras que hay en el código con exactamente j elementos a_i distintos de cero para $j \in \{2, 4, 6, 8\}$ se obtiene, teniendo en cuenta si a_9 es igual o distinto de cero. Si a_9 es igual a cero, el número de palabras con j elementos a_i distintos

de cero es $\binom{k}{j} = \binom{8}{j}$; elegimos subconjuntos de j elementos de la cabecera entre los 8 linealmente independientes, a_9 será cero puesto que es la suma de un número par de unos. En el otro caso, si a_9 es distinto de cero, entonces el número de palabras con j elementos a_i distintos de cero es $\binom{k}{j-1} = \binom{8}{j-1}$; elegimos $j-1$ elementos de la cabecera entre los 8 linealmente independientes, a_9 será igual a uno puesto que es la suma de un número impar de elementos distintos de cero, es decir, habrá $j-1+1$ elementos distintos de cero en total. En conclusión, el número de palabras con exactamente j elementos a_i distintos de cero para $j \in \{2,4,6,8\}$ es $\left(\binom{k}{j-1} + \binom{k}{j}\right)$. Además, en todo código lineal está la palabra con todas sus componentes nulas.

A continuación se muestra el número de palabras en relación a su peso destacando el hecho de que $\mathcal{C}_5$ se trata de un código con solo **tres pesos** no nulos. Por añadidura, todas los pesos del código son *divisibles entre cuatro*, lo cual implica que es un código **autoortogonal**.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{44} & = & 120 \\ A_{48} & = & 126 \\ A_{64} & = & 9 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 44$ y se tiene un código de parámetros $[93, 8, 44]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código óptimo.

n/k	**6**	**7**	**8**	**9**	**10**
91	45	44	43	41-42	40-41
92	46	45	44	42-43	41-42
93	46	46	44	42-44	42
94	47	46	44	43-44	42-43
95	48	47	45	44	43-44

Cuadro 3.10: Bounds on the minimum distance of linear codes over $GF(2)$

Advertimos que existe un $[92, 8, 44]_2$ código lineal binario, el cual es óptimo según la Definición 38 de la página 9.

3.6. Código lineal binario óptimo de parámetros $[120, 9, 56]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{120}$, de parámetros $[120, 9, d]_2$ siguiente.

En principio, las palabras-código tendrían, como ya hemos visto en los casos anteriores, una cabecera con elementos $a_1, \ldots, a_9 \in \mathbb{F}_2$ y, en la cola, todas las sumas posibles de tres y siete elementos de los anteriores con subíndices distintos.

Sin embargo, en este código eliminaremos la cabecera y nos quedaremos solo con la cola.

$$\mathcal{C}_6 = \left\{ (\sum_3 a_i, \sum_7 a_j) \ : \ a_i, a_j \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 9\} \right\} \subset \mathbb{F}_2^{120}$$

La longitud del código es

$$n = \binom{9}{3} + \binom{9}{7} = 84 + 36 = 120$$

Hemos comprobado con MAPLE que la dimensión es $k = 9$ y, por lo tanto, el número de palabras que hay en el código es $2^9 = 512$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla y, a continuación, se detallan las cuentas, que se han realizado de forma similar a los casos anteriores.

n_i	$\sum_3$	$\sum_7$	peso	nº
1	28	28	56	9
2	42	14	56	36
3	46	18	64	84
4	44	20	64	126
5	40	16	56	126
6	38	18	56	84
7	42	22	64	36
8	56	8	64	9
9	84	36	120	1

Cuadro 3.11: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$\binom{8}{2} + \binom{8}{6} = 28 + 28 = 56$$

- Exactamente dos $a_i \neq 0$:

$$2 \cdot \binom{7}{2} + 2 \cdot \binom{7}{6} = 2 \cdot 21 + 2 \cdot 7 = 42 + 14 = 56$$

- Exactamente tres $a_i \neq 0$:

$$\left(1 + 3 \cdot \binom{6}{2}\right) + \left(\binom{6}{4} + 3\right) = (1 + 3 \cdot 15) + (15 + 3) = 46 + 18 = 64$$

- Exactamente cuatro $a_i \neq 0$:

$$\left(\binom{4}{3} + 4 \cdot \binom{5}{2}\right) + \binom{4}{3} \cdot \binom{5}{4} = (4 + 4 \cdot 10) + 4 \cdot 5 = 44 + 20 = 64$$

- Exactamente cinco $a_i \neq 0$:

$$\left(\binom{5}{3} + 5 \cdot \binom{4}{2}\right) + \left(\binom{4}{2} + \binom{5}{3}\right) = (10 + 5 \cdot 6) + (6 + 10) = 40 + 16 = 56$$

- Exactamente seis $a_i \neq 0$:

$$\left(\binom{6}{3} + 6 \cdot \binom{3}{2}\right) + \binom{6}{5} \cdot \binom{3}{2} = (20 + 6 \cdot 3) + 6 \cdot 3 = 38 + 18 = 56$$

- Exactamente siete $a_i \neq 0$:

$$\left(\binom{7}{3}+7\right)+\left(1+\binom{7}{5}\right)=(35+7)+(1+21)=42+22=64$$

- Exactamente ocho $a_i \neq 0$:

$$\binom{8}{3}+\binom{8}{7}=56+8=64$$

- Exactamente nueve $a_i \neq 0$:

$$\binom{9}{3}+\binom{9}{7}=84+36=120$$

El código $\mathcal{C}_6$ se trata, igual que en el caso anterior, de un código *autocomplementario*, puesto que la palabra cuyas componentes son todas uno está en el código.

Observamos esta característica, junto con el curioso hecho de que el código es **autoortogonal** y tiene solo **tres pesos** no nulos.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{56} & = & 255 \\ A_{64} & = & 255 \\ A_{120} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 56$ y se tiene un código de parámetros $[120, 9, 56]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código óptimo.

n/k	**7**	**8**	**9**	**10**	**11**
118	58	56	56	55-56	53-54
119	59	57	56	56	54-55
120	60	58	56	56	54-56
121	60	58	56-57	56	55-56
122	60	58	57-58	56-57	56

Cuadro 3.12: Bounds on the minimum distance of linear codes over $GF(2)$

No obstante, existe un código de parámetros $[119, 10, 56]_2$, el cual tiene la misma distancia mínima pero menor longitud y más palabras-código pues su dimensión es mayor. También existen códigos de parámetros $[118, 9, 56]_2$, $[119, 9, 56]_2$ y $[120, 10, 56]_2$.

3.7. Códigos lineales binarios de parámetros $[26, 6, 11]_2$ y $[20, 6, 8]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{26}$, de parámetros $[26, 6, d]_2$ siguiente.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_6 \in \mathbb{F}_2$ y, en la cola, todas las sumas posibles de tres elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_7 = \left\{ (a_1, a_2, a_3, a_4, a_5, a_6, \sum_3 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 6\} \right\} \subset \mathbb{F}_2^{26}$$

La longitud del código es

$$n = 6 + \binom{6}{3} = 6 + 20 = 26$$

La dimensión es $k = 6$ y, por lo tanto, el número de palabras que hay en el código es $2^6 = 64$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla, y a continuación se detallan las cuentas.

$\boldsymbol{n_i}$	$\sum_{\mathbf{3}}$	**peso**	**nº**
1	10	11	6
2	12	14	15
3	10	13	20
4	8	12	15
5	10	15	6
6	20	26	1

Cuadro 3.13: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{5}{2} = 1 + 10 = 11$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{4}{2} = 2 + 2 \cdot 6 = 14$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(1 + 3 \cdot \binom{3}{2}\right) = 3 + (1 + 3 \cdot 3) = 3 + 10 = 13$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} + 4\right) = 4 + (4 + 4) = 12$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \binom{5}{3} = 5 + 10 = 15$$

- Exactamente seis $a_i \neq 0$:

$$6 + \binom{6}{3} = 6 + 20 = 26$$

El código $\mathcal{C}_7$ es un código *autocomplementario*, puesto que la palabra cuyas componentes son todas uno está en el código. Observamos una bonita estructura en la relación existente entre el número y peso de las palabras-código.

$$\begin{aligned} A_0 &= \binom{6}{0} = 1 \\ A_{11} &= \binom{6}{1} = 6 \\ A_{12} &= \binom{6}{2} = 15 \\ A_{13} &= \binom{6}{3} = 20 \\ A_{14} &= \binom{6}{4} = 15 \\ A_{15} &= \binom{6}{5} = 6 \\ A_{26} &= \binom{6}{6} = 1 \end{aligned}$$

En consecuencia, la distancia mínima del código es $d = 11$ y se tiene un código de parámetros $[26, 6, 11]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que se trata de un código *casi óptimo* pues el código óptimo es un código lineal binario de parámetros $[26, 6, 12]_2$.

Ahora bien, si consideramos el código de parámetros $[26, 6, 11]_2$ sin cabecera, obtenemos un $[20, 6, 8]_2$ código lineal binario, el cual sí es óptimo.

$$\mathcal{C}_{7^*} = \left\{ (\sum_3 a_i) \ : \ a_i \in \mathbb{F}_2, \quad i \in \{1, \ldots, 6\} \right\} \subset \mathbb{F}_2^{20}$$

Las columnas de una matriz generadora del código estarán formadas por todos los vectores que constan de tres unos y el resto ceros sin repetirse ninguno. Es decir, tendrá orden 6×20.

Se ha comprobado con MAPLE que el rango de dicha matriz es 6; por tanto, la dimensión sigue siendo $k = 6$ y no ha disminuido al eliminar la cabecera.

$$G_{6^*} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 1 & 1 & 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 1 \end{bmatrix}$$

Adaptamos la tabla 3.13 para el código de parámetros $[20, 6, 8]_2$.

$\boldsymbol{n_i}$	$\sum_{\mathbf{3}}$	**peso**	**nº**
1	10	10	6
2	12	12	15
3	10	10	20
4	8	8	15
5	10	10	6
6	20	20	1

Cuadro 3.14: Pesos del código y número de palabras

Este código es, como hemos visto en otros casos, *autocomplementario*. Observemos el número de palabras que hay en el código en relación a sus pesos. Advirtamos los pares de pesos complementarios y el hecho de que hay la misma cantidad de palabras de un peso y de su complementario.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_8 & = & 15 \\ A_{10} & = & 32 \\ A_{12} & = & 15 \\ A_{20} & = & 1 \end{array}$$

Veamos a continuación la tabla obtenida en [Grassl].

n/k	4	5	6	7	8
18	8	8	8	7	6
19	9	8	8	8	7
20	10	9	8	8	8
21	10	10	8	8	8
22	11	10	9	8	8
23	12	11	10	9	8
24	12	12	10	10	8
25	12	12	11	10	9
26	13	12	12	11	10
27	14	13	12	12	10
28	14	14	12	12	11

Cuadro 3.15: Bounds on the minimum distance of linear codes over $GF(2)$

Hemos visto que el código de parámetros $[20, 6, 8]_2$ es óptimo. No obstante, existen códigos de parámetros $[18, 6, 8]_2$ y $[19, 6, 8]_2$ con la misma distancia mínima y la misma dimensión que el código anterior, pero con menor longitud. El código de parámetros $[18, 6, 8]_2$ es óptimo con respecto a la Definición 38. También existen códigos de parámetros $[20, 7, 8]_2$ y $[20, 8, 8]_2$ con mayor dimensión.

3.8. Códigos lineales binarios de parámetros $[120, 8, 57]_2$ y $[121, 8, 58]_2$

Se construye un código lineal binario de parámetros $[120, 8, 57]_2$ del siguiente modo: tendremos ocho elementos en la cabecera, de los cuales tomaremos todas las sumas posibles de tres y cinco elementos con subíndices distintos, y estos serán los elementos de la cola.

$$\mathcal{C}_8 = \left\{ (a_1, \ldots, a_8, \sum_3 a_j, \sum_5 a_k) \ : \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, \ldots, 8\} \right\} \subset \mathbb{F}_2^{120}$$

El código tiene longitud

$$n = 8 + \binom{8}{3} + \binom{8}{5} = 8 + 56 + 56 = 120$$

y dimensión $k = 8$, por lo que el código tiene $2^8 = 256$ palabras.

Hallemos la distancia mínima calculando los pesos de todas las palabras no nulas y viendo cuál es el menor. Para ello emplearemos métodos combinatorios.

Veamos los resultados obtenidos en la siguiente tabla. Se precisarán los cálculos realizados posteriormente.

n_i	$\sum_3$	$\sum_5$	peso	nº
1	21	35	57	8
2	30	30	62	28
3	31	25	59	56
4	28	28	60	70
5	25	31	61	56
6	26	26	58	28
7	35	21	63	8
8	56	56	120	1

Cuadro 3.16: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{7}{2} + \binom{7}{4} = 1 + 21 + 35 = 57$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{6}{2} + 2 \cdot \binom{6}{4} = 2 + 2 \cdot 15 + 2 \cdot 15 = 62$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(1 + 3 \cdot \binom{5}{2}\right) + \left(\binom{5}{2} + 3 \cdot \binom{5}{4}\right) = 3 + (1 + 3 \cdot 10) + (10 + 3 \cdot 5) = 59$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} + 4 \cdot \binom{4}{2}\right) + \left(\binom{4}{3} \cdot \binom{4}{2} + 4\right) = 4 + (4 + 4 \cdot 6) + (4 \cdot 6 + 4) = 60$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \left(\binom{5}{3} + 5 \cdot \binom{3}{2}\right) + \left(1 + \binom{5}{3} \cdot \binom{3}{2}\right) = 5 + (10 + 5 \cdot 3) + (1 + 10 \cdot 3) = 61$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(\binom{6}{3} + 6\right) + \left(\binom{6}{5} + \binom{6}{3}\right) = 6 + (20 + 6) + (6 + 20) = 58$$

- Exactamente siete $a_i \neq 0$:

$$7 + \binom{7}{3} + \binom{7}{5} = 7 + 35 + 21 = 63$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \binom{8}{3} + \binom{8}{5} = 8 + 56 + 56 = 120$$

Este código es *autocomplementario*. En consecuencia, hay pares de pesos que suman 120 y hay el mismo número de palabras con un peso que con el otro. Observemos esta propiedad a continuación, destacando la bonita estructura de pesos que tiene el código.

$$\begin{array}{rcccc} A_0 & = & \binom{8}{0} & = & 1 \\ A_{57} & = & \binom{8}{1} & = & 8 \\ A_{58} & = & \binom{8}{2} & = & 28 \\ A_{59} & = & \binom{8}{3} & = & 56 \\ A_{60} & = & \binom{8}{4} & = & 70 \\ A_{61} & = & \binom{8}{5} & = & 56 \\ A_{62} & = & \binom{8}{6} & = & 28 \\ A_{63} & = & \binom{8}{7} & = & 8 \\ A_{120} & = & \binom{8}{8} & = & 1 \end{array}$$

Hemos visto que el peso mínimo es 57, luego el código $\mathcal{C}_8$ tiene parámetros $[120, 8, 57]_2$. Examinando las tablas de [Grassl], hemos comprobado que el código $\mathcal{C}_8$ es, sin embargo, un código *casi óptimo* puesto que existe un código de parámetros $[120, 8, 58]_2$. La construcción dada en [Grassl] de este último código se ha obtenido a partir de una matriz generadora proporcionada por I.Boukliev.

Ahora consideremos el código extendido $\bar{\mathcal{C}_8}$, que consiste en añadir a cada palabra un símbolo de control de paridad en última posición. De este modo, todas las palabras tienen peso par y obtendremos un código de parámetros $[121, 8, 58]_2$, el cual es un código óptimo. Veamos, pues, la relación entre los pesos y el número de palabras del código.

$$\begin{array}{rcc} A_0 & = & 1 \\ A_{58} & = & 36 \\ A_{60} & = & 126 \\ A_{62} & = & 84 \\ A_{64} & = & 8 \\ A_{120} & = & 1 \end{array}$$

Notemos en la siguiente tabla de [Grassl] que el código que cumple las dos definiciones de óptimo vistas es el código de parámetros $[120, 8, 58]_2$. Sin embargo, como hemos mencionado, el código extendido que hemos construido es óptimo.

n/k	6	7	8	9	10
118	59	58	56	56	55-56
119	60	59	57	56	56
120	60	60	58	56	56
121	60	60	58	56-57	56
122	61	60	58	57-58	56-57
123	62	61	59	58	56-58

Cuadro 3.17: Bounds on the minimum distance of linear codes over $GF(2)$

3.9. Códigos lineales binarios de parámetros $[171, 9, 72]_2$ y $[135, 9, 63]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{171}$, de parámetros $[171, 9, d]_2$ siguiente.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_9 \in \mathbb{F}_2$; y en la cola todas las sumas posibles de cinco y siete elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_9 = \left\{(a_1, \ldots, a_9, \sum_5 a_j, \sum_7 a_k) \ : \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, \ldots, 9\}\right\} \subset \mathbb{F}_2^{171}$$

La longitud del código es

$$n = 9 + \binom{9}{5} + \binom{9}{7} = 9 + 126 + 36 = 171$$

La dimensión es $k = 9$ y el número de palabras que hay en el código es $2^9 = 512$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla y, a continuación, se detallan las cuentas.

n_i	$\sum_5$	$\sum_7$	peso	nº
1	70	28	99	9
2	70	14	86	36
3	60	18	81	84
4	60	20	84	126
5	66	16	87	126
6	66	18	90	84
7	56	22	85	36
8	56	8	72	9
9	126	36	171	1

Cuadro 3.18: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{8}{4} + \binom{8}{6} = 1 + 70 + 28 = 99$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{7}{3} + 2 \cdot \binom{7}{6} = 2 + 2 \cdot 35 + 2 \cdot 7 = 86$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(\binom{6}{2} + 3 \cdot \binom{6}{4} \right) + \left(\binom{6}{4} + 3 \right) = 3 + (15 + 3 \cdot 15) + (15 + 3) = 81$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} \cdot \binom{5}{2} + 4 \cdot \binom{5}{4} \right) + \binom{4}{3} \cdot \binom{5}{4} = 4 + (4 \cdot 10 + 4 \cdot 5) + 4 \cdot 5 = 84$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \left(1 + \binom{5}{3} \cdot \binom{4}{2} + 5 \right) + \left(\binom{4}{2} + \binom{5}{3} \right) = 5 + (1 + 10 \cdot 6 + 5) + (6 + 10) = 87$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(\binom{6}{5} + \binom{6}{3} \cdot \binom{3}{2} \right) + \binom{6}{5} \cdot \binom{3}{2} = 6 + (6 + 20 \cdot 3) + 6 \cdot 3 = 90$$

- Exactamente siete $a_i \neq 0$:

$$7 + \left(\binom{7}{5} + \binom{7}{3} \right) + \left(1 + \binom{7}{5} \right) = 7 + (21 + 35) + (1 + 21) = 85$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \binom{8}{5} + \binom{8}{7} = 8 + 56 + 8 = 72$$

- Exactamente nueve $a_i \neq 0$:

$$9 + \binom{9}{5} + \binom{9}{7} = 9 + 126 + 36 = 171$$

El código $\mathcal{C}_9$ también se trata de un código *autocomplementario*, puesto que la palabra cuyas componentes son todas uno está en el código. Observamos dicho rasgo en el número y peso de las palabras-código. El peso de una palabra y su complementaria suman 171, luego debe haber parejas de pesos que sumen dicha cifra.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{72} & = & 9 \\ A_{81} & = & 84 \\ A_{84} & = & 126 \\ A_{85} & = & 36 \\ A_{86} & = & 36 \\ A_{87} & = & 126 \\ A_{90} & = & 84 \\ A_{99} & = & 9 \\ A_{171} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 72$ y se tiene un código de parámetros $[171, 9, 72]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], se observa que existe un código lineal binario de parámetros $[171, 9, 81]_2$. Sin embargo, para dichas longitud y dimensión, la cota para la distancia mínima es 82. Esto quiere decir que el código óptimo podría tener distancia mínima 81, ya conocido, o distancia mínima 82 para la cual aún no se conoce ningún código. Se trata de un problema abierto. La notación que se usa en las tablas de [Grassl] para señalar este hecho es 81-82.

El código de parámetros $[171, 9, 72]_2$ no tiene gran interés, pero si eliminamos los elementos de la cola correspondientes a las sumas de siete elementos, obtenemos un $[135, 9, 63]_2$ código lineal binario, el cual es *casi óptimo*, siendo el código óptimo un $[135, 9, 64]_2$ código lineal binario.

$$\mathcal{C}_{9^*} = \left\{ (a_1, \ldots, a_9, \sum_5 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 9\} \right\} \subset \mathbb{F}_2^{135}$$

Adaptando la tabla de pesos del código y número de palabras 3.18 obtenemos lo siguiente:

$\boldsymbol{n_i}$	$\sum_{\mathbf{5}}$	**peso**	**nº**
1	70	71	9
2	70	72	36
3	60	63	84
4	60	64	126
5	66	71	126
6	66	72	84
7	56	63	36
8	56	64	9
9	126	135	1

Cuadro 3.19: Pesos del código y número de palabras

La palabra cuyas componentes son todas uno está en el código $\mathcal{C}_{9^*}$, luego es *autocomplementario*. Observemos dicha peculiaridad en la relación entre los pesos y el número de palabras del código.

$$\begin{aligned} A_0 &= 1 \\ A_{63} &= 120 \\ A_{64} &= 135 \\ A_{71} &= 135 \\ A_{72} &= 120 \\ A_{135} &= 1 \end{aligned}$$

El código $\mathcal{C}_{9^*}$ extendido, resultado de añadir a $\mathcal{C}_{9^*}$ un bit de paridad, tiene parámetros $[136, 9, 64]_2$ y es un código óptimo, como hemos comprobado recurriendo a [Grassl].

Notemos que se trata de un ***three-weight code*** y cada uno de estos pesos son *divisibles entre cuatro*, el código $\mathcal{C}_{9^*}$ extendido es un código **autoortogonal**.

$$\begin{aligned} A_0 &= 1 \\ A_{64} &= 255 \\ A_{72} &= 255 \\ A_{136} &= 1 \end{aligned}$$

3.10. Códigos lineales binarios de parámetros $[250, 10, 114]_2$ y $[240, 10, 112]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{250}$, de parámetros $[250, 10, d]_2$ dado a continuación.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_{10} \in \mathbb{F}_2$ y, en la cola, todas las sumas posibles de tres y siete elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_{10} = \left\{ (a_1, \ldots, a_{10}, \sum_3 a_j, \sum_7 a_k) \ : \ a_i \in \mathbb{F}_2, \quad i, j, k \in \{1, \ldots, 10\} \right\} \subset \mathbb{F}_2^{250}$$

La longitud del código es

$$n = 10 + \binom{10}{3} + \binom{10}{7} = 10 + 120 + 120 = 250$$

La dimensión es $k = 10$ y, por lo tanto, el número de palabras que hay en el código es $2^{10} = 1024$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla y, a continuación, se detallan las cuentas.

$\boldsymbol{n_i}$	$\sum_{\boldsymbol{3}}$	$\sum_{\boldsymbol{7}}$	**peso**	**nº**
1	36	84	121	10
2	56	56	114	45
3	64	56	123	120
4	64	64	132	210
5	60	60	125	252
6	56	56	118	210
7	56	64	127	120
8	64	64	136	45
9	84	36	129	10
10	120	120	250	1

Cuadro 3.20: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{9}{2} + \binom{9}{6} = 1 + 36 + 84 = 121$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{8}{2} + 2 \cdot \binom{8}{6} = 2 + 2 \cdot 28 + 2 \cdot 28 = 114$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(1 + 3 \cdot \binom{7}{2}\right) + \left(\binom{7}{4} + 3 \cdot \binom{7}{6}\right) = 3 + (1 + 3 \cdot 21) + (35 + 3 \cdot 7) = 123$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} + 4 \cdot \binom{6}{2}\right) + \left(\binom{4}{3} \cdot \binom{6}{4} + 4\right) = 4 + (4 + 4 \cdot 15) + (4 \cdot 15 + 4) = 132$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \left(\binom{5}{3} + 5 \cdot \binom{5}{2}\right) + \left(\binom{5}{2} + \binom{5}{3} \cdot \binom{5}{4}\right) = 5 + (10 + 5 \cdot 10) + (10 + 10 \cdot 5) = 125$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(\binom{6}{3} + 6 \cdot \binom{4}{2}\right) + \left(\binom{6}{5} \cdot \binom{4}{2} + \binom{6}{3}\right) = 6 + (20 + 6 \cdot 6) + (6 \cdot 6 + 20) = 118$$

- Exactamente siete $a_i \neq 0$:

$$7 + \left(\binom{7}{3} + 7 \cdot \binom{3}{2}\right) + \left(1 + \binom{7}{5} \cdot \binom{3}{2}\right) = 7 + (35 + 7 \cdot 3) + (1 + 21 \cdot 3) = 127$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \left(\binom{8}{3} + 8\right) + \left(\binom{8}{7} + \binom{8}{5}\right) = 8 + (56 + 8) + (8 + 56) = 136$$

- Exactamente nueve $a_i \neq 0$:

$$9 + \binom{9}{3} + \binom{9}{7} = 9 + 84 + 36 = 129$$

- Exactamente diez $a_i \neq 0$:

$$10 + \binom{10}{3} + \binom{10}{7} = 10 + 120 + 120 = 250$$

El código $\mathcal{C}_{10}$ también se trata de un código *autocomplementario*. Observamos dicho rasgo en el número y peso de las palabras-código. El peso de una palabra y su complementaria suman 250, luego debe haber parejas de pesos que sumen dicha cifra.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{114} & = & 45 \\ A_{118} & = & 210 \\ A_{121} & = & 10 \\ A_{123} & = & 120 \\ A_{125} & = & 252 \\ A_{127} & = & 120 \\ A_{129} & = & 10 \\ A_{132} & = & 210 \\ A_{136} & = & 45 \\ A_{250} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 114$ y se tiene un código de parámetros $[250, 10, 114]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], observamos que existe un código lineal binario de parámetros $[250, 10, 120]_2$ y que la cota para la distancia mínima es 122.

Si consideramos el código de parámetros $[250, 10, 114]_2$ sin cabecera, obtenemos un $[240, 10, 112]_2$ código lineal binario, el cual está cerca de ser un código óptimo, siendo el código óptimo un código de parámetros $[240, 10, 114]_2$. Para esos parámetros de longitud y dimensión, la cota para la distancia mínima es 116.

$$\mathcal{C}_{10^*} = \left\{ (\sum_{3} a_i, \sum_{7} a_j) \ : \ a_i, a_j \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 10\} \right\} \subset \mathbb{F}_2^{240}$$

Una matriz generadora del código tendrá por columnas a todos los vectores con tres unos y el resto ceros, y todos los vectores con siete unos y las demás componentes nulas. Hemos comprobado con MAPLE que el rango de dicha matriz es 10 y, por tanto, la dimensión del código no ha disminuido con respecto al código del que partíamos, $k = 10$. Esta matriz tendrá orden 10×240.

$$G_{10^*} = \left[\begin{array}{cccccccccccc|ccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 1 & 1 & 0 & \cdots & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 1 & \cdots & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 1 & 0 & 0 & 0 & 1 & 0 & \cdots & 1
\end{array}\right]$$

A continuación exponemos la tabla adaptada a partir de la tabla 3.20.

n_i	$\sum_3$	$\sum_7$	**peso**	**nº**
1	36	84	120	10
2	56	56	112	45
3	64	56	120	120
4	64	64	128	210
5	60	60	120	252
6	56	56	112	210
7	56	64	120	120
8	64	64	128	45
9	84	36	120	10
10	120	120	240	1

Cuadro 3.21: Pesos del código y número de palabras

Veamos la relación entre los pesos de las palabras del código y el número de estas que tienen dichos pesos. Adicionalmente, observemos que todos los pesos son *divisibles entre cuatro*. El código $\mathcal{C}_{10^*}$ es **autoortogonal**.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{112} & = & 255 \\ A_{120} & = & 512 \\ A_{128} & = & 255 \\ A_{240} & = & 1 \end{array}$$

Fijémonos en el pequeño número de pesos que tiene el código. Además, podemos observar que se trata de un código *autocomplementario*, siendo los pares de pesos complementarios los siguientes: 0 y 240, 112 y 128; y, por último 120 es complementario de sí mismo. El número de palabras de un peso y de su peso complementario, como ya habíamos comentado anteriormente, es el mismo.

3.11. Código lineal binario de parámetros $[130, 9, 58]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{130}$, de parámetros $[130, 9, d]_2$ dado seguidamente.

En la cabecera de las palabras del código, se colocan los elementos $a_1, \ldots, a_{10} \in \mathbb{F}_2$, con el detalle de que $a_{10} = a_1 + \cdots + a_9$; y en la cola todas las sumas posibles de siete elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_{11} = \left\{ (a_1, \ldots, a_9, a_{10} = a_1 + \cdots + a_9, \sum_7 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 10\} \right\} \subset \mathbb{F}_2^{130}$$

La longitud del código es

$$n = 10 + \binom{10}{7} = 10 + 120 = 130$$

La dimensión es $k = 9$ y, por lo tanto, el número de palabras que hay en el código es $2^9 = 512$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Como ya vimos en un caso anterior, solo hay una cantidad par de elementos a_i distintos de cero en la cabecera, lo que simplifica los cálculos del peso.

Los resultados se muestran en la siguiente tabla y, a continuación, se detallan las cuentas.

$\boldsymbol{n_i}$	$\sum_{\mathbf{7}}$	**peso**	**nº**
2	56	58	45
4	64	68	210
6	56	62	210
8	64	72	45
10	120	130	1

Cuadro 3.22: Pesos del código y número de palabras

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{8}{6} = 2 + 2 \cdot 28 = 58$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} \cdot \binom{6}{4} + 4 \right) = 4 + (4 \cdot 15 + 4) = 68$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(\binom{6}{5} \cdot \binom{4}{2} + \binom{6}{3} \right) = 6 + (20 + 6 \cdot 6) = 62$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \left(\binom{8}{7} + \binom{8}{5} \right) = 8 + (8 + 56) = 72$$

- Exactamente diez $a_i \neq 0$:

$$10 + \binom{10}{7} = 10 + 120 = 130$$

Ya explicamos en un caso similar cómo hallar el número de palabras-código. El número de palabras que hay en el código con exactamente j elementos a_i distintos de cero para cada $j \in \{2, 4, 6, 8, 10\}$ es $\left(\binom{k}{j-1} + \binom{k}{j} \right)$. No olvidemos que en todo código lineal está la palabra nula.

El código $\mathcal{C}_{11}$ se trata igualmente de un código *autocomplementario*, puesto que la palabra cuyas componentes son todas uno está en el código. Observamos dicha característica en el número y peso de las palabras-código. El peso de una palabra y su complementaria suman 130, luego debe haber parejas de pesos que sumen dicha cifra.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{58} & = & 45 \\ A_{62} & = & 210 \\ A_{68} & = & 210 \\ A_{72} & = & 45 \\ A_{130} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 58$ y se tiene un código con parámetros $[130, 9, 58]_2$.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [Grassl], el código óptimo tiene parámetros $[130, 9, 62]_2$.

3.12. Código lineal binario de parámetros $[262, 10, 120]_2$

Sea el código lineal binario, subespacio vectorial de $\mathbb{F}_2^{262}$, de parámetros $[262, 10, d]_2$ siguiente.

En la cabecera de las palabras del código se colocan los elementos $a_1, \ldots, a_{10} \in \mathbb{F}_2$ y, en la cola, todas las sumas posibles de cinco elementos de los anteriores con subíndices distintos.

$$\mathcal{C}_{12} = \left\{ (a_1, \ldots, a_{10}, \sum_5 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 10\} \right\} \subset \mathbb{F}_2^{262}$$

La longitud del código es

$$n = 10 + \binom{10}{5} = 10 + 252 = 262$$

La dimensión es $k = 10$ y, por lo tanto, el número de palabras que hay en el código es $2^{10} = 1024$.

Para hallar la distancia mínima del código, se calculan los pesos de todas las palabras-código con métodos combinatorios.

Los resultados se muestran en la siguiente tabla y, a continuación, se detallan las cuentas.

n_i	$\sum_5$	peso	nº
1	126	127	10
2	140	142	45
3	126	129	120
4	120	124	210
5	126	131	252
6	132	138	210
7	126	133	120
8	112	120	45
9	126	135	10
10	252	262	1

Cuadro 3.23: Pesos del código y número de palabras

- Exactamente un $a_i \neq 0$:

$$1 + \binom{9}{4} = 1 + 126 = 127$$

- Exactamente dos $a_i \neq 0$:

$$2 + 2 \cdot \binom{8}{4} = 2 + 2 \cdot 70 = 142$$

- Exactamente tres $a_i \neq 0$:

$$3 + \left(\binom{7}{2} + 3 \cdot \binom{7}{4} \right) = 3 + (21 + 3 \cdot 35) = 129$$

- Exactamente cuatro $a_i \neq 0$:

$$4 + \left(\binom{4}{3} \cdot \binom{6}{2} + 4 \cdot \binom{6}{4} \right) = 4 + (4 \cdot 15 + 4 \cdot 15) = 124$$

- Exactamente cinco $a_i \neq 0$:

$$5 + \left(1 + \binom{5}{3} \cdot \binom{5}{2} + 5 \cdot \binom{5}{4} \right) = 5 + (1 + 10 \cdot 10 + 5 \cdot 5) = 131$$

- Exactamente seis $a_i \neq 0$:

$$6 + \left(\binom{6}{5} + \binom{6}{3} \cdot \binom{4}{2} + 6 \right) = 6 + (6 + 20 \cdot 6 + 6) = 138$$

- Exactamente siete $a_i \neq 0$:

$$7 + \left(\binom{7}{5} + \binom{7}{3} \cdot \binom{3}{2} \right) = 7 + (21 + 35 \cdot 3) = 133$$

- Exactamente ocho $a_i \neq 0$:

$$8 + \left(\binom{8}{5} + \binom{8}{3} \right) = 8 + (56 + 56) = 120$$

- Exactamente nueve $a_i \neq 0$:

$$9 + \binom{9}{5} = 9 + 126 = 135$$

- Exactamente diez $a_i \neq 0$:

$$10 + \binom{10}{5} = 10 + 252 = 262$$

El código $\mathcal{C}_{12}$ se trata de un código *autocomplementario*. Observamos dicha propiedad en el número y peso de las palabras-código. El peso de una palabra y su complementaria suman 262, luego debe haber parejas de pesos que sumen dicha cifra.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{120} & = & 45 \\ A_{124} & = & 210 \\ A_{127} & = & 10 \\ A_{129} & = & 120 \\ A_{131} & = & 252 \\ A_{133} & = & 120 \\ A_{135} & = & 10 \\ A_{138} & = & 210 \\ A_{142} & = & 45 \\ A_{262} & = & 1 \end{array}$$

Como consecuencia, la distancia mínima del código es $d = 120$ y se tiene un $[262, 10, 120]_2$ código lineal binario.

Examinando la tabla correspondiente a códigos lineales binarios óptimos en [SchSch], se observa que existe un código $[262, 10, 126]_2$. Sin embargo, dados esos parámetros de longitud y dimensión, la cota superior para la distancia mínima es 128.

Nuestro código de parámetros $[262, 10, 120]_2$ no tiene especial interés en cuanto a códigos óptimos; sin embargo, se trata de un código de gran longitud. En un código de tales características, generalmente no seríamos capaces de hacer los cálculos a mano para hallar sus pesos, su distancia mínima y otros parámetros. De hecho, hemos tenido que acudir a la tabla de [SchSch] puesto que en la tabla de [Grassl] no se muestran códigos lineales binarios con longitud mayor de 256.

En resumen, la naturaleza elemental de estos códigos permitirá su utilización como ejemplos en la asignatura de Códigos Correctores. Además, estas técnicas pueden proporcionar códigos con longitudes mucho mayores a las que hemos visto, v.g., el código

$$\mathcal{C} = \left\{ (a_1, \ldots, a_{21}, \sum_{17} a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 21\} \right\}$$

es un código lineal binario de parámetros $[5985, 21, d]_2$.

Capítulo 4

Construcciones sencillas basadas en el código simplex binario

En este capítulo expondremos otros métodos para obtener códigos óptimos. Seguiremos utilizando las definiciones de código óptimo y código *casi óptimo* presentadas en el capítulo anterior.

El uso de estas técnicas tan sencillas no resulta siempre fructífero, aunque en algunos casos sí hemos obtenido los resultados buscados. Compararemos estos resultados con los datos de las tablas de [Grassl] y [SchSch].

Una vez más, destacaremos el hecho de que la baja tasa de transmisión de información, debida a la pequeña dimensión, hace que estos códigos sean poco prácticos. A pesar de ello, la facilidad con la que se realizan los cálculos sigue siendo un rasgo significativo.

Como ya hemos visto, algunas características notables de estos códigos son el pequeño número de pesos, dos o tres pesos no nulos y la *divisibilidad* de estos pesos entre cuatro, lo cual implica la condición de autoortogonalidad.

Se han obtenido códigos lineales binarios con los siguientes parámetros:

- Códigos óptimos

$$[94, 7, 46]_2,\ \ [95, 6, 48]_2,\ \ [119, 6, 60]_2,\ \ [190, 7, 95]_2,\ \ [191, 7, 96]_2,\ \ [254, 9, 126]_2 \tag{4.1}$$

- Códigos autoortogonales con dos pesos no nulos

$$[95, 6, 48]_2,\ \ [119, 6, 60]_2,\ \ [191, 7, 96]_2$$

Comenzaremos exponiendo la noción de código simplex binario que nos será útil en lo que sigue.

Un código simplex binario $\mathcal{S}_r$ es un código lineal binario de longitud $2^r - 1$ y dimensión r, cuya matriz generadora de orden $r \times (2^r - 1)$ tiene por columnas a todos vectores no nulos de $\mathbb{F}_2^r$, es decir, es la matriz de control del código de Hamming $\mathcal{H}_r$. El código $\mathcal{S}_r$ es el código dual del código de Hamming $\mathcal{H}_r$.

Las columnas de la matriz generadora corresponden a todos los puntos del espacio proyectivo $(r-1)$-dimensional sobre el cuerpo finito $\mathbb{F}_2$.

La distribucion de pesos del código simplex es

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{2^{r-1}} & = & 2^r - 1 \end{array}$$

Todas las palabras no nulas de $\mathcal{S}_r$ tienen peso 2^{r-1}. Es un *constant-weight code*.

$\mathcal{S}_r$ tiene parámetros $[2^r-1, r, 2^{r-1}]_2$

El código simplex binario $\mathcal{S}_r$ es un código recortado del código Reed-Muller binario $\mathcal{RM}(1,r)$, código con parámetros $[2^r, 1+r, 2^{r-1}]_2$. Se toman todas las palabras de $\mathcal{RM}(1,r)$ cuya última coordenada sea cero y se suprime dicha coordenada; se obtiene el código $\mathcal{S}_r$.

El código simplex binario alcanza la cota de Griesmer (2.3) con igualdad, y, por lo tanto, es un código óptimo.

El código simplex binario aumentado, añadiendo la palabra cuyas componentes son todas uno, tiene parámetros $[2^r-1, r+1, 2^{r-1}-1]_2$.

A continuación mostraremos una de las técnicas utilizadas para hallar varios códigos de los dados en (4.1). Partimos de dos códigos lineales binarios, pudiendo ser ambos el mismo, y llegamos a otro código lineal binario de la siguiente forma: las palabras del nuevo código consisten en una palabra del primer código seguida de una palabra del segundo código y, como últimas coordenadas, todas las posibles sumas de un elemento de la primera palabra con un elemento de la segunda.

Esta técnica funciona con un código simplex binario o un código similar y probablemente no con otros códigos puesto que estos códigos tienen gran capacidad correctora y todas sus palabras no nulas tienen el mismo peso. Aun teniendo una tasa de transmisión pobre, son buenas *piezas* para construir otros códigos.

Sea $\mathcal{C}_1 \subseteq \mathbb{F}_2^{n_1}$ un código de parámetros $[n_1, k_1, d_1]_2$ y sea el código $\mathcal{C}_2 \subseteq \mathbb{F}_2^{n_2}$ de parámetros $[n_2, k_2, d_2]_2$. Definimos el código $\mathcal{C}_3$ de la siguiente forma.

$$\mathcal{C}_3 = \mathcal{C}_1 \boxplus \mathcal{C}_2 = \Big\{ (u_1, \ldots, u_{n_1}, v_1, \ldots, v_{n_2},\ u_i + v_j\ ) \ : \\ (u_1, \ldots, u_{n_1}) \in \mathcal{C}_1,\ \ (v_1, \ldots, v_{n_2}) \in \mathcal{C}_2,\ \ 1 \le i \le n_1,\ \ 1 \le j \le n_2 \Big\} \quad (4.2)$$

Observamos que la longitud del código $\mathcal{C}_3$ es igual a

$$n_3 = n_1 + n_2 + n_1 \cdot n_2$$

y la dimensión $k_3 = k_1 + k_2$ como subespacio de $\mathbb{F}_2^{n_3}$, ya que hay $k_1 + k_2$ parámetros libres y el resto de coordenadas dependen linealmente de las $k_1 + k_2$ anteriores. La distancia mínima no está, en principio, determinada.

El código $\mathcal{C}_3$ tiene parámetros $[n_1 + n_2 + n_1 \cdot n_2, k_1 + k_2, d_3]_2$.

Veamos un pequeño teorema para códigos simplex binarios.

Teorema 51 *Sean $\mathcal{S}_r$ y $\mathcal{S}_m$ códigos simplex binarios, entonces $\mathcal{S}_r \boxplus \mathcal{S}_m$ es el código simplex binario $\mathcal{S}_{r+m}$.*

Demostración: Los códigos $\mathcal{S}_r$ y $\mathcal{S}_m$ tienen parámetros $[2^r-1, r, 2^{r-1}]_2$ y $[2^m-1, m, 2^{m-1}]_2$, respectivamente. Luego el código $\mathcal{S}_r \boxplus \mathcal{S}_m$ tiene longitud

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

y dimensión $r + m$.

Veamos cual es su distancia mínima. Todas las palabras no nulas de $\mathcal{S}_r$ tienen peso 2^{r-1} y todas las palabras no nulas de $\mathcal{S}_m$ tienen peso 2^{m-1}. Luego en el código $\mathcal{S}_r \boxplus \mathcal{S}_m$ hay tres tipos de palabras no nulas: las palabras formadas por la palabra nula del primer código y una palabra no nula del segundo; las palabras formadas por una palabra no nula del primer código y por la palabra nula del segundo; y, por último, las palabras constituidas por ambas palabras no nulas.

En el primer caso, el peso sería

$$2^{r-1} + 0 + 2^{r-1}(2^m - 1) = 2^{(r+m)-1}$$

en el segundo caso

$$0 + 2^{m-1} + 2^{m-1}(2^r - 1) = 2^{(r+m)-1}$$

y en el tercer caso

$$2^{r-1} + 2^{m-1} + \left(2^{r-1}(2^m - 1 - 2^{m-1}) + 2^{m-1}(2^r - 1 - 2^{r-1})\right) = 2^{(r+m)-1}$$

Es decir, todas las palabras no nulas de $\mathcal{S}_r \boxplus \mathcal{S}_m$ tienen el mismo peso, $2^{(r+m)-1}$. En conclusión, el código tiene parámetros $[2^{r+m} - 1, r + m, 2^{(r+m)-1}]_2$. Es el código simplex $\mathcal{S}_{r+m}$.

□

Daremos ahora una serie de códigos obtenidos usando el procedimiento dado en (4.2).

4.1. Código lineal binario óptimo de parámetros $[95, 6, 48]_2$

Sea el código simplex binario $\mathcal{S}_3$, cuyos parámetros son $[7, 3, 4]_2$. Sabemos que todas las palabras no nulas de $\mathcal{S}_3$ tienen peso 4.

Sea el código lineal binario $\mathcal{C}$ de parámetros $[11, 3, 6]_2$ con matriz generadora

$$G = \left[\begin{array}{ccc|ccc|ccc|cc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

El código $\mathcal{C}$ es el subespacio vectorial de $\mathbb{F}_2^{11}$ siguiente

$$\mathcal{C} = \Big\{(a_1, a_2, a_3, a_1, a_2, a_3, a_1{+}a_2, a_1{+}a_3, a_2{+}a_3, a_1{+}a_2{+}a_3, a_1{+}a_2{+}a_3) : a_i \in \mathbb{F}_2, i \in \{1, 2, 3\}\Big\} \subset \mathbb{F}_2^{11}$$

Calculando a mano los pesos de las palabras del código, se observa que el código $\mathcal{C}$ solo tiene palabras de pesos 0, 6 y 8. La relación de los pesos con el número de palabras del código se muestra a continuación.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_6 & = & 6 \\ A_8 & = & 1 \end{array}$$

Construimos ahora el código $\mathcal{S}_3 \boxplus \mathcal{C}$ definido como en (4.2) y obtenemos el código $\mathcal{B}$.

$$\mathcal{B} = \mathcal{S}_3 \boxplus \mathcal{C} = \Big\{ (u_1, \ldots, u_7, v_1, \ldots, v_{11},\ u_i + v_j\ ) \ :\ (u_1, \ldots, u_7) \in \mathcal{S}_3, (v_1, \ldots, v_{11}) \in \mathcal{C} \Big\}$$

El nuevo código tiene longitud

$$n = 7 + 11 + 7 \cdot 11 = 95$$

y dimensión $k = 3 + 3 = 6$.

Para hallar la distancia mínima fijaremos nuestra atención en los pesos de las palabras de los códigos que hemos empleado para construir el código $\mathcal{B}$; combinando palabras de distintos pesos hallaremos los pesos de las palabras del código $\mathcal{B}$.

La siguiente tabla muestra las combinaciones de pesos de los dos códigos y el peso de las palabras del nuevo código en tales casos. En la primera columna se muestran los pesos de las palabras del código $\mathcal{S}_3$; en la segunda columna, los pesos de las palabras del código $\mathcal{C}$; y, finalmente, en la tercera columna se muestra el peso de las palabras del código $\mathcal{B}$, que son producto de combinar las palabras con dichos pesos de los códigos anteriores.

u_i	v_i	**peso**
0	6	48
0	8	64
4	0	48
4	6	48
4	8	48

Cuadro 4.1: Pesos del código

Las cuentas se detallan seguidamente.

Como ya hemos comentado, todas las palabras no nulas del código $\mathcal{S}_3$ tienen peso 4 y el código $\mathcal{C}$ tiene palabras de pesos 0, 6 y 8.

- Si tomamos la palabra de peso nulo del primer código y la combinamos con la palabra de peso nulo del segundo código, obtenemos la palabra de peso nulo; si la combinamos con una palabra de peso 6 del segundo código, el peso de la palabra obtenida será

  $$0 + 6 + 6 \cdot 7 = 48$$

  puesto que tenemos peso 0 de la palabra del primer código, peso 6 de la palabra del segundo código y, para la parte final de la palabra, la combinación de todas las posiciones distintas de cero de la palabra del segundo código con todas las posiciones nulas de la palabra del primer código; si combinamos la palabra nula del primer código con la palabra de peso 8 del segundo código obtendríamos peso

  $$0 + 8 + 8 \cdot 7 = 64$$

  para la palabra resultante.

- Si tomamos una palabra de peso 4 del primer código y la combinamos con palabras de distintos pesos del segundo código, obtendremos lo siguiente: si la combinamos con la palabra de peso 0, tendremos peso

  $$4 + 0 + 4 \cdot 11 = 48$$

si la combinamos con una palabra de peso 6, tendremos peso

$$4 + 6 + 4 \cdot (11 - 6) + 6 \cdot (7 - 4) = 48$$

y si la combinamos con la palabra de peso 8, el peso resultante será

$$4 + 8 + 4 \cdot (11 - 8) + 8 \cdot (7 - 4) = 48$$

Veamos la relación entre los pesos y el número de palabras del código.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{48} & = & 62 \\ A_{64} & = & 1 \end{array}$$

Advertimos que las palabras no nulas del código $\mathcal{B}$ pueden tomar **dos pesos** y que casi todas las palabras tienen peso 48, lo cual es una característica agradable. Todos los pesos del código son *divisibles entre cuatro*, esto es, $\mathcal{B}$ es un código **autoortogonal**.

Contrastando con las tablas de [Grassl], nótese que el código de parámetros $[95, 6, 48]_2$ se trata de un código óptimo. Además, también es óptimo considerando la definición de código óptimo dada en la Definición 38.

n/k	**4**	**5**	**6**	**7**	**8**
93	48	48	46	46	44
94	49	48	47	46	44
95	50	48	48	47	45
96	50	48	48	48	46
97	51	48	48	48	46

Cuadro 4.2: Bounds on the minimum distance of linear codes over $GF(2)$

4.2. Código lineal binario óptimo de parámetros $[119, 6, 60]_2$

Tomemos, de nuevo, el código simplex binario $\mathcal{S}_3$, que tiene parámetros $[7, 3, 4]_2$, y llamemos G a una matriz generadora de este código. Sea el código lineal binario $\mathcal{C}$ cuya matriz generadora es la matriz $[G|G]$. El código $\mathcal{C}$ tiene parámetros $[14, 3, 8]_2$.

Construyamos ahora siguiendo el procedimiento dado en (4.2) el código $\mathcal{B} = \mathcal{S}_3 \boxplus \mathcal{C}$

$$\mathcal{B} = \mathcal{S}_3 \boxplus \mathcal{C} = \left\{ (u_1, \ldots, u_7, v_1, \ldots, v_{14},\ u_i + v_j\ ) \ :\ (u_1, \ldots, u_7) \in \mathcal{S}_3, (v_1, \ldots, v_{14}) \in \mathcal{C} \right\}$$

El código $\mathcal{B}$ tiene longitud

$$n = 7 + 14 + 7 \cdot 14 = 119$$

y longitud $k = 3 + 3 = 6$. El número de palabras del código es, por lo tanto, $2^6 = 64$.

Hallaremos la distancia mínima del código $\mathcal{B}$ como hemos hecho en el caso anterior: combinaremos palabras de distintos pesos de los códigos $\mathcal{S}_3$ y $\mathcal{C}$ para hallar todos los pesos posibles del código $\mathcal{B}$;

una vez hecho esto, veremos cuál es el peso mínimo que, como ya sabemos, coincide con la distancia mínima. Notemos que ambos códigos son *constant-weight codes*, es decir, todas las palabras no nulas tienen el mismo peso, peso 4 en el caso de $\mathcal{S}_3$ y peso 8 en las palabras del código $\mathcal{C}$.

Así pues, formaremos la tabla con todas las combinaciones y pesos posibles. A continuación se describen las cuentas.

u_i	v_i	peso
0	8	64
4	0	60
4	8	60

Cuadro 4.3: Pesos del código

- Si combinamos las dos palabras de peso nulo, la palabra resultante tendrá peso nulo; si combinamos la palabra de peso nulo del primer código con una palabra de peso 8 del segundo código, el peso de la palabra obtenida será

$$0 + 8 + 8 \cdot 7 = 64$$

- Si tomamos una palabra de peso 4 del primer código y la combinamos con palabras de distintos pesos del segundo código, obtendremos lo siguiente: si la combinamos con la palabra de peso 0, tendremos peso

$$4 + 0 + 4 \cdot 14 = 60$$

y si la combinamos con la palabra de peso 8, el peso resultante será

$$4 + 8 + 4 \cdot (14 - 8) + 8 \cdot (7 - 4) = 60$$

Seguidamente se muestra la relación que existe entre los pesos y el número de palabras del código.

$$\begin{aligned} A_0 &= 1 \\ A_{60} &= 56 \\ A_{64} &= 7 \end{aligned}$$

De nuevo, se trata de un código **autoortogonal** con solo **dos pesos** no nulos.

La distancia mínima es 60 y, por esa razón, el código que hemos construido tiene parámetros $[119, 6, 60]_2$. Examinando la tabla de [Grassl] que se muestra a continuación, advertimos que dicho código es óptimo; también lo es en el sentido de la Definición 38.

n/k	4	5	6	7	8
117	62	60	58	58	56
118	62	60	59	58	56
119	63	60	60	59	57
120	64	61	60	60	58
121	64	62	60	60	58

Cuadro 4.4: Bounds on the minimum distance of linear codes over $GF(2)$

4.3. Código lineal binario óptimo de parámetros $[191, 7, 96]_2$

Sea $\mathcal{C}$ el código lineal binario de parámetros $[11, 3, 6]_2$ dado en la sección 4.1. Recordemos que las palabras del código $\mathcal{C}$ tienen peso 0, 6 u 8.

Tomemos el código simplex binario $\mathcal{S}_4$. El código $\mathcal{S}_4$ tiene parámetros $[15, 4, 8]_2$ y todas sus palabras no nulas tienen peso 8.

Llevando a cabo la construcción ya vista dada en (4.2), obtenemos el código lineal binario

$$\mathcal{B} = \mathcal{C} \boxplus \mathcal{S}_4 = \Big\{ (u_1, \ldots, u_{11}, v_1, \ldots, v_{15},\ u_i + v_j\ ) \ :\ (u_1, \ldots, u_{11}) \in \mathcal{C}, (v_1, \ldots, v_{15}) \in \mathcal{S}_4 \Big\}$$

cuya longitud es

$$n = 11 + 15 + 11 \cdot 15 = 191$$

y cuya dimensión es $k = 3 + 4 = 7$

De la misma forma que en el caso anterior, se halla la distancia mínima. Mostramos los resultados en la siguiente tabla y a continuación se precisan las cuentas.

u_i	v_i	peso
0	8	96
6	0	96
6	8	96
8	0	128
8	8	96

Cuadro 4.5: Pesos del código

- En primer lugar, si tomamos la palabra nula del código $\mathcal{C}$ y la combinamos con la palabra nula del código $\mathcal{S}_4$, obtenemos la palabra nula. Si, en cambio, la combinamos con una palabra de $\mathcal{S}_4$ de peso 8, el peso de la palabra resultante será

$$0 + 8 + 11 \cdot 8 = 96$$

- En segundo lugar, si escogemos una palabra de $\mathcal{C}$ de peso 6 y la combinamos con la palabra nula de $\mathcal{S}_4$, obtenemos una palabra de peso

$$6 + 0 + 6 \cdot 15 = 96$$

si la combinamos con una palabra de $\mathcal{S}_4$ de peso 8, tendremos peso

$$6 + 8 + 6 \cdot (15 - 8) + 8 \cdot (11 - 6) = 96$$

es decir, si separamos las coordenadas de las palabras de $\mathcal{B}$ en tres bloques siendo el primer bloque las coordenadas de una palabra de $\mathcal{C}$, el segundo bloque las coordenadas de una palabra de $\mathcal{S}_4$ y el tercer bloque el resto de coordenadas de la palabra de $\mathcal{B}$, entonces en este caso tendremos peso 6 del primer bloque, peso 8 del segundo bloque y, por último, las combinaciones de coordenadas con distintas de cero del primer bloque con coordenadas nulas del segundo bloque y las combinaciones de coordenadas distintas de cero del segundo bloque con coordenadas nulas del primer bloque, esto es, $6 \cdot (15 - 8) + 8 \cdot (11 - 6)$. En definitiva, la palabra resultante tendrá peso 96.

- Finalmente, si seleccionamos la palabra de peso 8 de $\mathcal{C}$ y la combinamos con la palabra nula de $\mathcal{S}_4$, obtenemos una palabra de peso

$$8 + 0 + 8 \cdot 15 = 128$$

y si la combinamos con una palabra de peso 8 de $\mathcal{S}_4$, el peso será

$$8 + 8 + 8 \cdot (15 - 8) + 8 \cdot (11 - 8) = 96$$

Veamos a continuación el número de palabras que hay con cada uno de los pesos del código. Notemos que el código, que solo cuenta con **dos pesos** no nulos, es **autoortogonal**, puesto que el peso de cada palabra es *divisible entre cuatro.*

$$\begin{aligned} A_0 &= 1 \\ A_{96} &= 126 \\ A_{128} &= 1 \end{aligned}$$

La distancia mínima del código es, entonces, 96 y $\mathcal{B}$ tendrá parámetros $[191, 7, 96]_2$.

Hemos comprobado que, efectivamente, el código de parámetros $[191, 7, 96]_2$ es un código óptimo según nuestra definición y también según la Definición 38. Por añadidura, resaltemos el hecho de que casi todas las palabras de $\mathcal{B}$ tienen peso 96.

Veamos la tabla de [Grassl] donde hemos obtenido la información relativa a códigos óptimos.

n/k	5	6	7	8	9
189	96	96	94	94	92
190	96	96	95	94	92
191	97	96	96	95	92
192	98	96	96	96	93
193	98	96	96	96	94

Cuadro 4.6: Bounds on the minimum distance of linear codes over $GF(2)$

4.4. Otras construcciones con el código simplex binario

Los siguientes códigos se han construido utilizando una técnica análoga a la dada en [Til] para códigos Reed-Muller. En nuestro caso, en lugar de esta familia de códigos, hemos utilizado códigos simplex, que, como ya sabemos, están estrechamente relacionados con los códigos Reed-Muller.

Recordemos que el código simplex binario $\mathcal{S}_r$ tiene parámetros $[2^r - 1, r, 2^{r-1}]_2$ y el código simplex binario aumentado, añadiendo el vector todo unos, tiene parámetros $[2^r - 1, r + 1, 2^{r-1} - 1]_2$ y los siguientes pesos: $2^{r-1} - 1$, 2^{r-1}, $2^r - 1$.

Denotemos por S_r una matrix generadora del código simplex binario $\mathcal{S}_r$.

4.4.1. Código lineal binario óptimo de parámetros $[94, 7, 46]_2$

Sea el código lineal binario $\mathcal{C}$ un código cuya matriz generadora es la siguiente:

$$G = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ & & & & & 1 & 1 & 1 & \dots & 1 \\ & & S_6 & & & & & S_5 & & \\ & & & & & & & & & \end{array}\right]$$

La longitud de $\mathcal{C}$ es $63 + 31 = 94$ y la dimensión es 7. La distancia mínima es 46 puesto que la distancia mínima del código $\mathcal{S}_6$ aumentado es 31 y la del código $\mathcal{S}_5$ aumentado es 15. Cualquier combinación de las filas de la matriz dará una palabra con peso mayor o igual que $31 + 15 = 46$, como ocurre si tomamos la primera fila cuyo peso es 63. Los pesos del código, en relación al número de palabras que hay con cada uno, son los siguientes:

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{46} & = & 31 \\ A_{47} & = & 62 \\ A_{48} & = & 31 \\ A_{62} & = & 1 \\ A_{63} & = & 2 \end{array}$$

En conclusión, hemos construido un código lineal binario de parámetros $[94, 7, 46]_2$. Examinando las tablas de [Grassl], observamos que es un código óptimo.

n/k	5	6	7	8	9
92	47	46	45	44	42-43
93	48	46	46	44	42-44
94	48	47	46	44	43-44
95	48	48	47	45	44
96	48	48	48	46	44

Cuadro 4.7: Bounds on the minimum distance of linear codes over $GF(2)$

4.4.2. Código lineal binario óptimo de parámetros $[190, 7, 95]_2$

Sea el código lineal binario $\mathcal{C}$ con matriz generadora G. Las primeras columnas de G serán las columnas del código simplex binario $\mathcal{S}_7$ y las siguientes serán las columnas del código simplex binario $\mathcal{S}_6$ aumentado, añadiendo al código $\mathcal{S}_6$ la palabra cuyas componentes son todas uno.

$$G = \left[\begin{array}{ccccc|ccccc} & & & & & 1 & 1 & 1 & \dots & 1 \\ & & S_7 & & & & & S_6 & & \\ & & & & & & & & & \end{array}\right]$$

El código simplex binario $\mathcal{S}_7$ tiene parámetros $[127, 7, 64]_2$ y el código $\mathcal{S}_6$ aumentado, $[63, 7, 31]_2$.

Por tanto, el código $\mathcal{C}$, construido a partir de su matriz generadora, tiene longitud $127 + 63 = 190$, dimensión 7 y distancia mínima 95. Esto último es debido a que todas las palabras de $\mathcal{S}_7$ tienen peso 64 y el peso mínimo del código $\mathcal{S}_6$ aumentado es 31; por consiguiente cualquier combinación de las filas de G tiene, como mínimo, distancia $64 + 31 = 95$, como vemos a continuación.

$$\begin{aligned} A_0 &= 1 \\ A_{95} &= 63 \\ A_{96} &= 63 \\ A_{127} &= 1 \end{aligned}$$

El código lineal binario $\mathcal{C}$ tiene parámetros $[190, 7, 95]_2$. Si ahora añadimos un bit de paridad a este código, obtenemos un código de parámetros $[191, 7, 96]_2$, que es un código **autoortogonal** con solo **dos pesos** no nulos. Este último código tiene los mismos parámetros y la misma distribución de pesos que el código dado en la sección 4.3, construido de forma muy diferente. Sin embargo, no es fácil ver si son códigos equivalentes.

$$\begin{aligned} A_0 &= 1 \\ A_{96} &= 126 \\ A_{128} &= 1 \end{aligned}$$

Ambos códigos son códigos óptimos, como podemos observar en la siguiente tabla de [Grassl].

n/k	**5**	**6**	**7**	**8**	**9**
188	96	95	94	93	91
189	96	96	94	94	92
190	96	96	95	94	92
191	97	96	96	95	92
192	98	96	96	96	93

Cuadro 4.8: Bounds on the minimum distance of linear codes over $GF(2)$

4.4.3. Código lineal binario óptimo de parámetros $[254, 9, 126]_2$

Sea el código lineal binario $\mathcal{C}$ cuya matriz generadora es

$$G = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 \\ & & & & & & & & & \\ & & S_7 & & & & & S_7 & & \\ & & & & & & & & & \end{array}\right]$$

El código simplex binario $\mathcal{S}_7$ tiene parámetros $[127, 7, 64]_2$, luego el código $\mathcal{C}$ tiene longitud $127 + 127 = 254$ y dimensión 9 puesto que hay 9 filas linealmente independientes.

Si consideramos las dos mitades de la matriz G que hemos diferenciado, observamos que en cada una de ellas está la matriz generadora del código simplex binario $\mathcal{S}_7$ aumentado. Con esto en mente, calculamos los pesos del código:

$$\begin{aligned} A_0 &= 1 \\ A_{126} &= 127 \\ A_{127} &= 256 \\ A_{128} &= 127 \\ A_{254} &= 1 \end{aligned}$$

La distancia mínima, por tanto, es 126. El código $\mathcal{C}$ tiene parámetros $[254, 9, 126]_2$ y es un código óptimo, como podemos ver en la siguiente tabla de [Grassl].

n/k	**7**	**8**	**9**	**10**	**11**
252	126	126	124	121-123	120-122
253	127	126	125	122-124	120-122
254	128	127	126	122-124	120-123
255	128	128	127	123-124	120-124
256	128	128	128	124	121-124

Cuadro 4.9: Bounds on the minimum distance of linear codes over $GF(2)$

Veamos, a continuación, el caso general. Sea el código $\mathcal{C}$ cuya matriz generadora es

$$G = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 \\ & & & & & & & & & \\ & & S_r & & & & & S_r & & \\ & & & & & & & & & \end{array}\right]$$

Sabemos que el código simplex binario $\mathcal{S}_r$ tiene parámetros $[2^r - 1, r, 2^{r-1}]_2$. De este modo, la longitud de $\mathcal{C}$ es $2^r - 1 + 2^r - 1 = 2^{r+1} - 2$ y la dimensión, $r + 2$, pues G tiene $r + 2$ filas linealmente independientes. Como hemos visto en el caso particular, cada una de las dos mitades de la matriz G contiene a la matriz generadora del código simplex binario aumentado, cuyos pesos son $2^{r-1} - 1$, 2^{r-1}, $2^r - 1$. Por tanto, los pesos del código $\mathcal{C}$, en relación al número de palabras con cada uno de los pesos, son los siguientes:

$$\begin{array}{lcl} A_0 & = & 1 \\ A_{2^r-2} & = & 2^r - 1 \\ A_{2^r-1} & = & 2(2^r - 1) + 2 \\ A_{2^r} & = & 2^r - 1 \\ A_{2^{r+1}-2} & = & 1 \end{array}$$

En conclusión, el código $\mathcal{C}$ tiene parámetros $[2^{r+1} - 2, r + 2, 2^r - 2]_2$.

Capítulo 5

Un código distinto

Llegados a este punto, daremos una nueva construcción para la obtención de un código lineal binario óptimo de parámetros $[110, 8, 52]_2$. El hecho de que, a partir de esta técnica, hallemos un código óptimo es realmente curioso.

Sea $\mathcal{C}$ el código lineal binario de parámetros $[5, 4, 2]_2$ definido de la siguiente manera:

$$\mathcal{C} = \Big\{(a_1, a_2, a_3, a_4, a_5 = a_1 + a_2 + a_3 + a_4) \ : \ a_i \in \mathbb{F}_2, \quad i \in \{1, 2, 3, 4, 5\}\Big\} \subset \mathbb{F}_2^5$$

Las palabras de $\mathcal{C}$ son todas de peso par a causa del bit de paridad. Los pesos en relación al número de palabras del código de parámetros $[5, 4, 2]_2$ se muestran seguidamente.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_2 & = & 10 \\ A_4 & = & 5 \end{array}$$

Dado $\mathcal{C}$, definimos el código $\mathcal{B}$ como sigue: en la cabecera de las palabras-código escribimos los vectores $(a_1, \ldots, a_5) \in \mathcal{C}$ y $(b_1, \ldots, b_5) \in \mathcal{C}$; y en la cola, por un lado, todas las combinaciones de sumas de tres elementos de los a_i más un elemento b_j, y, por otro lado, de forma simétrica, todas las combinaciones de a_i sumadas a adiciones de tres elementos de los b_i.

$$\mathcal{B} = \left\{\Big(a_1, \ldots, a_5, b_1, \ldots, b_5, \ (\sum_3 a_i) + b_j \ , \ a_k + (\sum_3 b_l)\Big) \ : \ (a_1, \ldots, a_5), (b_1, \ldots, b_5) \in \mathcal{C}\right\}$$

Una matriz generadora del código $\mathcal{B}$ tiene la siguiente estructura: las diez primeras columnas, que forman la cabecera, contienen dos matrices generadoras del código $\mathcal{C}$, lo cual era previsible pues hemos usado dos códigos $\mathcal{C}$ para la construcción de $\mathcal{B}$; las siguientes 50 columnas de G son todas las posibles columnas que combinan columnas con dos y tres unos en las primeras cuatro filas y columnas de la matriz generadora de $\mathcal{C}$ en las segundas cuatro filas; y, las últimas 50 columnas son, de forma análoga, todas las posibles columnas que combinan columnas de la matriz generadora de $\mathcal{C}$ en las primeras cuatro filas y columnas con dos y tres unos en las segundas cuatro filas.

$$G = \left[\begin{array}{ccccc|c|ccccccccccc|ccc} 1&0&0&0&1&&1&1&1&1&1&1&\cdots&0&1&\cdots&1&1&\cdots&0&1&\cdots&1\\ 0&1&0&0&1&&1&1&1&1&1&1&\cdots&1&1&\cdots&1&0&\cdots&0&0&\cdots&1\\ 0&0&1&0&1&0&1&1&1&1&1&0&\cdots&1&0&\cdots&0&1&\cdots&1&0&\cdots&1\\ 0&0&0&1&1&&0&0&0&0&0&1&\cdots&1&0&\cdots&0&0&\cdots&1&0&\cdots&1\\ \hline &&&&&1&0&0&0&1&1&0&\cdots&1&1&\cdots&1&1&\cdots&1&1&\cdots&0\\ &&&&&0&1&0&0&1&0&1&\cdots&1&0&\cdots&1&0&\cdots&1&1&\cdots&0\\ &&&0&&0&0&1&0&1&0&1&\cdots&1&0&\cdots&1&0&\cdots&1&1&\cdots&1\\ &&&&&0&0&0&1&1&0&0&\cdots&1&0&\cdots&1&0&\cdots&1&0&\cdots&1 \end{array}\right]$$

El código $\mathcal{B}$ tiene longitud

$$n = 5 + 5 + \binom{5}{3} \cdot 5 + 5 \cdot \binom{5}{3} = 110$$

y dimensión $k = 4+4 = 8$. Hallemos la distancia mínima de igual forma que en los casos anteriores. La simetría debida a que ambos códigos son el mismo nos ahorrará algunos cálculos.

- Si tomamos la palabra nula del primer código y la palabra nula del segundo, obtenemos la palabra nula de $\mathcal{B}$. Si tomamos la palabra nula del primer código y una palabra de peso 2 del segundo código, el peso de la palabra resultante será

  $$0 + 2 + \binom{5}{3} \cdot 2 + 5 \cdot 2 \cdot \binom{3}{2} = 52$$

  Si combinamos la palabra nula con una palabra de peso 4 del segundo código, tendremos peso

  $$0 + 4 + \binom{5}{3} \cdot 4 + 5 \cdot \binom{4}{3} = 64$$

- Si ahora tomamos una palabra de peso 2 del primer código y la combinamos con una palabra de peso también 2 del segundo código, el peso es

  $$2 + 2 + 2\left(2 \cdot \binom{3}{2} \cdot 3 + (1+3) \cdot 2\right) = 56$$

  y si la combinamos con una palabra de peso 4, el peso de la palabra será

  $$2 + 4 + \left(2 \cdot \binom{3}{2} + (1+3) \cdot 4\right) + \left(2 \cdot \binom{4}{2} + 3 \cdot \binom{4}{3}\right) = 52$$

- Por último, si escogemos una palabra de peso 4 del primer código y la combinamos con una del mismo peso del segundo código, obtenemos peso

  $$4 + 4 + 2\left(\binom{4}{3} + \binom{4}{2} \cdot 4\right) = 64$$

Los resultados los resumimos en la siguiente tabla.

a_i	b_i	peso
0	2	52
0	4	64
2	2	56
2	4	52
4	4	64

Cuadro 5.1: Pesos del código

Examinemos la relación entre los pesos y el número de palabras del código y notemos que se trata de un código con solo **tres pesos** no nulos. Además, todos los pesos del códigos son *divisibles entre cuatro* y, por ese motivo, $\mathcal{B}$ es un código **autoortogonal**.

$$\begin{aligned} A_0 &= 1 \\ A_{52} &= 120 \\ A_{56} &= 100 \\ A_{64} &= 35 \end{aligned}$$

La distancia mínima de $\mathcal{B}$ es, por lo tanto, 52. Hemos hallado un código de parámetros $[110, 8, 52]_2$, que es un código óptimo.

Observemos la tabla obtenida en [Grassl].

n/k	**6**	**7**	**8**	**9**	**10**
108	54	53	52	50	49-50
109	54	54	52	51	50
110	55	54	52	52	50-51
111	56	55	53	52	51-52
112	56	56	54	52	52

Cuadro 5.2: Bounds on the minimum distance of linear codes over $GF(2)$

Notemos, no obstante, que el código de parámetros $[110, 8, 52]_2$ no es óptimo conforme a la Definición 38 puesto que existen códigos lineales binarios de parámetros $[108, 8, 52]_2$ y $[109, 8, 52]_2$.

Capítulo 6

Códigos óptimos con la construcción $(u \mid u+v)$

A continuación detallaremos lo que se entiende por construcción $(u|u+v)$, una técnica bien conocida que resulta sencilla y útil para generar familias de códigos óptimos y códigos Reed-Muller binarios. Esto resultará interesante pues más adelante describiremos su generalización ternaria a partir de la cual se pueden construir los códigos Reed-Muller ternarios.

La idea de la construcción $(u \mid u+v)$ se intuye en su propio nombre:

Sean dos códigos lineales $\mathcal{U}$, $\mathcal{V}$, definidos sobre el mismo cuerpo y con la misma longitud n. El código $\mathcal{C}$ que construimos tiene longitud $2n$. Sea u una palabra de $\mathcal{U}$ y v una palabra de $\mathcal{V}$. Una palabra de $\mathcal{C}$ es de la forma $(u\,,\ u+v)$.

$$\mathcal{C} = \Big\{(u\,,\ u+v)\ :\ \ u \in \mathcal{U},\ \ v \in \mathcal{V}\Big\}$$

Veamos cuál es la dimensión y la distancia mínima del código $\mathcal{C}$:

Teorema 52 *Sean $\mathcal{U}$ y $\mathcal{V}$ códigos de parámetros $[n, k_U, d_U]_q$ y $[n, k_V, d_V]_q$, respectivamente, donde $d_U \leq d_V$. Podemos construir un código $[2n, k_U + k_V, d]_q$, donde $d = min\{2d_U, d_V\}$.*

Demostración: Construimos un código $\mathcal{C}$ como la imagen de $f : \mathcal{U} \oplus \mathcal{V} \longrightarrow \mathbb{F}_q^{2n}$ definida por $f(u, v) = (u, u + v)$. Claramente, f es inyectiva, lo cual implica que $\dim(\mathcal{C}) = k_U + k_V$.
Para acotar el peso mínimo, distinguimos dos casos: si $u \neq 0, v = 0$, entonces $w(u, u) \geq 2d_U$; si $v \neq 0$, entonces $w(u, u + v) \geq w(v) \geq d_V$. De hecho, cuando $v_i \neq 0$, tiene que ocurrir lo siguiente: que o bien $u_i \neq 0$ o $u_i + v_i \neq 0$. □

La estructura de la matriz generadora del código $\mathcal{C}$ es

$$\begin{bmatrix} G_U & G_U \\ 0 & G_V \end{bmatrix}$$

donde G_U y G_V son las matrices generadoras de los códigos $\mathcal{U}$ y $\mathcal{V}$, respectivamente.

Esta construcción puede generalizarse a códigos no lineales.

Veamos algunos ejemplos similares a los dados en [Bier]: Sea el código lineal binario de parámetros $[10, 3, 5]_2$ dado por la matriz generadora

$$\left[\begin{array}{ccc|ccc|ccc|c} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right]$$

Llamaremos código de repetición al código de parámetros $[m, 1, m]_q$, $m \in \mathbb{N}$.

Aplicando la construcción $(u \,|\, u+v)$ a los códigos de parámetros $[10, 3, 5]_2$ y $[10, 1, 10]_2$, obtenemos el código de parámetros $[20, 4, 10]_2$. Si seguimos aplicando la construcción $(u \,|\, u+v)$ recursivamente a los códigos que vamos obteniendo con sus respectivos códigos de repetición binarios, generamos los códigos de parámetros $[40, 5, 20]_2$, $[80, 6, 40]_2$, $[160, 7, 80]_2$, y en general $[2^i \cdot 10, 3+i, 2^i \cdot 5]_2$ para todo $i \geq 1$.

Si ahora empezamos por el código trivial de parámetros $[2, 2, 1]_2$, usando el mismo método que arriba, obtenemos códigos de parámetros $[4, 3, 2]_2$, $[8, 4, 4]_2$, $[16, 5, 8]_2$ y en general $[2^i, i+1, 2^{i-1}]_2$ para todo $i \geq 1$. Estos son los códigos Reed-Muller binarios de primer orden, $\mathcal{RM}(1, i)$, bien conocidos. Además, encontramos otra construcción del código de Hamming binario extendido $[8, 4, 4]_2$.

Todos estos códigos alcanzan la cota de Griesmer (2.3) con igualdad. Son códigos óptimos.

Corolario 53 *La existencia de un código lineal de parámetros* $[n, k, n/2]_q$ *implica la existencia de códigos lineales de parámetros* $[2^i n, k+i, 2^{i-1} n]_q$ *para todo* $i \geq 1$.

Demostración: Es un caso especial del Teorema 52 cuando $d_U = n/2$ y el segundo código utilizado en cada caso es el código de repetición conveniente. □

Algunos parámetros de códigos lineales binarios óptimos con la forma $[n, k, n/2]_2$, distintos de los mostrados en los ejemplos anteriores, son $[6, 3, 3]_2$, $[12, 4, 6]_2$, $[14, 4, 7]_2$, $[22, 4, 11]_2$, $[26, 4, 13]_2$, $[30, 5, 15]_2$, $[46, 5, 23]_2$, $[62, 6, 31]_2$, etcéctera.

Capítulo 7

Códigos lineales ternarios

Se han intentado trasladar algunos métodos de los Capítulos 3 y 5 a códigos ternarios con sumas y restas. Tras hacer las cuentas con MAPLE, pues ya resulta complejo realizar los cálculos a mano, se observa que dichas técnicas no proporcionan resultados alentadores para códigos lineales sobre el cuerpo $\mathbb{F}_3$, como hicieron en el caso binario. Se han obtenido códigos con distancia mínima claramente menor que la del código óptimo de misma longitud y dimensión. Una excepción son los códigos presentados en la Sección 7.4. Por otro lado, el código simplex ternario y la técnica $(u + v + w \mid 2u + v \mid u)$ aportan buenas ideas.

7.1. Código simplex ternario

En esta sección expondremos los códigos simplex ternarios presentados en [Bier]. Para ello comenzaremos presentando la noción de código de Hamming sobre $\mathbb{F}_q$, $\mathcal{H}_q(r)$.

El código de Hamming sobre $\mathbb{F}_q$, denotado por $\mathcal{H}_q(r)$, es un subespacio vectorial de $\mathbb{F}_q^n$ cuya matriz de control tiene una estructura concreta. Sea H la matriz de control del código $\mathcal{H}_q(r)$. Las columnas de H son todos los vectores no nulos de $\mathbb{F}_q^r$ tomando un único representante de la relación producto por escalar, es decir, si está la columna u, entonces no está la columna λu, $\lambda \neq 1$. Por esa razón, H tiene orden $r \times n$ y rango r.

De este modo, el código $\mathcal{H}_q(r)$ tiene los siguientes parámetros:

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]_q$$

El código de Hamming $\mathcal{H}_3(r)$ sobre $\mathbb{F}_3$ tiene parámetros

$$\left[\frac{3^r-1}{2}, \frac{3^r-1}{2} - r, 3\right]_3$$

En este caso, si en la matriz de control está la columna u, entonces no está $-u$.

Dicho esto, se define el código simplex ternario $\mathcal{S}_r$ como el dual del código de Hamming ternario $\mathcal{H}_3(r)$. La matriz generadora de $\mathcal{S}_r$ es la matriz de control del código de Hamming.

Teorema 54 *Los parámetros del código $\mathcal{S}_r$ son*

$$\left[\frac{3^r-1}{2}, r, 3^{r-1}\right]_3$$

Demostración: La longitud y dimensión de $\mathcal{S}_r$ quedan claras por las propiedades del código dual. Ahora veamos que, ciertamente, la distancia mínima es $d = 3^{r-1}$.

Sea G la matriz generadora de $\mathcal{S}_r$ y sean e_i, donde $i \in \{1, \ldots, r\}$, las filas de G con las siguientes coordenadas

$$\begin{aligned} e_1 &= (x_{11}, \ldots, x_{1n}) \\ e_2 &= (x_{21}, \ldots, x_{2n}) \\ &\cdots \\ e_r &= (x_{r1}, \ldots, x_{rn}) \end{aligned}$$

Tomemos un vector $v \in \mathcal{S}_r$, v es una combinación de las filas de G

$$v = a_1e_1 + \cdots + a_re_r, \;\; a_i \in \mathbb{F}_3$$

El peso de v es

$$w(v) = \frac{3^r-1}{2} - \text{coordenadas de } v \text{ que se anulan}$$

Veamos cuántas coordenadas de v se anulan. La coordenada i-ésima de v se anula si y solo si $a_1x_{1i} + \cdots + a_rx_{ri} = 0$. Ahora bien,

$$a_1z_1 + \cdots + a_rz_r = 0$$

es un hiperplano de $\mathbb{F}_3^r$ con dimensión $r-1$, es decir, tiene 3^{r-1} vectores y $3^{r-1}-1$ vectores no nulos. Teniendo en cuenta que si se anula en $u = (x_{1i}, \ldots, x_{ri})$ entonces se anula en $-u = (-x_{1i}, \ldots, -x_{ri})$, el hiperplano tiene $\frac{3^{r-1}-1}{2}$ vectores no nulos escogiendo uno entre u y $-u$.

En conclusión, el peso de $v = a_1e_1 + \cdots + a_re_r$, $a_i \in \mathbb{F}_3$ es

$$\frac{3^r-1}{2} - \frac{3^{r-1}-1}{2} = \frac{3^r-3^{r-1}}{2} = 3^{r-1}$$

Esto demuestra que el código simplex ternario $\mathcal{S}_r$, al igual que el código simplex binario, es un *constant-weight code* y su distancia mínima es, por tanto, $d = 3^{r-1}$. □

Los códigos simplex ternarios alcanzan la cota de Griesmer (2.3) con igualdad y, por ello, son códigos óptimos.

$$\sum_{i=0}^{r-1} \left\lceil \frac{3^{r-1}}{3^i} \right\rceil = 3^{r-1} + 3^{r-2} + \cdots + 1 = \frac{3^r-1}{2}$$

7.2. Construcción $(u + v + w \mid 2u + v \mid u)$

En esta sección describiremos la construcción ternaria $(u + v + w \mid 2u + v \mid u)$ sobre $\mathbb{F}_3$ que expone [KsPa]. Esta construcción nos permite combinar tres códigos ternarios de longitud n para formar un código de longitud $3n$. Puede usarse para generar todos los códigos Reed-Muller ternarios, así como otros tantos códigos.

Un caso especial de la anterior es la construcción $(u + v \mid 2u + v \mid u)$, la cual combina dos códigos ternarios de longitud n para formar un código ternario de longitud $3n$.

Sean $\mathcal{U}$, $\mathcal{V}$ y $\mathcal{W}$ códigos lineales ternarios de parámetros $[n, k_U, d_U]_3$, $[n, k_V, d_V]_3$ y $[n, k_W, d_W]_3$, respectivamente. Definimos el código $\mathcal{C}$ como sigue

$$\mathcal{C} = \Big\{(u + v + w\ ,\ 2u + v\ ,\ u)\ :\ \ u \in \mathcal{U}, v \in \mathcal{V}, w \in \mathcal{W}\Big\} \tag{7.1}$$

Escribiremos, en algún caso, $\mathcal{C} = (\mathcal{U} + \mathcal{V} + \mathcal{W} \mid 2\mathcal{U} + \mathcal{V} \mid \mathcal{U})$ cuando $\mathcal{C}$ esté definido como en (7.1).

Es claro que la longitud del código $\mathcal{C}$ es $3n$ y la dimensión $k_U + k_V + k_W$. Veamos que la distancia mínima de $\mathcal{C}$ es igual a $\min(3d_U, 2d_V, d_W)$.

Examinemos los diferentes casos posibles. En lo que sigue distinguiremos cada una de las tres partes de las palabras de $\mathcal{C}$, $(u + v + w\ ,\ 2u + v\ ,\ u)$, y las llamaremos primer, segundo y tercer bloque.

- Si $u \neq 0$, $v = 0$, $w = 0$, tenemos palabras del tipo $(u, 2u, u) \in \mathcal{C}$. El código $\mathcal{U}$ tiene distancia mínima d_U, luego el peso de $(u, 2u, u)$ es mayor o igual que $3d_U \geq \min(3d_U, 2d_V, d_W)$, pudiendo ser, en algún caso, exactamente $3d_U$.

- Si $u = 0$, $v \neq 0$, $w = 0$, tenemos palabras del tipo $(v, v, 0) \in \mathcal{C}$. El código $\mathcal{V}$ tiene distancia mínima d_V, entonces el peso de $(v, v, 0)$ es mayor o igual que $2d_V \geq \min(3d_U, 2d_V, d_W)$, siendo $2d_V$ si la palabra v es una palabra de peso mínimo del código $\mathcal{V}$.

- Si $u = 0$, $v = 0$, $w \neq 0$, tenemos palabras del tipo $(w, 0, 0) \in \mathcal{C}$, y, puesto que el código $\mathcal{W}$ tiene distancia mínima d_W, el peso de $(w, 0, 0)$ es mayor o igual que $d_W \geq \min(3d_U, 2d_V, d_W)$, siendo d_W en algún caso.

- Si $u \neq 0$, $v \neq 0$, $w = 0$, tenemos palabras del tipo $(u+v, 2u+v, u) \in \mathcal{C}$. La palabra v tiene, al menos, d_V coordenadas no nulas, luego la palabra $(v, v, 0)$ tiene, al menos, $2d_V$ coordenadas no nulas. Ahora bien, es fácil ver que si u_i+v_i se anula con $v_i \neq 0$, $2u_i+v_i$ no se anula, y además, se añade una coordenada no nula en la u del tercer bloque. Lo mismo pasaría al revés. De este modo el peso de cada una de estas palabras es mayor o igual que $2d_V \geq \min(3d_U, 2d_V, d_W)$.

- Si $u \neq 0$, $v = 0$, $w \neq 0$, tenemos palabras del tipo $(u + w, 2u, u) \in \mathcal{C}$. La palabra w tiene como mínimo peso d_W. Por cada coordenada que se anule al sumar u en los casos que $w_i \neq 0$, se añade una coordenada no nula en cada uno de los dos últimos bloques. En conclusión, las palabras de este tipo tienen peso mayor o igual que $d_W \geq \min(3d_U, 2d_V, d_W)$.

- Si $u = 0$, $v \neq 0$, $w \neq 0$, tenemos palabras del tipo $(v + w, v, 0) \in \mathcal{C}$. Al igual que en el caso anterior, la palabra w tiene, al menos, peso d_W, y, por cada coordenada $w_i \neq 0$ que al sumarse v_i sea cero, añadimos una coordenada no nula en el segundo bloque de la palabra. El peso es entonces mayor o igual que $d_W \geq \min(3d_U, 2d_V, d_W)$.

- Si $u \neq 0$, $v \neq 0$, $w \neq 0$, tenemos palabras del tipo $(u + v + w, 2u + v, u) \in \mathcal{C}$. Una vez más, sabemos que la palabra w tiene al menos d_W coordenadas no nulas. Ahora, por cada

coordenada $w_i \neq 0$ que se anule al sumarle $u_i + v_i$, $u_i + v_i$ será distinto de cero, lo cual implica que o $-u_i + v_i$ es distinto de cero o lo es u_i. Por consiguiente, por cada coordenada $u_i + v_i + w_i$ que se anule siendo $w_i \neq 0$ se añade una coordenada no nula a uno de los dos bloques, al menos. En definitiva, el peso de las palabras de este tipo es mayor o igual que $d_W \geq \min(3d_U, 2d_V, d_W)$.

El código $\mathcal{C}$ tiene, por tanto, parámetros

$$[3n, k_U + k_V + k_W, \min(3d_U, 2d_V, d_W)]_3$$

Veamos la estructura de la matriz generadora del código $\mathcal{C}$. Si los códigos $\mathcal{U}$, $\mathcal{V}$ y $\mathcal{W}$ tienen matrices generadoras G_U, G_V y G_W, respectivamente, entonces el código $\mathcal{C}$ tiene la siguiente matriz generadora:

$$\begin{bmatrix} G_W & 0 & 0 \\ G_V & G_V & 0 \\ G_U & 2G_U & G_U \end{bmatrix} \tag{7.2}$$

En el caso especial en que la construcción es $(u+v \,|\, 2u+v \,|\, u)$, el código resultante tiene parámetros

$$[3n, k_U + k_V, \min(3d_U, 2d_V)]_3$$

y la matriz generadora tiene la siguiente forma:

$$\begin{bmatrix} G_V & G_V & 0 \\ G_U & 2G_U & G_U \end{bmatrix} \tag{7.3}$$

7.2.1. Código lineal ternario óptimo de parámetros $[18, 9, 6]_3$

Veamos un ejemplo de la construcción $(u + v + w \mid 2u + v \mid u)$ combinando los siguientes códigos lineales ternarios:

- Sea $\mathcal{U}$ el código lineal de parámetros $[6, 5, 2]_3$.
- Sea $\mathcal{V}$ el código lineal de parámetros $[6, 3, 3]_3$ dado por la matriz generadora

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

- y, por último, sea $\mathcal{W}$ el código lineal de parámetros $[6, 1, 6]_3$.

Notemos que $3d_U = 2d_V = d_W = 6$.

El código dado por

$$\mathcal{C} = \Big\{ (u + v + w \,,\, 2u + v \,,\, u) \;:\; u \in \mathcal{U}, v \in \mathcal{V}, w \in \mathcal{W} \Big\}$$

tiene longitud $3 \cdot 6 = 18$, dimensión $5 + 3 + 1 = 9$ y distancia mínima 6. Se trata de un código lineal ternario con parámetros $[18, 9, 6]_3$, el cual es óptimo, si bien existen códigos de parámetros $[17, 9, 6]_3$ y $[18, 10, 6]_3$. Veamos la tabla de [Grassl].

n/k	**7**	**8**	**9**	**10**	**11**
16	6	6	5	4	4
17	7	6	6	5	4
18	8	7	6	6	5
19	9	8	7	6	6
20	9	9	8	7	6

Cuadro 7.1: Bounds on the minimum distance of linear codes over $GF(3)$

7.3. Código Reed-Muller ternario

El propósito principal de esta sección es presentar los códigos Reed-Muller ternarios haciendo uso de la construcción $(u + v + w \,|\, 2u + v \,|\, u)$ vista en la sección anterior, de forma análoga a la manera en que se generan los códigos Reed-Muller binarios a partir de la construcción $(u \,|\, u + v)$, como sugiere [KsPa]. Para empezar, describiremos con detalle los códigos Reed-Muller más simples, con el fin de hacer más sencilla la comprensión del caso general. Para concluir, citaremos brevemente cómo se definieron originalmente los códigos Reed-Muller ternarios en [Mass].

Se define el código $\mathcal{R}_3(r, 0)$ como

$$\mathcal{R}_3(r,0) = \begin{cases} \{0\}, & r < 0 \\ \mathbb{F}_3, & r \geq 0 \end{cases} \tag{7.4}$$

es decir, el código $\mathcal{R}_3(r, 0)$ con $r < 0$ es el código lineal trivial de longitud uno cuya única palabra es la palabra nula. Siguiendo [KsPa], denotaremos a sus parámetros por $[1, 0, \infty]_3$. El código $\mathcal{R}_3(r, 0)$ con $r \geq 0$ tiene como palabras los elementos del cuerpo finito $\mathbb{F}_3$ y parámetros $[1, 1, 1]_3$.

Se define ahora el código $\mathcal{R}_3(r, m)$ de forma inductiva como

$$\mathcal{R}_3(r,m) = \Big\{(u+v+w, 2u+v, u) : u \in \mathcal{R}_3(r, m-1), v \in \mathcal{R}_3(r-1, m-1), w \in \mathcal{R}_3(r-2, m-1)\Big\} \tag{7.5}$$

La recurrencia (7.5) define una familia infinita de códigos lineales ternarios. Denotaremos por $[n(r, m), k(r, m), d(r, m)]_3$ los parámetros de $\mathcal{R}_3(r, m)$ y por $G(r, m)$ la matriz generadora del código.

7.3.1. Código Reed-Muller ternario $\mathcal{R}_3(1, m)$

Puesto que los códigos Reed-Muller ternarios se definen recurrentemente, estudiaremos, en primer lugar, los códigos $\mathcal{R}_3(1, m)$. Para ello, previamente, examinemos los códigos Reed-Muller ternarios $\mathcal{R}_3(0, m)$.

De acuerdo con la definición dada en (7.4), el código $\mathcal{R}_3(0, 0) = \mathbb{F}_3$ es el código de parámetros $[1, 1, 1]_3$ con matriz generadora $G(0, 0) = [\,1\,]$.

El código $\mathcal{R}_3(0, 1)$, a partir de lo anterior, es

$$\mathcal{R}_3(0,1) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ u \in \mathcal{R}_3(0,0), v \in \mathcal{R}_3(-1,0), w \in \mathcal{R}_3(-2,0)\Big\}$$

De nuevo, por la defínción dada en (7.4), sabemos que los códigos $\mathcal{R}_3(r,0)$ con $r<0$ son los códigos de parámetros $[1,0,\infty]_3$ y *no aportan nada* a la construcción anterior, al igual que *no aportarán nada* los códigos $\mathcal{R}_3(r,m)$ con $r<0$ en los casos posteriores. El código $\mathcal{R}_3(0,1)$ es, por tanto, el siguiente:

$$\mathcal{R}_3(0,1) = \Big\{(0,0,0),(1,1,1),(2,2,2)\Big\}$$

es decir, tiene parámetros $[3,1,3]_3$ y matriz generadora $G(0,1) = [1\ 1\ 1]$.

De forma recurrente, observamos que el código $\mathcal{R}_3(0,m)$ construido de la forma

$$\mathcal{R}_3(0,m) = \{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ u \in \mathcal{R}_3(0,m-1), v \in \mathcal{R}_3(-1,m-1), w \in \mathcal{R}_3(-2,m-1)\}$$

es el código

$$\mathcal{R}_3(0,m) = \Big\{(0,0,\ldots,0),(1,1,\ldots,1),(2,2,\ldots,2)\Big\}$$

con parámetros $[3^m,1,3^m]_3$ y matriz generadora $G(0,m) = [\overbrace{1\ 1\ \cdots\ 1}^{m}]$

Conocidas la estructura y los parámetros de los códigos $\mathcal{R}_3(0,m)$, estamos en condiciones de construir los códigos $\mathcal{R}_3(1,m)$.

Estos códigos se generan de forma especial puesto que se emplea la construcción $(u+v\,|\,2u+v\,|\,u)$, dado que, como vimos en (7.4), los códigos $\mathcal{R}_3(-1,m) = [1,0,\infty]$ *no aportan nada* a la construcción. En (7.4) también se advierte que el código $\mathcal{R}_3(1,0) = \mathbb{F}_3$ es el código lineal ternario de parámetros $[1,1,1]_3$ y su matriz generadora es $G(1,0) = [\,1\,]$.

Sabiendo esto, somos capaces de construir el código $\mathcal{R}_3(1,1)$:

$$\mathcal{R}_3(1,1) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ u \in \mathcal{R}_3(1,0), v \in \mathcal{R}_3(0,0), w \in \mathcal{R}_3(-1,0)\Big\}$$

Hemos visto que los códigos $\mathcal{R}_3(1,0)$ y $\mathcal{R}_3(0,0)$ tienen, ambos, parámetros $[1,1,1]_3$. Hallaremos los parámetros de $\mathcal{R}_3(1,1)$ teniendo en cuenta que estamos utilizando la construcción $(u+v\,|\,2u+v\,|\,u)$. Por tanto, como vimos en la sección anterior, la longitud es $n(1,1) = 3\cdot 1 = 3$, la dimensión $k(1,1) = 1+1 = 2$ y la distancia mínima $d(1,1) = \min(3\cdot 1, 2\cdot 1) = 2$. El código $\mathcal{R}_3(1,1)$ tiene parámetros $[3,2,2]_3$.

Una matriz generadora de $\mathcal{R}_3(1,1)$ tiene orden 2×3 y la estructura dada en (7.3):

$$G(1,1) = \begin{bmatrix} G(0,0) & G(0,0) & 0 \\ G(1,0) & 2G(1,0) & G(1,0) \end{bmatrix} = \left[\begin{array}{c|c|c} 1 & 1 & 0 \\ \hline 1 & 2 & 1 \end{array}\right]$$

A partir de lo anterior, el código $\mathcal{R}_3(1,2)$

$$\mathcal{R}_3(1,2) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ u \in \mathcal{R}_3(1,1), v \in \mathcal{R}_3(0,1), w \in \mathcal{R}_3(-1,1)\Big\}$$

tiene parámetros $[9,3,6]_3$ y la siguiente matriz generadora de orden 3×9:

$$G(1,2) = \begin{bmatrix} G(0,1) & G(0,1) & 0 \\ G(1,1) & 2G(1,1) & G(1,1) \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{array}\right]$$

Siguiendo la misma línea, el código $\mathcal{R}_3(1,3)$

$$\mathcal{R}_3(1,3) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ \ u \in \mathcal{R}_3(1,2), v \in \mathcal{R}_3(0,2), w \in \mathcal{R}_3(-1,2)\Big\}$$

es el código de parámetros $[27,4,18]_3$ y su matriz generadora tiene orden 4×27 y la siguiente forma:

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

$$= \left[\begin{array}{ccccccccc|ccccccccc|ccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{array}\right]$$

El código $\mathcal{R}_3(1,m)$ se construye, como vimos en (7.5), de la siguiente forma:

$$\mathcal{R}_3(1,m) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ \ u \in \mathcal{R}_3(1,m-1), v \in \mathcal{R}_3(0,m-1), w \in \mathcal{R}_3(-1,m-1)\Big\}$$

Su matriz generadora es

$$G(1,m) = \begin{bmatrix} G(0,m-1) & G(0,m-1) & 0 \\ G(1,m-1) & 2G(1,m-1) & G(1,m-1) \end{bmatrix}$$

y sus parámetros cumplen las siguientes propiedades, las cuales son consecuencia directa de las propiedades de la construcción $(u+v+w \mid 2u+v \mid u)$ por inducción sobre m:

- $n = 3^m$
- $k(1,m) = k(1,m-1) + k(0,m-1) + k(-1,m-1) = k(1,m-1) + 1 + 0 = m+1$
- $d(1,m) = \min\{3(2\cdot 3^{m-2}), 2\cdot 3^{m-1}\} = 2\cdot 3^{m-1}$

El código $\mathcal{R}_3(1,m)$ tiene parámetros $[3^m, m+1, 2\cdot 3^{m-1}]_3$.

Este código cumple la cota de Griesmer (2.3) con igualdad y, por tanto, es óptimo.

$$\sum_{i=0}^{m} \left\lceil \frac{2\cdot 3^{m-1}}{3^i} \right\rceil = 2\cdot 3^{m-1} + 2\cdot 3^{m-2} + \cdots + 2\cdot 3 + 2 + 1 = 2\cdot \frac{3^m - 1}{2} + 1 = 3^m$$

7.3.2. Código Reed-Muller ternario $\mathcal{R}_3(2,m)$

En la misma línea, examinemos los códigos Reed-Muller ternarios $\mathcal{R}_3(2,m)$. Igual que en los casos anteriores, para $m=0$, por la definición dada en (7.4), el código $\mathcal{R}_3(2,0) = \mathbb{F}_3$ tiene parámetros $[1,1,1]_3$.

El código general $\mathcal{R}_3(2,m)$ se construye de la siguiente forma:

$$\mathcal{R}_3(2,m) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ \ u \in \mathcal{R}_3(2,m-1), v \in \mathcal{R}_3(1,m-1), w \in \mathcal{R}_3(0,m-1)\Big\}$$

Su matriz generadora tiene la siguiente configuración:

$$G(2,m) = \begin{bmatrix} G(0,m-1) & 0 & 0 \\ G(1,m-1) & G(1,m-1) & 0 \\ G(2,m-1) & 2G(2,m-1) & G(2,m-1) \end{bmatrix}$$

El código $\mathcal{R}_3(2,m)$ tiene parámetros

- $n = 3^m$
- La dimensión es

$$k(2,m) = k(2,m-1) + k(1,m-1) + k(0,m-1) = k(2,m-1) + m + 1 \qquad (7.6)$$

- $d(2,m) = \min\{3 \cdot 3^{m-2}, 2 \cdot 2 \cdot 3^{m-2}, 3^{m-1}\} = 3^{m-1}$

obtenidos por inducción a partir de las propiedades de la construcción $(u+v+w \mid 2u+v \mid u)$.

Veamos cuál es exactamente la dimensión del código $\mathcal{R}_3(2,m)$. Calcularemos inicialmente las dimensiones de los primeros códigos más sencillos y veremos cómo se ajustan a una forma cuadrática.

$$\begin{aligned} k(2,0) &= 1 \\ k(2,1) &= 1+1+1 = 3 \\ k(2,2) &= 3+2+1 = 6 \\ k(2,3) &= 6+3+1 = 10 \\ k(2,4) &= 10+4+1 = 15 \\ k(2,5) &= 15+5+1 = 21 \end{aligned}$$

Como se cumple (7.6), sabemos que $k(2,m) = am^2 + bm + c$. Hallemos los parámetros a, b y c:

Para $m = 0$, tenemos que $c = 1$. Para $m = 1$, tenemos las ecuaciones $a + b + 1 = 3$, $a + b = 2$ y, finalmente, para $m = 2$, tenemos $4a + 2b + 1 = 6$.

De las tres ecuaciones anteriores, obtenemos los valores $a = 1/2$ y $b = 3/2$, por tanto, la siguiente igualdad:

$$k(2,m) = \frac{m^2+3m+2}{2} = \frac{(m+2)(m+1)}{2} = \binom{m+2}{2}$$

Nótese que

$$\binom{m+2}{2} = \binom{m+1}{2} + m + 1$$

Por inducción sobre m, se sigue que el código $\mathcal{R}_3(2,m)$ tiene parámetros $\left[3^m, \binom{m+2}{2}, 3^{m-1}\right]_3$.

7.3.3. Código Reed-Muller ternario $\mathcal{R}_3(3,m)$

Los códigos Reed-Muller ternarios $\mathcal{R}_3(3,m)$ se construyen a partir de los códigos que hemos visto previamente de la forma

$$\mathcal{R}_3(3,m) = \Big\{(u+v+w\ ,\ 2u+v\ ,\ u)\ :\ \ u \in \mathcal{R}_3(3,m-1), v \in \mathcal{R}_3(2,m-1), w \in \mathcal{R}_3(1,m-1)\Big\}$$

y una matriz generadora suya es

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

Al igual que en los casos anteriores, los parámetros de los códigos $\mathcal{R}_3(3,m)$ se obtienen por inducción sobre m a partir de las características de la construcción $(u+v+w \,|\, 2u+v \,|\, u)$ y son los siguientes:

- $n = 3^m$
- La dimensión es

$$k(3,m) = k(3,m-1) + k(2,m-1) + k(1,m-1) = k(3,m-1) + \binom{m+1}{2} + m \qquad (7.7)$$

- $d(3,m) = \min\{3 \cdot 2 \cdot 3^{m-3}, 2 \cdot 3^{m-2}, 2 \cdot 3^{m-2}\} = 2 \cdot 3^{m-2}$

Puesto que la dimensión $k(3,m)$ sigue la fórmula inductiva (7.7), sabemos que $k(3,m) = am^3 + bm^2 + cm + d$. Calculemos los primeros valores de este parámetro para hallar los coeficientes del polinomio anterior.

$$\begin{aligned} k(3,0) &= 1 \\ k(3,1) &= 1+1+1 = 3 \\ k(3,2) &= 3 + \tbinom{3}{2} + 2 = 8 \\ k(3,3) &= 8 + \tbinom{4}{2} + 3 = 17 \\ k(3,4) &= 17 + \tbinom{5}{2} + 4 = 31 \\ k(3,5) &= 31 + \tbinom{6}{2} + 5 = 51 \end{aligned}$$

Dichos coeficientes son $a = 1/6$, $b = 1$, $c = 5/6$ y $d = 1$. En definitiva, dada la recursión (7.7) junto con los valores anteriores, obtenemos la bonita fórmula

$$k(3,m) = \binom{m+3}{3} - m$$

Es curiosa la sucesión de dimensiones que hemos ido obteniendo: $\binom{m}{0}$, $\binom{m+1}{1}$, $\binom{m+2}{2}$, $\binom{m+3}{3} - m \ldots$

Por ejemplo, el código $\mathcal{R}_3(3,5)$ tiene parámetros $[3^5, 51, 2 \cdot 3^3]_3 = [243, 51, 54]_3$. Sin embargo, está lejos de ser un código óptimo, puesto que existe un código de parámetros $[243, 51, 85]_3$ y, para un código con dicha longitud y dimensión, la distancia mínima tiene cota superior 122.

El código $\mathcal{R}_3(3,m)$ tiene parámetros $\left[3^m, \binom{m+3}{3} - m, 2 \cdot 3^{m-2}\right]_3$.

7.3.4. Código Reed-Muller ternario $\mathcal{R}_3(r,m)$

En general, los códigos $\mathcal{R}_3(r,m)$ pueden generarse haciendo uso de la construcción $(u+v+w|2u+v|u)$ y, como vimos al principio de las sección, teniendo en cuenta (7.4), se definen como

$$\mathcal{R}_3(r,m) = \Big\{ (u+v+w\,,\, 2u+v\,,\, u) \,:\, u \in \mathcal{R}_3(r,m-1), v \in \mathcal{R}_3(r-1,m-1), w \in \mathcal{R}_3(r-2,m-1) \Big\}$$

De este modo, su matriz generadora $G(r,m)$ es de la forma dada en (7.2), siendo G_U, G_V y G_W las matrices generadoras de los códigos convenientes, como se muestra a continuación:

$$G(r,m) = \begin{bmatrix} G(r-2,m-1) & 0 & 0 \\ G(r-1,m-1) & G(r-1,m-1) & 0 \\ G(r,m-1) & 2G(r,m-1) & G(r,m-1) \end{bmatrix}$$

Las propiedades del código Reed-Muller ternario $\mathcal{R}_3(r,m)$, ya estudiadas en sus formas más sencillas, son las siguientes:

(I) $n(r,m) = 3^m$

(II) $k(r,m) = k(r,m-1) + k(r-1,m-1) + k(r-2,m-1)$

(III) $d(r,m) = \begin{cases} \infty, & r < 0 \\ 3^{m-r/2} & 0 \le r \text{ par} \le 2m \\ 2 \cdot 3^{m-(r+1)/2}, & 1 \le r \text{ impar} \le 2m-1 \\ 1, & r > 2m \end{cases}$

(IV) $\mathcal{R}_3(r,m) \subset \mathcal{R}_3(r+1,m)$

Demostración: Las propiedades (I), (II), (III) son consecuencia de las propiedades de la construcción $(u + v + w \mid 2u + v \mid u)$ por inducción sobre m. La propiedad (IV) también se demuestra por inducción sobre m teniendo en cuenta que $\mathcal{U}' \subset \mathcal{U}$, $\mathcal{V}' \subset \mathcal{V}$ y $\mathcal{W}' \subset \mathcal{W}$ implica $(\mathcal{U}' + \mathcal{V}' + \mathcal{W}' \mid 2\mathcal{U}' + \mathcal{V}' \mid \mathcal{U}') \subset (\mathcal{U} + \mathcal{V} + \mathcal{W} \mid 2\mathcal{U} + \mathcal{V} \mid \mathcal{U})$. □

					$\mathcal{R}_3(0,5)$
				$\mathcal{R}_3(0,4)$	$\mathcal{R}_3(1,5)$
			$\mathcal{R}_3(0,3)$	$\mathcal{R}_3(1,4)$	$\mathcal{R}_3(2,5)$
		$\mathcal{R}_3(0,2)$	$\mathcal{R}_3(1,3)$	$\mathcal{R}_3(2,4)$	$\mathcal{R}_3(3,5)$
$\mathcal{R}_3(-1,0)$	$\mathcal{R}_3(0,1)$	$\mathcal{R}_3(1,2)$	$\mathcal{R}_3(2,3)$	$\mathcal{R}_3(3,4)$	$\mathcal{R}_3(4,5)$
$\mathcal{R}_3(0,0)$	$\mathcal{R}_3(1,1)$	$\mathcal{R}_3(2,2)$	$\mathcal{R}_3(3,3)$	$\mathcal{R}_3(4,4)$	$\mathcal{R}_3(5,5)$
		$\mathcal{R}_3(3,2)$	$\mathcal{R}_3(4,3)$	$\mathcal{R}_3(5,4)$	$\mathcal{R}_3(6,5)$
			$\mathcal{R}_3(5,3)$	$\mathcal{R}_3(6,4)$	$\mathcal{R}_3(7,5)$
				$\mathcal{R}_3(7,4)$	$\mathcal{R}_3(8,5)$
					$\mathcal{R}_3(9,5)$

Cuadro 7.2: Secuencia de construcción de los códigos Reed-Muller sobre el cuerpo finito $\mathbb{F}_3$

Hemos visto que los códigos Reed-Muller ternarios se construyen de forma inductiva haciendo uso de la construcción $(u + v + w \mid 2u + v \mid u)$. De esta manera, componen una secuencia de códigos formados unos a partir de otros. Este hecho se ilustra en la figura 7.2 y, a continuación, se muestran los parámetros de algunos de estos códigos en la tabla 7.3. Observamos que los códigos con *mejores* parámetros, a pesar de no ser óptimos en algún caso, son los códigos que están en el interior de la figura 7.2, pues los códigos que la limitan son poco interesantes.

	n	k	d		n	k	d
$\mathcal{R}_3(r,0)$	1	1	1	$\mathcal{R}_3(5,4)$	81	66	6
$\mathcal{R}_3(-r,0)$	1	0	∞	$\mathcal{R}_3(4,4)$	81	50	9
$\mathcal{R}_3(1,1)$	3	2	2	$\mathcal{R}_3(3,4)$	81	31	18
$\mathcal{R}_3(0,1)$	3	1	3	$\mathcal{R}_3(2,4)$	81	15	27
$\mathcal{R}_3(3,2)$	9	8	2	$\mathcal{R}_3(1,4)$	81	5	54
$\mathcal{R}_3(2,2)$	9	6	3	$\mathcal{R}_3(0,4)$	81	1	81
$\mathcal{R}_3(1,2)$	9	3	6	$\mathcal{R}_3(9,5)$	243	242	2
$\mathcal{R}_3(0,2)$	9	1	9	$\mathcal{R}_3(8,5)$	243	237	3
$\mathcal{R}_3(5,3)$	27	26	2	$\mathcal{R}_3(7,5)$	243	222	6
$\mathcal{R}_3(4,3)$	27	23	3	$\mathcal{R}_3(6,5)$	243	192	9
$\mathcal{R}_3(3,3)$	27	17	6	$\mathcal{R}_3(5,5)$	243	147	18
$\mathcal{R}_3(2,3)$	27	10	9	$\mathcal{R}_3(4,5)$	243	96	27
$\mathcal{R}_3(1,3)$	27	4	18	$\mathcal{R}_3(3,5)$	243	51	54
$\mathcal{R}_3(0,3)$	27	1	27	$\mathcal{R}_3(2,5)$	243	21	81
$\mathcal{R}_3(7,4)$	81	80	2	$\mathcal{R}_3(1,5)$	243	6	162
$\mathcal{R}_3(6,4)$	81	76	3	$\mathcal{R}_3(0,5)$	243	1	243

Cuadro 7.3: Parámetros de los códigos Reed-Muller sobre el cuerpo finito $\mathbb{F}_3$

Para terminar, se expone de forma sucinta y sin demostraciones la definición primitiva de los códigos Reed-Muller ternarios, que puede verse en [KsPa] y [Mass].

Primeramente, sea

$$G_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix}$$

y se define G_m recursivamente como

$$G_m = \begin{bmatrix} G_{m-1} & 0 & 0 \\ G_{m-1} & G_{m-1} & 0 \\ G_{m-1} & 2G_{m-1} & G_{m-1} \end{bmatrix}$$

La fila j-ésima de G_m corresponde a la fila j-ésima del triángulo de Pascal reducida módulo 3, es decir, G_m es una tabla de los coeficientes binomiales reducidos módulo 3.

En [Mass] se prueba que G_m tiene la siguiente propiedad: un código generado por un subconjunto de las filas de G_m cuyos pesos sean $\{w_1, w_2, \ldots, w_k\}$ tiene distancia mínima $\min(w_1, w_2, \ldots, w_k)$. Por tanto, si elegimos todas las filas de G_m cuyos pesos sean $w \geq d$, se genera un código con distancia mínima d. Se dice que dicho código es un código Reed-Muller ternario.

Veamos, usando inducción, que cualquier código Reed-Muller ternario, o cualquier código generado a partir de las filas de G_m, puede generarse recursivamente usando la construcción $(u+v+w|2u+v|u)$.

Sean los códigos de parámetros $[1, 1, 1]_3$ y $[1, 0, \infty]_3$ anteriores. Es claro que cualquier combinación de las filas de G_1 puede obtenerse con la construcción $(u + v + w \mid 2u + v \mid u)$ siendo

- $\mathcal{W} = [1, 1, 1]_3$ si la primera fila de G_1 está incluida;
  $\mathcal{W} = [1, 0, \infty]_3$ en otro caso.
- $\mathcal{V} = [1, 1, 1]_3$ si la segunda fila de G_1 está incluida;
  $\mathcal{V} = [1, 0, \infty]_3$ en otro caso.
- $\mathcal{U} = [1, 1, 1]_3$ si la tercera fila de G_1 está incluida;
  $\mathcal{U} = [1, 0, \infty]_3$ en otro caso.

De forma similar, si G es una matriz generadora obtenida a partir de filas de G_m, entonces, por definición de G_m, G se escribe de la forma siguiente:

$$\begin{bmatrix} G_W & 0 & 0 \\ G_V & G_V & 0 \\ G_U & 2G_U & G_U \end{bmatrix}$$

donde G_W, G_V y G_U consisten en una combinación de filas de G_{m-1}. Claramente, asignando $\mathcal{U}$, $\mathcal{V}$ y $\mathcal{W}$ a los códigos generados por G_U, G_V y G_W, respectivamente, y aplicando la construcción $(u+v+w|2u+v|u)$, se produce el código generado por G. Por inducción, todos los códigos generados por las filas de G_m pueden obtenerse inductivamente con la construcción $(u + v + w \mid 2u + v \mid u)$ usando los códigos $[1, 1, 1]_3$ y $[1, 0, \infty]_3$ como *bloques de construcción*.

Una familia infinita de códigos ternarios con propiedades similares a las de los códigos Reed-Muller binarios pueden construirse recursivamente a partir de los códigos $[1, 1, 1]_3$ y $[1, 0, \infty]_3$.

7.4. Códigos lineales ternarios obtenidos con Maple

Se muestran, a continuación, algunos ejemplos en los que, aplicando técnicas similares a las descritas en los Capítulos 3 y 5 a códigos lineales ternarios, se obtienen códigos próximos a códigos óptimos. Como apéndice mostraremos los códigos MAPLE utilizados para hallar todos los pesos de los códigos.

7.4.1. Código lineal ternario de parámetros $[21, 6, 10]_3$

Sea $\mathcal{C}$ el código lineal ternario cuyas palabras-código tienen la siguiente forma: se colocan seis elementos libres $a_i \in \mathbb{F}_3$, seguidos de todas las sumas posibles de cuatro elementos de los anteriores con subíndices distintos.

$$\mathcal{C} = \left\{ (a_1, a_2, a_3, a_4, a_5, a_6, \sum_4 a_j) \ : \ a_i \in \mathbb{F}_3, \quad i, j \in \{1, \ldots, 6\} \right\} \subset \mathbb{F}_3^{21}$$

La longitud del código $\mathcal{C}$ es

$$n = 6 + \binom{6}{4} = 6 + 15 = 21$$

y la dimensión es $k = 6$, por lo que hay $3^6 = 729$ palabras en el código.

Una matriz generadora de $\mathcal{C}$ tiene la siguiente estructura:

$$G = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 1 \end{array}\right]$$

Debido a que ahora las operaciones son en el cuerpo $\mathbb{F}_3$, los cálculos no son fácilmente realizables a mano y hemos recurrido a MAPLE para hallar todos los pesos del código, en relación al número de palabras con cada peso, y, en consecuencia, la distancia mínima.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{10} & = & 42 \\ A_{11} & = & 42 \\ A_{12} & = & 140 \\ A_{14} & = & 210 \\ A_{15} & = & 70 \\ A_{16} & = & 210 \\ A_{21} & = & 14 \end{array}$$

La distancia mínima del código $\mathcal{C}$ es $d = 10$ y, por tanto, hemos construido un código lineal ternario de parámetros $[21, 6, 10]_3$. Examinando las tablas de [Grassl], observamos que el código óptimo es un código de parámetros $[21, 6, 11]_3$, luego nuestro código $\mathcal{C}$ es un código *casi óptimo*.

Nótese que el correspondiente código binario

$$\mathcal{C}^* = \left\{ (a_1, a_2, a_3, a_4, a_5, a_6, \sum_4 a_j) \ : \ a_i \in \mathbb{F}_2, \quad i, j \in \{1, \ldots, 6\} \right\} \subset \mathbb{F}_2^{21}$$

tiene parámetros $[21, 6, 6]_2$ ya que, si todos los elementos de la cabecera son distintos de cero, $a_1 = a_2 = \ldots = a_6 = 1$, el peso de dicha palabra es 6.

7.4.2. Código lineal ternario de parámetros $[42, 7, 20]_3$

Otra muestra del uso de los métodos expuestos en el Capítulo 3 para códigos lineales ternarios, con resultados no muy favorables, es el siguiente: sea el código de parámetros $[42, 7, d]_3$ cuya cabecera consta de siete elementos libres en el cuerpo $\mathbb{F}_3$ y cuya cola está formada por todas las posibles sumas de cuatro elementos distintos de los anteriores.

$$\mathcal{C} = \left\{ (a_1, a_2, a_3, a_4, a_5, a_6, a_7, \sum_4 a_j) \ : \ a_i \in \mathbb{F}_3, \quad i, j \in \{1, \ldots, 7\} \right\} \subset \mathbb{F}_3^{42}$$

En efecto, la longitud del código $\mathcal{C}$ es

$$n = 7 + \binom{7}{4} = 7 + 35 = 42$$

y la dimensión $k = 7$. Por tanto, el número de palabras-código es $3^7 = 2187$. Una matriz generadora del código tiene la siguiente estructura:

$$G = \left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \cdots & 1 \end{array}\right]$$

Hemos hallado todos los pesos del código, en relación al número de palabras-código con dichos pesos, con ayuda de MAPLE.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{20} & = & 42 \\ A_{21} & = & 28 \\ A_{22} & = & 42 \\ A_{24} & = & 70 \\ A_{25} & = & 210 \\ A_{26} & = & 210 \\ A_{27} & = & 350 \\ A_{28} & = & 210 \\ A_{29} & = & 420 \\ A_{30} & = & 140 \\ A_{31} & = & 294 \\ A_{32} & = & 84 \\ A_{33} & = & 70 \\ A_{42} & = & 16 \end{array}$$

La distancia mínima del código $\mathcal{C}$ es $d = 20$ y, por consiguiente, hemos encontrado un código lineal ternario de parámetros $[42, 7, 20]_3$. Sin embargo, las tablas de [Grassl] nos indican que el código óptimo, para los mismos parámetros de longitud y dimensión, tiene parámetros $[42, 7, 24]_3$.

7.4.3. Código lineal ternario óptimo de parámetros $[126, 6, 81]_3$

Por último, se presenta la construcción de un código lineal ternario óptimo hallado con estas técnicas. Sea el código con seis elementos libres en $\mathbb{F}_3$ en la cabecera y todas las sumas posibles $a_i \pm a_j \pm a_k \pm a_h$ con $i < j < k < h$ en la cola.

$$\mathcal{C} = \left\{ (a_1, a_2, a_3, a_4, a_5, a_6, a_i \pm a_j \pm a_k \pm a_h) \ : \ a_i \in \mathbb{F}_3, \quad i < j < k < h \right\} \subset \mathbb{F}_3^{126}$$

El código $\mathcal{C}$ tiene dimensión $k = 6$ y, puesto que en la cola hay ocho posibilidades para las sumas, su longitud es

$$n = 6 + 8 \cdot \binom{6}{4} = 6 + 8 \cdot 15 = 126$$

Una matriz generadora tiene la siguiente forma:

$$G = \left[\begin{array}{cccccc|cccccccccccccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \cdots & 0 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \cdots & 0 & 2 & \cdots & 1 & \cdots & 1 & \cdots & 2 & \cdots & 2 & \cdots & 1 & \cdots & 2 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 2 & \cdots & 1 & \cdots & 2 & \cdots & 1 & \cdots & 2 & \cdots & 2 & \cdots & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \cdots & 1 & 1 & \cdots & 1 & \cdots & 2 & \cdots & 1 & \cdots & 2 & \cdots & 2 & \cdots & 2 & \cdots & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 2 \end{array}\right]$$

Como en los casos anteriores, recurriendo a MAPLE, hemos calculado todos los pesos del código. A continuación, se muestra su relación con el número de palabras del código.

$$\begin{array}{rcl} A_0 & = & 1 \\ A_{81} & = & 476 \\ A_{90} & = & 252 \end{array}$$

El código $\mathcal{C}$ solo tiene **dos pesos** no nulos y cada uno de ellos es múltiplo de 9, quizá este hecho tenga alguna consecuencia significativa.

De este modo, hemos obtenido un código lineal ternario de parámetros $[126, 6, 81]_3$. Observemos en la siguiente tabla de [Grassl] que, de hecho, es un código óptimo. Sin embargo, existen códigos de parámetros $[124, 6, 81]_3$ y $[125, 6, 81]_3$.

n/k	4	5	6	7	8
124	82	81	81	78-80	75-78
125	83	81	81	79-81	75-79
126	84	82	81	80-81	76-80
127	84	83	81-82	81	77-80
128	85	84	82-83	81-82	78-81

Cuadro 7.4: Bounds on the minimum distance of linear codes over $GF(3)$

```
> with(combinat):
> with(LinearAlgebra[Modular]):

> generomatriz:=proc(LL::list)
> local lista,j,B,k,n;
> k:=6;
> n:=21;
> B:=Matrix(k,n,0,datatype=integer);
> for j from 1 to k do
> B[j,j]:=1;
> end do;
> for j from 1 to n-k do
> lista:=LL[j];
> B[lista[1],6+j]:=1;
> B[lista[2],6+j]:=1;
> B[lista[3],6+j]:=1;
> B[lista[4],6+j]:=1;
> end do;
> B;
> end proc:


> peso:=proc(L::list)
> local j,m,weight;
> m:=nops(L);
> weight:=0;
> for j from 1 to m do
> if (L[j] mod 3)<>0 then
> weight:=weight+1;end if;
> end do;
> weight;
> end proc:


> codepesos:=proc(matriz::Matrix)
> local codeword,combination,weight,j,m,n,k,A,b;
> k:=6;
> n:=21;
> for j from 0 to n do
> A[j]:=0;
> end do;
> for j from 1 to k do
> b[j]:=convert(matriz[j],list);
> end do;
> for m from 1 to 3^k-1 do
> codeword:=[seq(0,i=1..n)];
> combination:=convert(m,base,3);
> for j from 1 to nops(combination) do
> codeword:=(codeword+combination[j]*b[j])
mod 3;
> end do;
> weight:=peso(codeword);
> A[weight]:=A[weight]+1;
> end do;
> for j from 0 to n do;
> if A[j]<>0 then print([j],A[j]);end
if;
> end do;
> A;
> end proc:
```

```
> LL:=choose(6,4):nops(LL):

> C:=generomatriz(LL):

> Rank(3,C):

> pesos:=codepesos(C);
                    [10], 42
                    [11], 42
                    [12], 140
                    [14], 210
                    [15], 70
                    [16], 210
                    [21], 14
```

```
> with(combinat):
> with(LinearAlgebra[Modular]):

> generomatriz:=proc(LL::list)
> local lista,i,j,B,k,n;
> k:=6; n:=126;
> B:=Matrix(k,n,0,datatype=integer);
> for j from 1 to k do B[j,j]:=1; end
do;
> for j from 1 to 15 do
> lista:=LL[j];i:=0;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=1;
> B[lista[3],6+i+j]:=1;
> B[lista[4],6+i+j]:=1;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=15;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=2;
> B[lista[3],6+i+j]:=1;
> B[lista[4],6+i+j]:=1;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=30;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=1;
> B[lista[3],6+i+j]:=2;
> B[lista[4],6+i+j]:=1;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=45;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=1;
> B[lista[3],6+i+j]:=1;
> B[lista[4],6+i+j]:=2;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=60;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=2;
> B[lista[3],6+i+j]:=2;
> B[lista[4],6+i+j]:=1;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=75;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=2;
> B[lista[3],6+i+j]:=1;
> B[lista[4],6+i+j]:=2;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=90;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=1;
> B[lista[3],6+i+j]:=2;
> B[lista[4],6+i+j]:=2;
> end do;
> for j from 1 to 15 do
> lista:=LL[j];i:=105;
> B[lista[1],6+i+j]:=1;
> B[lista[2],6+i+j]:=2;
> B[lista[3],6+i+j]:=2;
> B[lista[4],6+i+j]:=2;
> end do;
> B;
> end proc:

> peso:=proc(L::list)
> local j,m,weight;
> m:=nops(L);
> weight:=0;
> for j from 1 to m do
> if (L[j] mod 3)<>0 then
> weight:=weight+1;end if;
> end do;
> weight;
> end proc:

> codepesos:=proc(matriz::Matrix)
> local codeword,combinat,weight,j,m,n,k,A,b;
> k:=6;
> n:=126;
> for j from 0 to n do
> A[j]:=0;
> end do;
> for j from 1 to k do
> b[j]:=convert(matriz[j],list);
> end do;
> for m from 1 to 3^k-1 do
> codeword:=[seq(0,i=1..n)];
> combinat:=convert(m,base,3);
> for j from 1 to nops(combinat) do
> codeword:=(codeword+combinat[j]*b[j])
mod 3;
> end do;
> weight:=peso(codeword);
> A[weight]:=A[weight]+1;
> end do;
> for j from 0 to n do;
> if A[j]<>0 then print([j],A[j]);end
if;
> end do;
> A;
> end proc:

> LL := choose(6, 4): nops(LL):
> C:=generomatriz(LL):
> Rank(3,C):
> pesos:=codepesos(C);
```

[81], 476

[90], 252

Bibliografía

[Bier] J. Bierbrauer, *Introduction to Coding Theory*, Chapman & Hall, CRC, 2005.

[BoJac] I. Bouyukliev, E. Jacobsson, "Results on binary linear codes with minimum distance 8 and 10", *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6089-6093, Sep. 2011.

[BoJaf] I. Bouyukliev, D. Jaffe, "Optimal binary linear codes of dimension at most seven", *Discrete Mathematics*, 226, pp.51-70, 2001.

[BoJaVe] I. Bouyukliev, D. Jaffe, V. Vavrek, "The smallest length of eight-dimensional binary linear codes with prescribed minimum distance", *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1539-1544, Jul. 2000.

[Ding] K. Ding, C. Ding, "Binary linear codes with three weights", *IEEE Communications Letters*, vol. 18, no. 11, pp. 1879-1882, Nov. 2014.

[DoGuSi] S. Dodunekov, S. Guritman, J. Simonis, "Some new results on the minimum length of binary linear codes of dimension nine", *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2543-2546, Nov. 1999.

[GuBh] T.A. Gulliver, V.K. Bhargava, "New optimal binary linear codes of dimensions 9 and 10", *IEEE Trans. Inf. Theory*, vol. 43, no. 1, pp. 314-316, Jan. 1997.

[Hill] R. Hill, *A First Course in Coding Theory*, Oxford University Press, 1986.

[Hoff] D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, *Coding Theory, The Essentials*, Marcel Dekker, P.A.M., New York, 1991.

[HuPl] W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[KsPa] F.R. Kschischang, S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings", *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 227-246, Mar. 1992.

[LiPi] R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer, 1998.

[Mar] J.E. Marcos, comunicación personal, 2019.

[Mass] J.L. Massey, D.J. Costello, J. Justesen, "Polynomial weights and code constructions", *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 101-110, Jan. 1973.

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

[Sha] C.E. Shannon, "A mathematical theory of communication", *Bell Syst. Tech. J.*, 27, pp. 379-423 and 623-656, 1948.

[Til] H.v. Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance", *Discrete Mathematics*, 33, pp. 197-207, 1981.

[WaDiXu] Q. Wang, K. Ding, R. Xue, "Binary linear codes with two weights", *IEEE Communications Letters*, vol. 19, no. 7, pp. 1097-1100, Jul. 2015.

[Grassl] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes". Online available at `http://www.codetables.de/`

[SchSch] W.Ch. Schmid, R. Schürer, `http://mint.sbg.ac.at/`