Matemáticas y sus Aplicaciones 4, Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, ISBN: 978 607 487 791 5

Capítulo 1

Códigos de Hamming

Carlos Alberto López Andrade
FCFM, BUAP

Resumen

Los códigos detectores-correctores de errores son el medio por el cual los errores que pueden ser introducidos en los datos digitales, como resultado de la transmisión a través de un canal de comunicación, pueden ser corregidos en base a los datos recibidos. Los códigos de Hamming son probablemente entre los códigos correctores de errores los más famosos. Fueron descubiertos de forma independiente por Marcel Golay en 1949 y Richard Hamming en 1950. Son códigos correctores de un sólo error, muy fáciles de codificar y decodificar. En este trabajo, a través de un código binario de Hamming, se introducen los conceptos básicos de la Teoría de Códigos Lineales Detectores-Correctores de Errores y posteriormente se describen los códigos de Hamming, cabe señalar que este es un capítulo de libro de divulgación, enfocado a introducir en el tema, de una manera sencilla, a los alumnos de los primeros semestres de las licenciaturas en Matemáticas, Matemáticas Aplicadas, Física, Física Aplicada y Ciencias de la Computación, entre otros. Este no es un material nuevo, se puede consultar en los diversos textos citados en las referencias, más sí la forma en que se divulga.

1. Introducción

Todo dispositivo de lectura o grabación de CD's o DVD's o unidad de disco duro, emplea códigos detectores-correctores de errores para proteger los datos grabados, cada llamada telefónica hecha a través del teléfono móvil los emplea, así como cada fotografía transmitida desde una nave espacial a la Tierra. Cada paquete transmitido a través de internet tiene una envoltura protectora de codificación utilizada para determinar si el paquete ha sido recibido correctamente. Incluso en el comercio cotidiano están presentes los códigos detectores-correctores de errores; por ejemplo, los códigos de barras que identifican los distintos productos en los supermercados y el ISBN (International Standard Book Number) para la catalogación de libros.

Varias familias de códigos lineales fueron construidas en los años 50's y principios de los años 60's del siglo XX, entre las cuales se encuentran los códigos de Hamming, Golay, Reed-Muller y los códigos cíclicos, entre otros.

La leyenda dice que Richard Hamming estaba tan frustrado de que la computadora se parara cada vez que detectaba un error, que se ensimismó en una pila de tarjetas perforadas, pensó en una forma en la que la computadora fuera capaz no sólo de detectar el error sino también de corregirlo automáticamente y volvió con su hoy en día famoso código de Hamming.

La idea en los códigos correctores de errores consiste en añadir información redundante de tal manera que es posible detectar o incluso corregir errores después de la transmisión. La adición de un símbolo de chequeo de paridad permite detectar un error tal como sucede con el código ISBN para los libros, y el Código Universal de Producto (UPC) para los productos.

En esta sección introductoria ilustramos las ideas centrales de la teoría de la información (cf. [3]) por medio de un par específico de modelos matemáticos, la fuente simétrica binaria y el canal símetrico binario.

La *fuente simétrica binaria* (la fuente, para abreviar) es un objeto que emite uno de dos posibles símbolos, los cuales tomamos como " 0 " y " 1 ", a una tasa de R símbolos por unidad de tiempo. Llamaremos a estos símbolos bits, una abreviación de dígitos binarios. Los bits emitidos por la fuente son aleatorios, y un " 0 " es igualmente probable de ser emitido que un " 1 ".

El *canal simétrico binario* (CSB para abreviar) es un objeto a través del cual es posible transmitir un bit por unidad de tiempo. Sin embargo el canal no es completamente fiable; hay una probabilidad fija p (llamada la probabilidad de errores de bits en bruto), $0 \leq p < \frac{1}{2}$, de que el bit de salida no sea el mismo bit de entrada Figura 1.

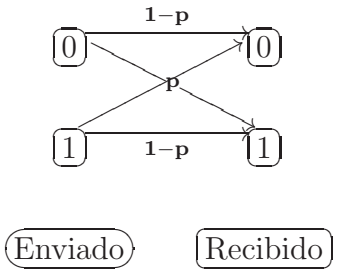

Figura 1: Canal simétrico binario (CBS)

Ahora imaginemos a dos individuos, el remitente (emisor) y el receptor. El remitente debe tratar de transmitir al receptor con la mayor precisión posible la salida de la fuente, y el único vínculo de comunicación permitido entre los dos es el CSB descrito arriba.

2. Codificación

Los códigos detectores correctores de errores fueron inventados para detectar y corregir errores producidos por el ruido en los canales de comunicación (cf. [2]). Vamos a codificar mensajes para darles alguna protección contra errores en el canal. En la Figura 2 se muestra un sistema general de transmisión de información.

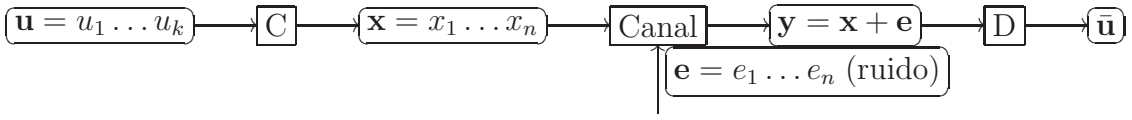

Figura 2: Sistema general de transmisión de información

Un campo es una estructura algebraica en donde se puede sumar, restar, multiplicar y dividir. Formalmente un campo es un conjunto $\mathbb{F}$ junto con dos operaciones binarias, " $+$ " y " $\cdot$ ", tales que

1. $\mathbb{F}$ es un grupo abeliano bajo " $+$ ", cuyo elemento neutro es 0.

2. Los elementos distintos de cero de $\mathbb{F}$ forman un grupo abeliano bajo " $\cdot$ ", cuyo elemento neutro es 1.

3. La ley distributiva $a \cdot (b + c) = a \cdot b + a \cdot c$ se cumple.

Un campo es llamado finito o infinito dependiendo de si el conjunto es finito o infinito. Como ejemplos de campos infinitos tenemos al campo de los números reales, al campo de los números racionales, al campo de los números complejos y al campo de las funciones racionales definidas sobre un campo.

Un campo finito extremadamente interesante en todas las aplicaciones digitales es $\mathbb{F}_2 = \{0, 1\}$, definido a través de las operaciones binarias " $+$ " y " $\cdot$ " dadas por las Tablas de Cayley,

$+$	0	1
0	0	1
1	1	0

y

$\cdot$	0	1
0	0	0
1	0	1

,

es decir, en $\mathbb{F}_2$, realizamos aritmética módulo 2.

Sea $\mathbb{F}_2^n$ el conjunto de n-adas de elementos de $\mathbb{F}_2$, $\mathbb{F}_2^n$ es un espacio vectorial sobre $\mathbb{F}_2$. Se dice que $\mathcal{C}$ es un *código de longitud n sobre* $\mathbb{F}_2$ o que $\mathcal{C}$ es un *código binario de longitud n* si $\mathcal{C}$ es un

subconjunto de $\mathbb{F}_2^n$. Un (n, M)-*código* $\mathcal{C}$ sobre $\mathbb{F}_2$ es un código de longitud n y tamaño M. A los elementos de un código $\mathcal{C}$ se les llama *palabras-código*.

Un bloque de mensaje de k símbolos $\mathbf{u} = u_1u_2 \dots u_k$ $(u_i \in \mathbb{F}_2)$ será codificado en una palabra-código $\mathbf{x} = x_1x_2 \dots x_n$ $(x_i \in \mathbb{F}_2)$ donde $n \geq k$.

Si utilizamos un método de codificación sistemático la primera parte de la palabra-código consistirá del mensaje mismo $x_1 = u_1, x_2 = u_2, \dots, x_k = u_k$, seguida por $n - k$ símbolos comprobadores o checadores de paridad -bits de redundancia- $x_{k+1}, \dots, x_n$. Los símbolos comprobadores son escogidos de manera que las palabras-código $\mathbf{x}$ satisfagan

$$H\mathbf{x}^t = \mathbf{0} \tag{1}$$

donde $H \in \mathcal{M}_{(n-k)\times n}$ es la *matriz comprobadora de paridad estándar* o *matriz de chequeo de paridad estándar* del código, dada por

$$H = [A|I_{n-k}], \tag{2}$$

donde $A \in \mathcal{M}_{(n-k)\times k}(\mathbb{F}_2)$ fija e $I_{n-k} \in \mathcal{M}_{(n-k)\times(n-k)}(\mathbb{F}_2)$ es la matriz identidad, la aritmética en la ecuación (1) es realizada módulo 2.

Podemos usar la ecuación (1) como nuestra definición general de código lineal binario.

Definición 2.1. Sea $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_2)$ arbitraria. Llamamos código lineal binario $\mathcal{C}$ con matriz de chequeo de paridad H al conjunto que consiste de todos los vectores $\mathbf{x} \in \mathbb{F}_2^n$ tales que $H\mathbf{x}^t = \mathbf{0}$, i.e.,

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_2^n : H\mathbf{x}^t = \mathbf{0}\}.$$

Es conveniente, pero no esencial, que H tenga la forma mostrada en (2). A lo largo de este trabajo desarrollamos un ejemplo que nos será útil para ilustrar los distintos conceptos que se presentarán.

Ejemplo 2.2. Sea

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \tag{3}$$

en $\mathcal{M}_{3\times 7}(\mathbb{F}_2)$ la matriz de chequeo de paridad del código lineal $\mathcal{H}$ dada como en (2) donde

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \tag{4}$$

$n = 7$ y $k = 4$. Cada palabra-código contiene cuatro símbolos de mensaje x_1, x_2, x_3, x_4 y tres símbolos checadores x_5, x_6, x_7 tales que satisfacen las ecuaciones

$$\begin{aligned} x_1 + x_2 + x_4 + x_5 &= 0 \\ x_1 + x_3 + x_4 + x_6 &= 0 \\ x_2 + x_3 + x_4 + x_7 &= 0. \end{aligned} \tag{5}$$

Las ecuaciones (5) son llamadas las *ecuaciones de chequeo de paridad*, o simplemente *chequeos de paridad del código lineal* $\mathcal{H}$. Observemos que la suma de las componentes de toda palabra-código involucradas en cada una de las ecuaciones debe ser igual a un número par, es decir, debe sumar 0 módulo 2.

Si el mensaje es $\mathbf{u} = 0110$ entonces los símbolos de mensaje son $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0$ y los símbolos checadores son $x_5 = 1, x_6 = 1, x_7 = 0$, así, el mensaje $\mathbf{u} = 0110$ está codificado en la palabra-código $\mathbf{x} = 0110110$, como se puede apreciar la palabra-código comienza con el mensaje. Como cada uno de los 4 símbolos de mensaje es 0 o 1, hay 2^4 mensajes y por ende 2^4 palabras-códigos.

En la siguiente tabla se exhiben todos y cada uno de los posibles mensajes con su palabra-código correspondiente y el peso de cada palabra-código, el cual se define como el número de componentes de $\mathbf{x}$ distintas de cero, del código lineal $\mathcal{H}$.

$\mathbf{u} = u_1u_2u_3u_4$	$\mathbf{x} = x_1x_2x_3x_4x_5x_6x_7$	$wt(\mathbf{x})$	$\mathbf{u} = u_1u_2u_3u_4$	$\mathbf{x} = x_1x_2x_3x_4x_5x_6x_7$	$wt(\mathbf{x})$
0000	0000000	0	1000	1000110	3
0001	0001111	4	1001	1001001	3
0010	0010011	3	1010	1010101	4
0011	0011100	3	1011	1011010	4
0100	0100101	3	1100	1100011	4
0101	0101010	3	1101	1101100	4
0110	0110110	4	1110	1110000	3
0111	0111001	4	1111	1111111	7

□

De la Definición 2.1 se desprende que $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_2^n$ ya que si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ y $\lambda \in \mathbb{F}_2$ entonces $H(\mathbf{x}+\mathbf{y})^t = H\mathbf{x}^t + H\mathbf{y}^t = \mathbf{0} + \mathbf{0} = \mathbf{0}$ y $H(\lambda\mathbf{x})^t = H\lambda\mathbf{x}^t = \lambda H\mathbf{x}^t = \lambda\mathbf{0} = \mathbf{0}$, i.e., $H(\mathbf{x}+\mathbf{y})^t = \mathbf{0}$ y $H(\lambda\mathbf{x})^t = \mathbf{0}$ para cada $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ y $\lambda \in \mathbb{F}_2$, por consiguiente, si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ y $\lambda \in \mathbb{F}_2$ entonces $\mathbf{x}+\mathbf{y} \in \mathcal{C}$ y $\lambda\mathbf{x} \in \mathcal{C}$. De hecho, $\mathcal{C}$ es el espacio vectorial de las soluciones de la ecuación matricial $H\mathbf{x}^t = \mathbf{0}$ o equivalentemente es el espacio vectorial de las soluciones del sistema de ecuaciones lineales homogéneas que tiene a la matriz de chequeo de paridad H como la matriz asociada al sistema de ecuaciones lineales homogéneas o equivalentemente es el espacio nulo de la matriz H.

Ejemplo 2.3. Continuación del Ejemplo 2.2. Sea H la matriz del Ejemplo 2.2, dicha matriz es equivalente a la matriz escalonada reducida por filas

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{6}$$

Deseamos resolver el sistema de ecuaciones lineales homogéneas cuya matriz asociada al sistema es (6), para ello, tenemos que x_3, x_5, x_6 y x_7 son variables libres entonces el sistema de ecuaciones lineales homogéneas (5) es equivalente a

$$\begin{aligned} x_1 &= x_3 + x_5 + x_7 \\ x_2 &= x_3 + x_5 + x_6 \\ x_4 &= x_5 + x_6 + x_7 \end{aligned} \tag{7}$$

cuyo espacio vectorial de soluciones tiene al conjunto

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

como una base, tomemos a estos vectores como los vectores fila de la matriz

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{8}$$

la matriz (8) es equivalente a la matriz escalonada reducida por filas

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{9}$$

luego la matriz (9) genera al espacio de soluciones de la ecuación matricial $H\mathbf{x}^t = \mathbf{0}$ donde H es la matriz dada por (3). Tal espacio de soluciones es el código lineal $\mathcal{H}$ cuyas palabras-código están enlistadas en la Tabla del Ejemplo 2.2, luego la matriz G es una matriz generadora del código lineal $\mathcal{H}$, la matriz dada por (8) también es una matriz generadora del mismo código lineal. Obsérvese que la matriz G tiene la forma $[I_4| - A^t]$, i.e.,

$$G = [I_4| - A^t] \tag{10}$$

donde A es la matriz dada por (4) y toda $\mathbf{x} \in \mathcal{H}$ es tal que $\mathbf{x} = \mathbf{u}G$.

□

Si un código lineal $\mathcal{C}$, usando el método de codificación sistemático, tiene como matriz generadora a $G = [I_k| - A^t]$ donde $A \in \mathcal{M}_{(n-k)\times k}(\mathbb{F}_2)$ se dice que G es la *matriz generadora estándar* del código lineal $\mathcal{C}$.

Proposición 2.4. *Si $\mathcal{C}$ es un código lineal binario con matriz de chequeo de paridad $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_2)$, entonces su matriz generadora está dada por $G = [I_k| - A^t]$ y viceversa.*

Demostración. Si el mensaje es $\mathbf{u} = u_1 \cdots u_k$, entonces $\mathbf{x} = x_1 \cdots x_n \in \mathcal{C}$ es tal que $x_1 = u_1, \ldots, x_k = u_k$, de ahí que,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = I_k \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}.$$

A partir de (1) y (2), tenemos que

$$[A|I_{n-k}] \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{0}$$

entonces

$$\mathbf{0} = A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + I_{n-k} \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}$$

esto implica que,

$$\begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

por consiguiente,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \\ x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} I_k \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} \\ -A \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} \end{pmatrix} = \begin{pmatrix} I_k \\ -A \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}, \text{ i.e., } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} I_k \\ -A \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix},$$

trasponiendo la última ecuación, obtenemos $\mathbf{x} = [x_1 x_2 \dots x_n] = [u_1 \dots u_k][I_k| - A^t] = \mathbf{u}G$, donde $G = [I_k| - A^t]$.

Por lo tanto,

$$\mathbf{x} = \mathbf{u}G, \tag{11}$$

" $\mathbf{u}$ " es el mensaje y " $\mathbf{x}$ " la palabra-código correspondiente. □

De (11) se sigue que un código lineal binario $\mathcal{C}$ es el espacio fila de su matriz generadora.

Proposición 2.5. *Si $\mathcal{C}$ es un código lineal binario con matriz de chequeo de paridad $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_2)$, entonces dim $\mathcal{C} = k$ y $|\mathcal{C}| = 2^k$.*

Demostración. Como $rango(H) = n-k$ entonces $nulidad(H) = n-(n-k) = k$, por consiguiente, $dim\ \mathcal{C} = k$ y toda palabra-código se puede escribir como combinación lineal de k vectores en $\mathcal{C}$, i.e., $\mathbf{x} = \sum_{i=1}^{k} \alpha_i \mathbf{x}_i$ donde $\alpha_i \in \mathbb{F}_2$ y $\mathbf{x}_i \in \mathcal{C}$, $i = 1, \dots, k$. Hay 2^k de tales combinaciones lineales, por lo tanto, $|\mathcal{C}| = 2^k$. □

Definición 2.6. Un $[n, k]$-código lineal sobre $\mathbb{F}_2$ es un subespacio k-dimensional del espacio vectorial n-dimensional $\mathbb{F}_2^n$; n es llamado la longitud del código y k la dimensión.

Usualmente la matriz de chequeo de paridad H de un $[n, k]$-código lineal $\mathcal{C}$ es una matriz de tamaño $(n-k) \times n$ de la forma $H = [A|I_{n-k}]$, sin embargo, H no necesariamente debe tener esta forma ya que si H es equivalente a una matriz escalonada reducida por filas H', entonces el espacio nulo de H' es igual al espacio nulo de H, a saber, $\mathcal{C}$. Así H' también es una matriz de chequeo de paridad del $[n, k]$-código lineal $\mathcal{C}$.

Un chequeo de paridad en un $[n, k]$-código lineal $\mathcal{C}$ es cualquier vector fila $\mathbf{h}$ tal que $\mathbf{h}\mathbf{x}^t = 0$ para cada palabra-código $\mathbf{x} \in \mathcal{C}$. Cualquier conjunto maximal de $n-r$ chequeos de paridad linealmente independientes pueden ser usados como las filas de una matriz de chequeo de paridad H de $\mathcal{C}$. Por otro lado, cualquier conjunto maximal de k palabras-código linealmente independientes tomadas de un código dado $\mathcal{C}$ pueden ser usadas como las filas de una matriz generadora para ese código.

Definición 2.7. Sea $\mathcal{C}$ un $[n, k]$-código lineal sobre $\mathbb{F}_2$. Una matriz G cuyo espacio fila es igual a $\mathcal{C}$ es llamada una matriz generadora para $\mathcal{C}$. Recíprocamente, si G es una matriz con entradas en $\mathbb{F}_2$, su espacio fila es llamado el código lineal generado por G.

Hay una estrecha relación entre la matriz de chequeo de paridad y la matriz generadora de un código lineal como se puede observar a través de la siguiente proposición.

Proposición 2.8. *Si $\mathcal{C}$ es un $[n, k]$-código lineal sobre $\mathbb{F}_2$ con matriz de chequeo de paridad H y matriz generadora G entonces $HG^t = 0$ o $GH^t = 0$.*

Demostración. Como $\mathbf{x} = \mathbf{u}G$ para cada $\mathbf{x} \in \mathcal{C}$ y $\mathbf{u} \in \mathbb{F}_2^k$ entonces $\mathbf{x}^t = G^t\mathbf{u}^t$, pero $H\mathbf{x}^t = \mathbf{0}$, de ahí que, $\mathbf{0} = H\mathbf{x}^t = HG^t\mathbf{u}^t$, i.e., $\mathbf{0} = HG^t\mathbf{u}^t$ para cada $\mathbf{u} \in \mathbb{F}_2^k$, por consiguiente, $HG^t = 0$ o bien, $GH^t = 0$. □

3. Decodificación

Supóngase que el mensaje $\mathbf{u} = u_1 \dots u_k$ es codificado en la palabra-código $\mathbf{x} = x_1 \dots x_n$ la cual es enviada por el canal, debido al ruido del canal, el vector recibido $\mathbf{y} = y_1 \dots y_n$ quizá sea diferente de $\mathbf{x}$. Definimos el *vector error*

$$\mathbf{e} = \mathbf{y} - \mathbf{x} = e_1 \dots e_n. \tag{12}$$

Si al recibir la palabra codificada después del envío por el canal de comunicación el i-ésimo símbolo es correcto, $e_i = 0$ y tiene probabilidad $1 - p$, por otro lado, si el i-ésimo símbolo es equivocado $e_i = 1$ con probabilidad p donde p es tal que $0 \leq p < \frac{1}{2}$. Así, describimos la acción del canal diciendo que distorsiona la palabra-código $\mathbf{x}$ al sumarle el vector error $\mathbf{e}$.

La decodificación Figura 2 debe decidir a partir de $\mathbf{y}$ que mensaje $\mathbf{u}$ o (usualmente más simple) que palabra-código $\mathbf{x}$ fue transmitida. Por supuesto es suficiente si la decodificacción encuentra $\mathbf{e}$, pues $\mathbf{x} = \mathbf{y} - \mathbf{e}$. Ahora bien, la decodificación nunca puede ser positiva si no sabemos lo que $\mathbf{e}$ fue. Por consiguiente, la estrategia será escoger el vector error $\mathbf{e}$ más probable dado que $\mathbf{y}$ fue recibido. Dadas las palabras-código todas son igualmente probables, esta estrategia es óptima en el sentido de que minimiza la probabilidad de que la decodificación hecha sea equivocada, y es llamada *decodificación probabilística máxima*. Para describir cómo funciona el decodificador, necesitamos las siguientes definiciones y sus derivados.

Definición 3.1. La *distancia de Hamming* entre dos vectores $\mathbf{x} = (x_1, \dots, x_n)$ y $\mathbf{y} = (y_1, \dots, y_n)$ en $\mathbb{F}_2^n$, lo cual denotamos por $d(\mathbf{x}, \mathbf{y})$, se define como

$$d(\mathbf{x}, \mathbf{y}) = |\{i | 1 \leq i \leq n, x_i \neq y_i\}| \tag{13}$$

Definición 3.2. El *peso de Hamming* de un vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_2^n$, lo cual denotamos por $wt(\mathbf{x})$, se define como

$$wt(\mathbf{x}) = |\{i | 1 \leq i \leq n, x_i \neq 0\}| \tag{14}$$

De las definiciones 3.1 y 3.2 se sigue que $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$, ya que si $s = d(\mathbf{x}, \mathbf{y})$, entonces hay s coordenadas en las que $\mathbf{x}$ y $\mathbf{y}$ difieren y $n - s$ coordenadas en las que $\mathbf{x}$ y $\mathbf{y}$ coinciden luego en la diferencia $\mathbf{x} - \mathbf{y}$ hay $n - s$ ceros y s coordenas distintas de cero, así $wt(\mathbf{x} - \mathbf{y}) = s$.

Definición 3.3. Definimos *la intersección de vectores binarios* $\mathbf{x} = (x_1, \dots, x_n)$ y $\mathbf{y} = (y_1, \dots, y_n)$ como el vector $\mathbf{x} * \mathbf{y} = (x_1 y_1, \dots, x_n y_n)$, el cual tiene 1's sólo donde $\mathbf{x}$ y $\mathbf{y}$ los tienen.

Lema 3.4. *Si* $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_2^n$ *entonces*

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} * \mathbf{y}).$$

Demostración. Sean $wt(\mathbf{x}) = p$ y $wt(\mathbf{y}) = q$, supóngase, sin pérdida de generalidad que $0 \leq p \leq q \leq n$. Si $0 = p = q$ entonces $\mathbf{x} = \mathbf{0} = \mathbf{y}$ y el resultado es trivialmente cierto. Si $0 = p < q$ entonces $\mathbf{x} = \mathbf{0}$ y $\mathbf{x}+\mathbf{y} = \mathbf{y}$, de ahí que, $wt(\mathbf{x}+\mathbf{y}) = q$, además $\mathbf{x}*\mathbf{y} = \mathbf{0}$ y $wt(\mathbf{x}*\mathbf{y}) = 0$, por consiguiente, $wt(\mathbf{x}+\mathbf{y}) = q = 0+q-2\cdot 0 = wt(\mathbf{x})+wt(\mathbf{y})-2wt(\mathbf{x}*\mathbf{y})$, i.e., $wt(\mathbf{x}+\mathbf{y}) = wt(\mathbf{x})+wt(\mathbf{y})-2wt(\mathbf{x}*\mathbf{y})$. Si $0 < p \leq q$ y $r = wt(\mathbf{x}*\mathbf{y})$ entonces $\mathbf{x}$ y $\mathbf{y}$ coinciden en r coordenadas, de ahí que, $r \leq p \leq q$. Hay $p - r$ coordenadas con 1's en $\mathbf{x}$ ninguna de las cuales coincide con $q - r$ coordenadas con 1's en $\mathbf{y}$. Entonces, al sumar $\mathbf{x}$ y $\mathbf{y}$ se obtienen r coordenadas con 0's y hay $(p - r) + (q - r)$ coordenadas con 1's, las coordenadas restantes tienen 0's, así, $wt(\mathbf{x} + \mathbf{y}) = p + q - 2r$, por otro lado, $wt(\mathbf{x})+wt(\mathbf{y})-2wt(\mathbf{x}*\mathbf{y}) = p+q-2r$, por lo tanto, $wt(\mathbf{x}+\mathbf{y}) = wt(\mathbf{x})+wt(\mathbf{y})-2wt(\mathbf{x}*\mathbf{y})$, con lo cual queda establecido el resultado. □

Teorema 3.5. *La función $d : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{N} \cup \{0\}$ dada por $d(\mathbf{x}, \mathbf{y})$ satisface las siguientes propiedades para toda $\mathbf{x}, \mathbf{y}, \mathbf{z}$ en $\mathbb{F}_2^n$.*

1. *$d(\mathbf{x}, \mathbf{y}) \geq 0$ y $d(\mathbf{x}, \mathbf{y}) = 0$ sí y sólo si $\mathbf{x} = \mathbf{y}$,*
2. *$d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$,*
3. *$d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.*

Por lo tanto, $(\mathbb{F}_2^n, d)$ es un espacio métrico.

Demostración. Sean $\mathbf{x}, \mathbf{y}$ en $\mathbb{F}_2^n$, si $\mathbf{x} = \mathbf{y}$ entonces $d(\mathbf{x}, \mathbf{y}) = 0$. Si $\mathbf{x} \neq \mathbf{y}$ entonces $\mathbf{x}$ y $\mathbf{y}$ difieren en al menos una coordenada, de ahí que, $d(\mathbf{x}, \mathbf{y}) \geq 1 > 0$. De cualquier forma, para cualquier $\mathbf{x}, \mathbf{y}$ en $\mathbb{F}_2^n$, $d(\mathbf{x}, \mathbf{y}) \geq 0$. Ahora bien, si $d(\mathbf{x}, \mathbf{y}) = 0$, esto significa que hay cero coordenadas en las que $\mathbf{x}$ y $\mathbf{y}$ difieren, es decir, $\mathbf{x} = \mathbf{y}$. Por consiguiente, $d(\mathbf{x}, \mathbf{y}) = 0$ sí y sólo si $\mathbf{x} = \mathbf{y}$. Por otro lado, $d(\mathbf{x}, \mathbf{y}) = |\{i|1 \leq i \leq n, x_i \neq y_i\}| = |\{i|1 \leq i \leq n, y_i \neq x_i\}| = d(\mathbf{y}, \mathbf{x})$, i.e., $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$. Finalmente, como $wt(\mathbf{x} - \mathbf{y}) = wt(\mathbf{x} + \mathbf{y})$ y $2\mathbf{z} = \mathbf{0}$ tenemos que:

$$\begin{aligned}
d(\mathbf{x}, \mathbf{y}) &= wt(\mathbf{x} - \mathbf{y}) \\
&= wt(\mathbf{x} + \mathbf{y}) \\
&= wt(\mathbf{x} + 2\mathbf{z} + \mathbf{y}) \\
&= wt((\mathbf{x} + \mathbf{z}) + (\mathbf{z} + \mathbf{y})) \\
&= wt(\mathbf{x} + \mathbf{z}) + wt(\mathbf{z} + \mathbf{y}) - 2wt((\mathbf{x} + \mathbf{z}) * (\mathbf{z} + \mathbf{y})) \\
&\leq wt(\mathbf{x} + \mathbf{z}) + wt(\mathbf{z} + \mathbf{y}) \\
&= wt(\mathbf{x} - \mathbf{z}) + wt(\mathbf{z} - \mathbf{y}) \\
&= d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})
\end{aligned}$$

de ahí que, $d(\mathbf{x},\mathbf{y}) \leq d(\mathbf{x},\mathbf{z}) + d(\mathbf{z},\mathbf{y})$. Por lo tanto, d es una distancia, llamada distancia de Hamming y $(\mathbb{F}_2^n, d)$ resulta un espacio métrico. □

Los errores en cada coordenada ocurren con probabilidad p, si consideramos las palabras-código $\mathbf{x}$ del $[7,4]$-código lineal $\mathcal{H}$ del Ejemplo 2.2 y si $\mathbf{v}$ es algún vector fijo de peso a, $0 \leq a \leq 7$, entonces la probabilidad de que $\mathbf{e} = \mathbf{v}$ es $p^a(1-p)^{7-a}$, i.e.,

$$Prob\{\mathbf{e} = \mathbf{v}\} = p^a(1-p)^{7-a} \tag{15}$$

por ejemplo;

$Prob\{\mathbf{e} = 0000000\} = (1-p)^7$ (0 errores o 7 éxitos en los siete símbolos),
$Prob\{\mathbf{e} = 0100000\} = p(1-p)^6$ (1 error o 6 éxitos en los siete símbolos),
$Prob\{\mathbf{e} = 0110000\} = p^2(1-p)^5$ (2 errores o 5 éxitos en los siete símbolos).

Como $p < \frac{1}{2}$, tenemos $2p < 1$, i.e., $p < 1-p$, o bien, $1-p > p$, de donde, $(1-p)^7 = (1-p)^6(1-p) > (1-p)^6 p$, i.e., $(1-p)^7 > p(1-p)^6$ pero $p(1-p)^6 = p(1-p)^5(1-p) > p(1-p)^5 p = p^2(1-p)^5$ entonces $p(1-p)^6 > p^2(1-p)^5$, etc.

De ahí que, $(1-p)^7 > p(1-p)^6 > p^2(1-p)^5 > \ldots$ Por consiguiente, un vector error particular de peso 1 es más probable que un vector error particular de peso 2, y así sucesivamente.

Así, la estrategia de decodificación consiste en decodificar $\mathbf{y}$ como la palabra-código $\mathbf{x}$ más cercana (más cercana con respecto a la distancia de Hamming), esto es, escoger el vector error $\mathbf{e}$ que tiene peso más pequeño, esto es llamado *decodificación de vecino más cercano*. Por consiguiente, en un CSB, decodificación probabilística máxima y decodificación de vecino más cercano son equivalentes.

Un esquema de decodificación de fuerza bruta para un $[n,k]$-código lineal binario $\mathcal{C}$ consiste en comparar $\mathbf{y}$ con todas las 2^k palabras-código y escoger la más cercana, esto es viable para códigos pequeños pero si k es grande ¡esto es imposible!

El tercer parámetro importante de un código $\mathcal{C}$, además de la longitud y dimensión, es la distancia mínima de Hamming entre sus palabras-código.

Definición 3.6. La *distancia mínima de Hamming* (ó *distancia mínima*) de $\mathcal{C}$, lo cual denotamos por d (ó $d_{\text{mín}}(\mathcal{C})$), se define como

$$d = \text{mín}\{d(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}, \tag{16}$$

o bien,

$$d = \text{mín}\{wt(\mathbf{u}-\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\} \tag{17}$$

Un código lineal $\mathcal{C}$ de longitud n, dimensión k y distancia mínima d será llamado un $[n,k,d]$-*código lineal*.

Teorema 3.7. *La distancia mínima de un código lineal* $\mathcal{C}$ *es el peso mínimo de cada palabra-código diferente de cero.*

Demostración. Sea d la distancia mínima de un código lineal $\mathcal{C}$, i.e., $d = \text{mín}\{d(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\} = \text{mín}\{wt(\mathbf{u}-\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}$, como $\mathbf{u},\mathbf{v} \in \mathcal{C}$ y $\mathbf{u} \neq \mathbf{v}$ entonces $\mathbf{w} := \mathbf{u}-\mathbf{v} \in \mathcal{C}$ y $\mathbf{w} \neq \mathbf{0}$, de ahí que, $\text{mín}\{wt(\mathbf{u}-\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\} = \text{mín}\{wt(\mathbf{w}) : \mathbf{w} \in \mathcal{C}, \mathbf{w} \neq \mathbf{0}\}$, por lo tanto, $d = \text{mín}\{wt(\mathbf{w}) : \mathbf{w} \in \mathcal{C}, \mathbf{w} \neq \mathbf{0}\}$. □

La distancia mínima del código lineal $\mathcal{H}$ de los Ejemplos 2.2 y 2.3 es $d = 3$, por consiguiente, el código lineal $\mathcal{H}$ es un $[7,4,3]$-código lineal.

La distancia mínima del código juega un papel esencial en la respuesta a la pregunta ¿cuántos errores puede corregir un código?, pero antes de responder dicha pregunta damos la siguiente definición.

Definición 3.8. La *esfera (ó esfera de Hamming) de radio* r *y centro* $\mathbf{u}$, lo cual denotamos por $B_r(\mathbf{u})$, se define como

$$B_r(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_2^n : d(\mathbf{u},\mathbf{v}) \leq r\}. \tag{18}$$

Teorema 3.9. *Un código* $\mathcal{C}$ *con distancia mínima* d *(o peso mínimo* d*) puede corregir* $[\frac{1}{2}(d-1)]$ *o menos errores.*

Demostración. Sea $t = [\frac{1}{2}(d-1)]$ (t es el mayor entero menor o igual a $\frac{1}{2}(d-1)$), si una palabra-código $\mathbf{x}$ es transmitida y ocurren t o menos errores, la palabra recibida $\mathbf{y}$ se encontrará en la esfera de radio t alrededor de la palabra-código transmitida $\mathbf{x}$, para que el código pueda corregir t errores o menos verifiquemos que las esferas de radio t con centro en las palabras-código son disjuntas. Sean $\mathbf{x}_1,\mathbf{x}_2 \in \mathcal{C}$ y supóngase que $B_t(\mathbf{x}_1) \cap B_t(\mathbf{x}_2) \neq \emptyset$, entonces existe $\mathbf{v} \in \mathbb{F}$ tal que $\mathbf{v} \in B_t(\mathbf{x}_1)$ y $\mathbf{v} \in B_t(\mathbf{x}_2)$, por consiguiente,

$$d(\mathbf{x}_1,\mathbf{x}_2) \leq d(\mathbf{x}_1,\mathbf{v}) + d(\mathbf{v},\mathbf{x}_2) \leq t + t = 2t,$$

i.e., $d(\mathbf{x}_1,\mathbf{x}_2) \leq 2t$ pero $d \leq d(\mathbf{x}_1,\mathbf{x}_2) \leq 2t$ entonces $d \leq 2t$. Dado que $t \leq \frac{1}{2}(d-1)$, puesto que $t = [\frac{1}{2}(d-1)]$, tenemos que $2t \leq d-1$ luego $d \leq 2t \leq d-1$, de ahí que, $d \leq d-1$, lo cual es absurdo. En consecuencia, las esferas de radio t con centro en las palabras-código son disjuntas. De manera que, la palabra recibida $\mathbf{y}$ está más cerca de $\mathbf{x}$ que de cualquier otra palabra-código $\mathbf{u}$. Así, la decodificación de vecino más cercano corregirá estos errores. □

El código lineal $\mathcal{H}$ es un $[7,4,3]$-código lineal corrector de un único error.

La matriz de chequeo de paridad H de un $[n,k]$-código lineal $\mathcal{C}$ resulta ser una herramienta útil para la decodificación. Si $\mathbf{x}$ es transmitida, $\mathbf{x}$ es una palabra código luego $H\mathbf{x}^t = \mathbf{0}$. Si el canal provoca algunos errores, esto es, si $\mathbf{e} \neq \mathbf{0}$ entonces es muy probable que $H\mathbf{y}^t \neq \mathbf{0}$ donde $\mathbf{y}$ es la palabra recibida. El vector $\mathbf{s} = H\mathbf{y}^t$ es llamado el *síndrome*. El síndrome depende sólo del vector error $\mathbf{e}$ y no de la palabra código transmitida ya que si $\mathbf{s} = H\mathbf{y}^t = H(\mathbf{x}+\mathbf{e})^t = H\mathbf{x}^t + H\mathbf{e}^t = H\mathbf{e}^t$, i.e., $\mathbf{s} = H\mathbf{e}^t$. El síndrome proporciona cierta información sobre $\mathbf{e}$, pero no la suficiente. Esto es debido a que para un $\mathbf{s} \in \mathbb{F}_2^n$ fijo, el conjunto de soluciones de $H\mathbf{e}^t = \mathbf{s}$ forma una *clase* del código $\mathcal{C}$.

Definición 3.10. Sea $\mathcal{C}$ un $[n,k]$-código lineal sobre $\mathbb{F}_2$, para cualquier vector $\mathbf{a} \in \mathbb{F}_2^n$, el conjunto

$$\mathbf{a} + \mathcal{C} = \{\mathbf{a} + \mathbf{x} : \mathbf{x} \in \mathcal{C}\} \tag{19}$$

es llamado una *clase* de $\mathcal{C}$

Proposición 3.11. *Sea $\mathcal{C}$ un $[n,k]$-código lineal binario. Entonces*

1. *Todo vector $\mathbf{b} \in \mathbb{F}_2^n$ está en alguna clase.*
2. *Dos vectores $\mathbf{a}$ y $\mathbf{b}$ están en la misma clase sí y sólo si $\mathbf{a} - \mathbf{b} \in \mathcal{C}$*
3. *Cada clase contiene 2^k vectores.*

Demostración. Sea $\mathbf{b} \in \mathbb{F}_2^n$, $\mathbf{b} = \mathbf{b} + \mathbf{0} \in \mathbf{b} + \mathcal{C}$, ya que $\mathbf{0} \in \mathcal{C}$, i.e., $\mathbf{b} \in \mathbf{b} + \mathcal{C}$. Así, todo vector $\mathbf{b} \in \mathbb{F}_2^n$ está en alguna clase. Supóngase que $\mathbf{a}, \mathbf{b} \in \mathbf{u} + \mathcal{C}$ para algún $\mathbf{u} \in \mathbb{F}_2^n$ entonces $\mathbf{a} = \mathbf{u} + \mathbf{x}_1$ y $\mathbf{b} = \mathbf{u} + \mathbf{x}_2$ para algunos $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$ luego $\mathbf{a} - \mathbf{b} = (\mathbf{u} + \mathbf{x}_1) - (\mathbf{u} + \mathbf{x}_2) = \mathbf{x}_1 - \mathbf{x}_2 \in \mathcal{C}$, i.e., $\mathbf{a} - \mathbf{b} \in \mathcal{C}$. Recíprocamente, si $\mathbf{a} - \mathbf{b} \in \mathcal{C}$ entonces $\mathbf{a} - \mathbf{b} = \mathbf{x}$ para algún $\mathbf{x} \in \mathcal{C}$, luego $\mathbf{a} = \mathbf{b} + \mathbf{x} \in \mathbf{b} + \mathcal{C}$, de ahí que, $\mathbf{a} \in \mathbf{b} + \mathcal{C}$ pero $\mathbf{b} \in \mathbf{b} + \mathcal{C}$, por consiguiente, $\mathbf{a}, \mathbf{b} \in \mathbf{b} + \mathcal{C}$. Finalmente, como $\mathcal{C}$ tiene 2^k palabras-código distintas entonces $\mathbf{a} + \mathcal{C}$ tiene 2^k vectores distintos, ya que si $\mathbf{a} + \mathbf{x}_1 = \mathbf{a} + \mathbf{x}_2$ para $\mathbf{x}_1 \neq \mathbf{x}_2$ en $\mathcal{C}$ entonces $\mathbf{x}_1 = \mathbf{x}_2$, lo cual es absurdo. □

Definición 3.12. Sea $\mathcal{C}$ un $[n,k]$-código lineal binario, se define la relación $\sim$ en $\mathbb{F}_2^n$, de la siguiente manera, $\mathbf{a} \sim \mathbf{b}$ sí y sólo si $\mathbf{a} - \mathbf{b} \in \mathcal{C}$.

Proposición 3.13. *La relación $\sim$ en $\mathbb{F}_2^n$ es una relación de equivalencia.*

Demostración. Veamos que:

1. Para cada $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{a} \sim \mathbf{a}$.
2. $\mathbf{a} \sim \mathbf{b}$ implica que $\mathbf{b} \sim \mathbf{a}$

3. $\mathbf{a} \sim \mathbf{b}$ y $\mathbf{b} \sim \mathbf{c}$ implica $\mathbf{a} \sim \mathbf{c}$

Para cada $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{a}-\mathbf{a} = \mathbf{0} \in \mathcal{C}$ entonces $\mathbf{a}-\mathbf{a} \in \mathcal{C}$, por consiguiente, $\mathbf{a} \sim \mathbf{a}$. Supóngase que $\mathbf{a} \sim \mathbf{b}$ entonces $\mathbf{a}-\mathbf{b} \in \mathcal{C}$, esto implica que, $-(\mathbf{a}-\mathbf{b}) \in \mathcal{C}$ luego $\mathbf{b}-\mathbf{a} \in \mathcal{C}$, de ahí que, $\mathbf{b} \sim \mathbf{a}$. Finalmente, supóngase que $\mathbf{a} \sim \mathbf{b}$ y $\mathbf{b} \sim \mathbf{c}$ entonces $\mathbf{a}-\mathbf{b} \in \mathcal{C}$ y $\mathbf{b}-\mathbf{c} \in \mathcal{C}$ luego $(\mathbf{a}-\mathbf{b})+(\mathbf{b}-\mathbf{c}) \in \mathcal{C}$, i.e., $\mathbf{a}-\mathbf{c} \in \mathcal{C}$, por consiguiente, $\mathbf{a} \sim \mathbf{c} \in \mathcal{C}$, en consecuencia, la relación $\sim$ en $\mathbb{F}_2^n$ es una relación reflexiva,simétrica y transitiva. Por lo tanto, $\sim$ es una relación de equivalencia. □

Definición 3.14. La *clase de equivalencia de* $\mathbf{a}$ para la relación de equivalencia $\sim$ en $\mathbb{F}_2^n$, lo cual se denota por $[\mathbf{a}]$, se define como

$$[\mathbf{a}] \;=\; \{\mathbf{v} \in \mathbb{F}_2^n : \mathbf{v} \sim \mathbf{a}\}$$

Proposición 3.15. *Para cada* $\mathbf{a} \in \mathbb{F}_2^n$, $[\mathbf{a}] = \mathbf{a} + \mathcal{C}$

Demostración.

$$\begin{aligned}
\mathbf{v} \in [\mathbf{a}] &\Leftrightarrow \mathbf{v} \sim \mathbf{a} \\
&\Leftrightarrow \mathbf{v} - \mathbf{a} \in \mathcal{C} \\
&\Leftrightarrow \mathbf{v} - \mathbf{a} = \mathbf{x} \text{ para algún } \mathbf{x} \in \mathcal{C} \\
&\Leftrightarrow \mathbf{v} = \mathbf{a} + \mathbf{x} \text{ para algún } \mathbf{x} \in \mathcal{C} \\
&\Leftrightarrow \mathbf{v} \in \mathbf{a} + \mathcal{C}
\end{aligned}$$

□

La relación de equivalencia $\sim$ en $\mathbb{F}_2^n$ induce una partición de $\mathbb{F}_2^n$ en clases de equivalencia no vacías y disjuntas por parejas.

Como $|\mathbb{F}_2^n| = 2^n$, $|\mathbf{a}+\mathcal{C}| = 2^k$ y $\mathbb{F}_2^n = \cup\{\mathbf{a}+\mathcal{C} : \mathbf{a} \in \mathbb{F}_2^n\}$, tenemos que, $2^n = |\cup\{\mathbf{a}+\mathcal{C} : \mathbf{a} \in \mathbb{F}_2^n\}| = r2^k$ donde r es el número de clases de equivalencia en $\mathbb{F}_2^n$, luego $2^n = r2^k$, de ahí que, $r = 2^{n-k}$. Hay 2^{n-k} clases de $\mathcal{C}$, correspondientes a los 2^{n-k} posibles síndromes $\mathbf{s}$. Así, una vez que el receptor calcula $\mathbf{s}$, reduce su búsqueda para $\mathbf{e}$ de 2^n a 2^k posibilidades, a saber, los elementos de la clase correspondiente a $\mathbf{s}$.

El Algoritmo 1 muestra cómo funciona el síndrome en el decodificador, al menos en principio. Por supuesto el paso 2 en este algoritmo representa una gran cantidad de trabajo. Sin embargo, si k y $n-k$ son relativamente pequeños, es posible implementar el paso 2 vía un procedimiento de una tabla de búsqueda, el cual describimos abajo.

Así la estrategia del decodificador es, dado $\mathbf{y}$, escoger un vector de peso mínimo $\hat{\mathbf{e}}$ en la clase que contiene a $\mathbf{s}$, y decodificar a $\mathbf{y}$ como $\hat{\mathbf{x}} = \mathbf{y} - \hat{\mathbf{e}}$. El vector de peso mínimo en una clase es

Algoritmo 1 Algoritmo de la función del síndrome en la decodificación para un CBS

Input: Palabra recibida $\mathbf{y}$

Output: Estimado de la palabra-código transmitida $\hat{\mathbf{x}}$

1: Calcular el síndrome $\mathbf{s} = H\mathbf{y}^t$

2: Encontrar el vector de peso mínimo en la clase que contiene a $\mathbf{s}$ y lo denotamos por $\hat{\mathbf{e}}$

3: Calcular el estimado de la palabra-código transmitida $\hat{\mathbf{x}} = \mathbf{y} - \hat{\mathbf{e}}$

llamado *líder de clase*. (Si hay más de un vector de peso mínimo en la clase se escoge uno de manera aleatoria y se le llama líder de clase.)

La *tabla de búsqueda* o también llamada *arreglo estándar* se construye de la siguiente manera; la primera fila consiste del código $\mathcal{C}$ (la clase $\mathbf{0} + \mathcal{C}$), con la palabra código $\mathbf{0}$ en la izquierda:

$$\mathbf{x}^{(1)} = \mathbf{0}, \quad \mathbf{x}^{(2)}, \quad \ldots, \mathbf{x}^{(j)} \quad (j = 2^k)$$

y las otras filas son las $2^{n-k} - 1$ clases $\mathbf{a}_i + \mathcal{C}$, arregladas en el mismo orden y con el líder de clase en la izquierda:

$$\mathbf{a}_i + \mathbf{x}^{(1)}, \quad \mathbf{a}_i + \mathbf{x}^{(2)}, \quad \ldots, \quad \mathbf{a}_i + \mathbf{x}^{(j)} \quad (i = 1, \ldots, 2^{n-k} - 1)$$

El decodificador usa la tabla de búsqueda de la siguiente manera: cuando $\mathbf{y}$ es recibido su posición en la tabla es ubicada, entonces el decodificador decide que el vector error $\hat{\mathbf{e}}$ es el líder de la clase encontrada en el extremo izquierdo de $\mathbf{y}$, y $\mathbf{y}$ es decodificada como la palabra-código $\hat{\mathbf{x}} = \mathbf{y} - \hat{\mathbf{e}}$ encontrada en la cima de la columna que contiene a $\mathbf{y}$

Teorema 3.16. *(Propiedades del síndrome) Para un $[n, k]$-código lineal binario $\mathcal{C}$ con matriz de chequeo de paridad $H \in \mathcal{M}_{(n-k)\times n}$, sea $\mathbf{s} = H\mathbf{y}^t$ el síndrome de la palabra recibida $\mathbf{y}$. Entonces*

1. *$\mathbf{s}$ es un vector columna de longitud $n - k$.*

2. *Si $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_2^n$ y $e_{i_j} = 1$ para $i_j \in \{1, 2, \ldots, n\}$, $j = 1, \ldots, t$, es tal que $\mathbf{y} = \mathbf{x} + \mathbf{e}$ entonces*

$$\mathbf{s} = \sum_{j=1}^{t} \mathbf{H}_{i_j} \tag{20}$$

   donde ($\mathbf{H}_{i_j}$ es la i_j-ésima columna de H), i.e., el síndrome $\mathbf{s}$ es igual a la suma de las columnas de H en donde los errores ocurren.

3. *Dos vectores están en la misma clase de $\mathcal{C}$ sí y sólo si ellos tienen el mismo síndrome.*

4. *Hay una correspondencia uno a uno entre los síndromes y las clases.*

Demostración. La primera propiedad es inmediata a partir de la definición del síndrome. Sea $\{\mathbf{v}_i\}_{i=1}^n$ la base canónica de $\mathbb{F}_2^n$, dado $\mathbf{e} \in \mathbb{F}_2^n$ tenemos que $\mathbf{e} = \sum_{i=1}^n e_i\mathbf{v}_i$ donde $e_i \in \mathbb{F}_2$. Entonces

$$\begin{aligned}
\mathbf{s} &= H\mathbf{y}^t \\
&= H\mathbf{e}^t \\
&= H(\sum_{i=1}^{n} e_i\mathbf{v}_i)^t \\
&= H(\sum_{j=1}^{t} e_{i_j}\mathbf{v}_{i_j})^t \\
&= H(\sum_{j=1}^{t} e_{i_j}\mathbf{v}_{i_j}^t) \\
&= \sum_{j=1}^{t} e_{i_j}H\mathbf{v}_{i_j}^t \\
&= \sum_{j=1}^{t} \mathbf{H}_{i_j}
\end{aligned}$$

donde $\mathbf{H}_{i_j}$ es la i_j-ésima columna de H. Sean $\mathbf{u}_1$ y $\mathbf{u}_2$ dos vectores en $\mathbb{F}_2^n$ denotamos $syn(\mathbf{u}_1)$ y $syn(\mathbf{u}_2)$ los síndromes de $\mathbf{u}_1$ y $\mathbf{u}_2$ respectivamente.

$$\begin{aligned}
\mathbf{u}_1, \mathbf{u}_2 \in \mathbf{u}_1 + \mathcal{C} &\Leftrightarrow \mathbf{u}_1 - \mathbf{u}_2 \in \mathcal{C} \\
&\Leftrightarrow H(\mathbf{u}_1 - \mathbf{u}_2)^t = \mathbf{0} \\
&\Leftrightarrow H\mathbf{u}_1^t = H\mathbf{u}_2^t \\
&\Leftrightarrow syn(\mathbf{u}_1) = syn(\mathbf{u}_2).
\end{aligned}$$

La última propiedad se sigue de que como hay 2^{n-k} clases distintas hay 2^{n-k} síndromes distintos. □

Observación 3.17. De la segunda propiedad del Teorema 3.16 tenemos que $\mathbf{s}$ es llamado el síndrome debido a que da los síntomas de los errores.

Ejemplo 3.18. Continuación del Ejemplo 2.3. En la Figura 3 exhibimos la tabla de búsqueda del $[7, 4, 3]$-código lineal binario $\mathcal{H}$ de nuestro Ejemplo (2.2 y 2.3). Cuando $\mathbf{y} = 1111100$ es recibido el decodificador decide que el vector error líder de la clase $\hat{\mathbf{e}}$ es el vector 0010000 que se encuentra en la segunda columna de la fila que contiene a $\mathbf{y}$, i.e., $\hat{\mathbf{e}} = 0010000$, así, $\mathbf{y}$ es decodificada como $\hat{\mathbf{x}} = \mathbf{y} - \hat{\mathbf{e}} = 1111100 - 0010000 = 1101100$ que está ubicada en la segunda fila de la columna que contiene a $\mathbf{y}$, de ahí que, el estimado del mensaje correspondiente a esa palabra-código es $\hat{\mathbf{u}} = 1101$.

□

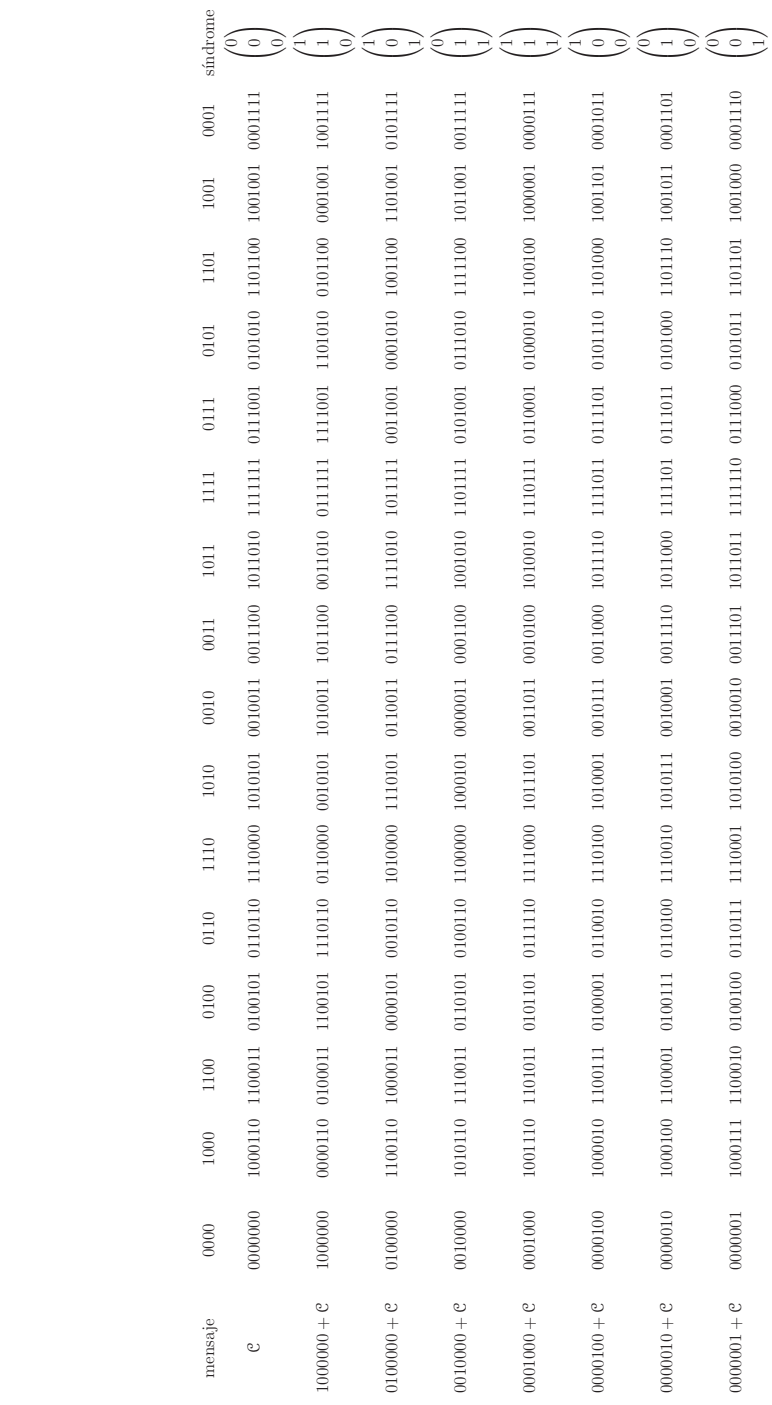

Figura 3: Tabla de búsqueda del $[7, 4, 3]$-código lineal binario $\mathcal{H}$

Definición 3.19. Se dice que dos códigos $\mathcal{C}_1$ y $\mathcal{C}_2$ son *equivalentes* si uno se obtiene a partir del otro por una permutación de sus coordenadas.

Ejemplo 3.20. Continuación del Ejemplo 2.3. Las columnas de la matriz de chequeo de paridad

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

del $[7, 4, 3]$-código lineal binario $\mathcal{H}$ son los vectores columna (síndromes) que aparecen en la Figura 3, excepto el primero, tomados siguiendo el orden de arriba hacia abajo, estas columnas corresponden a todos los vectores distintos de cero en $\mathbb{F}_2^3$. Consideremos los números $1, 2, \ldots, 7$ en su representación binaria, i.e.,

$$\begin{aligned} 1 &= 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 \\ 2 &= 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 \\ 3 &= 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 \\ 4 &= 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \\ 5 &= 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \\ 6 &= 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 \\ 7 &= 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 \end{aligned}$$

tomando los bits de las representaciones binarias de estos números vamos a construir los vectores columna de una matriz de chequeo de paridad

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{21}$$

Las matrices H y H_3 dadas arriba generan el mismo código (salvo equivalencia), a saber, el famoso $[7, 4, 3]$-código lineal binario de Hamming $\mathcal{H}_3$. En la Figura 4 exhibimos las palabras-código de los códigos lineales $\mathcal{H}$ y $\mathcal{H}_3$ asociados a las matrices de chequeo de paridad H y H_3 respectivamente, $\mathcal{H}_3$ se puede obtener a partir de $\mathcal{H}$ permutando en $\mathcal{H}$ la quinta coordenada por la séptima.

□

$\mathcal{H}$	$\mathcal{H}_3$
0 0 0 0 0 0 0	0 0 0 0 0 0 0
1 0 0 0 1 1 0	1 0 0 0 0 1 1
1 1 0 0 0 1 1	1 1 0 0 1 1 0
0 1 0 0 1 0 1	0 1 0 0 1 0 1
0 1 1 0 1 1 0	0 1 1 0 0 1 1
1 1 1 0 0 0 0	1 1 1 0 0 0 0
1 0 1 0 1 0 1	1 0 1 0 1 0 1
0 0 1 0 0 1 1	0 0 1 0 1 1 0
0 0 1 1 1 0 0	0 0 1 1 0 0 1
1 0 1 1 0 1 0	1 0 1 1 0 1 0
1 1 1 1 1 1 1	1 1 1 1 1 1 1
0 1 1 1 0 0 1	0 1 1 1 1 0 0
0 1 0 1 0 1 0	0 1 0 1 0 1 0
1 1 0 1 1 0 0	1 1 0 1 0 0 1
1 0 0 1 0 0 1	1 0 0 1 1 0 0
0 0 0 1 1 1 1	0 0 0 1 1 1 1

Figura 4: Los códigos lineales $\mathcal{H}$ y $\mathcal{H}_3$ son equivalentes

4. Códigos binarios de Hamming

A continuación se definen los códigos binarios de Hamming. Sean $r \geq 2$, $n = 2^r - 1$ y $\mathbb{F}_2^r$, como $|\mathbb{F}_2^r \setminus \{\mathbf{0}\}| = 2^r - 1$, hay $2^r - 1$ r-tuples binarios distintos de cero.

Definición 4.1. Definimos la $r \times (2^r - 1)$ matriz de chequeo de paridad H_r cuyas columnas, en orden, son los bits de las representaciones binarias de los números $1, 2, \ldots, 2^r - 1$ (i.e., H_r está formada por el conjunto de todos los r-tuples binarios distintos de cero como sus columnas). El *código lineal binario de Hamming* $\mathcal{H}_r$ de longitud $n = 2^r - 1$ ($r \geq 2$) es el espacio de soluciones del sistema lineal homogéneo dado por la matriz H_r.

Teorema 4.2. *$\mathcal{H}_r$ es un $[n = 2^r - 1, k = 2^r - 1 - r, 3]$-código lineal binario.*

Demostración. Sabemos que el $rango(H) \leq r$ pero hay r columnas linealmente independientes, entonces $rango(H) = r$, por consiguiente, $dim(nulidad(H)) = n - r = 2^r - 1 - r$. Ahora veamos que $\mathcal{H}_r$ tiene peso mínimo mayor o igual a 3. Sea $\{\mathbf{v}_i\}_{i=1}^n$ la base canónica de $\mathbb{F}_2^n$ donde $n = 2^r - 1$ y sea $\mathbf{y} \in \mathbb{F}_2^n$. Si $wt(\mathbf{y}) = 1$ tenemos que $\mathbf{y} = \mathbf{v}_i$ para algún $i \in \{1, 2, \ldots, n\}$ entonces $syn(\mathbf{y}) = H\mathbf{y}^t = \mathbf{H}_i$, por (20), donde $\mathbf{H}_i$ es alguna columna de H, en consecuencia, $\mathbf{H}_i \neq \mathbf{0}$ ya que $\mathbf{H}_i \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, de ahí que, $syn(\mathbf{y}) \neq \mathbf{0}$. Por lo tanto, si $wt(\mathbf{y}) = 1$ entonces $\mathbf{y} \notin \mathcal{H}_r$. Si $wt(\mathbf{y}) = 2$

entonces $\mathbf{y} = \mathbf{v}_i + \mathbf{v}_j$ con $i \neq j$ luego $syn(\mathbf{y}) = H\mathbf{y}^t = \mathbf{H}_i + \mathbf{H}_j$, otra vez por (20), donde $\mathbf{H}_i, \mathbf{H}_j$ son columnas distintas de H. Supongamos que $syn(\mathbf{y}) = \mathbf{0}$ entonces $\mathbf{H}_i + \mathbf{H}_j = \mathbf{0}$, por consiguiente, $\mathbf{H}_i = \mathbf{H}_j$, lo cual es absurdo, en consecuencia, $syn(\mathbf{y}) \neq \mathbf{0}$. Por lo tanto, si $wt(\mathbf{y}) = 2$ entonces $\mathbf{y} \notin \mathcal{H}_r$. Sólo resta demostrar que para cada $\mathbf{x} \in \mathcal{H}_r$, $wt(\mathbf{x}) \geq 3$, para esto vamos a exhibir que $\mathcal{H}_r$ tiene una palabra-código de peso 3. Sean $\mathbf{H}_1$ y $\mathbf{H}_2$ las dos primeras columnas de la matriz de chequeo de paridad H. Como $\mathbf{H}_1 \neq \mathbf{H}_2$ tenemos que $\mathbf{H}_1 + \mathbf{H}_2 \neq \mathbf{0}$ entonces $\mathbf{H}_1 + \mathbf{H}_2 = \mathbf{H}_i$ para alguna $i \in \{3, \ldots, n\}$. Si $\mathbf{x} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_i$ entonces $wt(\mathbf{x}) = 3$ y $syn(\mathbf{x}) = H\mathbf{x}^t = \mathbf{H}_1 + \mathbf{H}_2 + \mathbf{H}_i$, una vez más por (20), i.e., $wt(\mathbf{x}) = 3$ y $syn(\mathbf{x}) = \mathbf{0}$, por consiguiente, $\mathbf{x} \in \mathcal{H}_r$ y $wt(\mathbf{x}) = 3$. Así para cada $\mathbf{x} \in \mathcal{H}_r$, $wt(\mathbf{x}) \geq 3$ y existe una palabra-código de peso 3. En consecuencia, $d_{\text{mín}}(\mathcal{H}_r) = 3$. Por lo tanto, $\mathcal{H}_r$ es un $[n = 2^r - 1, k = 2^r - 1 - r, 3]$-código lineal binario. □

Cualquier reordenamiento de las columnas de H_r da un código equivalente, y por lo tanto uno cualquiera de estos códigos equivalentes será llamado el código binario de Hamming de longitud $n = 2^r - 1$ y denotado por $\mathcal{H}_r$ o $\mathcal{H}_2(r)$.

Los códigos lineales binarios de Hamming pertenecen a una clase de códigos extremadamente exclusiva, los *códigos perfectos*. Los únicos otros códigos lineales binarios perfectos son los códigos de repetición y el $[23, 12, 7]$ código de Golay $\mathcal{G}_{23}$ (cf. [3],[2],[4],[1]).

Definición 4.3. Sea $\mathcal{C} = \{\mathbf{x}_1, \ldots, \mathbf{x}_M\}$ un código de longitud n sobre $\mathbb{F}_2$, se dice que $\mathcal{C}$ es un código perfecto si existe un entero positivo t tal que las esferas de Hamming de radio t y centro en las palabras-código cubren a $\mathbb{F}_2^n$ sin traslaparse, i.e., si existe $t \in \mathbb{N}$ tal que $\mathbb{F}_2^n = \cup_{i=1}^{M} B_t(\mathbf{x}_i)$ y $B_t(\mathbf{x}_i) \cap B_t(\mathbf{x}_j) = \emptyset$ siempre que $i \neq j$.

Teorema 4.4. *Los códigos lineales binarios de Hamming $\mathcal{H}_r$ son códigos perfectos.*

Demostración. Como la $dim(\mathcal{H}_r) = n - r = 2^r - 1 - r$ tenemos que $|\mathcal{H}_r| = 2^{n-r} = 2^{2^r-1-r}$ y dado que $d_{\text{mín}}(\mathcal{H}_r) = 3$ entonces el código lineal binario de Hamming $\mathcal{H}_r$ puede corregir $t = 1$ error, de la demostración del teorema 3.9 se sigue que $B_t(\mathbf{x}_i) \cap B_t(\mathbf{x}_j) = \emptyset$ siempre que $i \neq j$. Ahora bien, $|B_t(\mathbf{0})| = n + 1 = 2^r - 1 + 1 = 2^r$, de ahí que, $|B_t(\mathbf{x}_i)| = 2^r$ para cada $i \in \{1, \ldots, 2^{n-r}\}$. Entonces

$$\begin{aligned} |\cup_{i=1}^{2^{n-r}} B_t(\mathbf{x}_i)| &= \sum_{i=1}^{2^{n-r}} |B_t(\mathbf{x}_i)| \\ &= \sum_{i=1}^{2^{n-r}} 2^r \\ &= 2^{n-r} \cdot 2^r \\ &= 2^n \\ &= |\mathbb{F}_2^n|. \end{aligned}$$

Así, $\cup_{i=1}^{2^{n-r}} B_t(\mathbf{x}_i) = \mathbb{F}_2^n$, con lo cual queda demostrado el teorema. □

$\mathcal{H}_r$ es un código lineal binario corrector de error-único y es único salvo equivalencia, fácil de codificar y decodificar.

5. Códigos de Hamming sobre $\mathbb{F}_q$

De manera similar, los códigos de Hamming $H_{q,k}$ (ó $\mathcal{H}_q(k)$) pueden ser definidos sobre un campo finito arbitrario $\mathbb{F}_q$, donde $q = p^n$, p-primo y $n \in \mathbb{N}$.

Para construir los códigos de Hamming sobre $\mathbb{F}_q$ se dan algunas definiciones básicas.

Definición 5.1. Sea $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$ arbitraria. Llamamos código lineal de longitud n sobre $\mathbb{F}_q$ con matriz de chequeo de paridad H al conjunto $\mathcal{C}$ que consiste de todos los vectores $\mathbf{x} \in \mathbb{F}_q^n$ tales que $H\mathbf{x}^t = \mathbf{0}$, i.e.,

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

Definición 5.2. Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$. Una matriz G cuyo espacio fila es igual a $\mathcal{C}$ es llamada una matriz generadora para $\mathcal{C}$. Recíprocamente, si G es una matriz con entradas en $\mathbb{F}_q$, su espacio fila es llamado el código lineal sobre $\mathbb{F}_q$ generado por G.

Se enuncian sin demostración las siguientes proposiciones ya que sus pruebas son análogas a las dadas en la Sección 1

Proposición 5.3. *Si $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_q$ con matriz de chequeo de paridad estándar $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$, entonces su matriz generadora estándar está dada por $G = [I_k|-A^t]$ y viceversa.*

Proposición 5.4. *Si $\mathcal{C}$ es un código lineal con matriz de chequeo de paridad $H = [A|I_{n-k}] \in \mathcal{M}_{(n-k)\times n}(\mathbb{F}_q)$, entonces dim $\mathcal{C} = k$ y $|\mathcal{C}| = q^k$.*

Definición 5.5. Un $[n, k]$-código lineal sobre $\mathbb{F}_q$ es un subespacio k-dimensional del espacio vectorial $\mathbb{F}_q^n$; n es llamado la longitud del código y k la dimensión.

Los conceptos de distancia de Hamming, peso de Hamming, distancia mínima de Hamming, esfera de Hamming se pueden definir de manera análoga reemplazando el campo $\mathbb{F}_2$ por el campo $\mathbb{F}_q$.

Teorema 5.6. *Sea $\mathcal{C}$ un $[n, k, d]$-código lineal sobre el campo finito $\mathbb{F}_q$ con matriz de chequeo de paridad H. Entonces d es el entero más pequeño r para el cual hay r columnas linealmente dependientes en H. (Así, H tiene d columnas linealmente dependientes, pero cualesquiera $d-1$ columnas son linealmente independientes.)*

Demostración. Sean $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_n$ las columnas de H y supóngase que una elección particular de w de tales columnas son linealmente dependientes. Entonces existen coeficientes $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$ con exactamente w de ellos distintos de cero para los cuales $x_1\mathbf{H}_1 + x_2\mathbf{H}_2 + \cdots + x_n\mathbf{H}_n = \mathbf{0}$, esto es equivalente a $\mathbf{x}H^t = \mathbf{0}$ donde $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, i.e., $H\mathbf{x}^t = \mathbf{0}$ entonces $\mathbf{x} \in \mathcal{C}$, por consiguiente, $\mathbf{x}$ tiene peso w y $d_{min}(\mathcal{C}) = wt(\mathcal{C}) \leq w$. Recíprocamente, si $\mathbf{x}$ es una palabra-código de peso w, entonces, $H\mathbf{x}^t = \mathbf{0}$, i.e., $\mathbf{x}H^t = \mathbf{0}$ y por consiguiente w columnas de H son linealmente dependientes. □

De acuerdo al Teorema 5.6 la distancia mínima de un $[n, k]$ código lineal sobre $\mathbb{F}_q$ con matriz de chequeo de paridad H es el entero positivo d para el cual existen d columnas linealmente dependientes en H. Por consiguiente, la matriz de chequeo de paridad de un $[n, k, 3]$ código lineal sobre $\mathbb{F}_q$ tiene la propiedad de que ningun par de sus columnas son linealmente dependientes, esto es, ninguna columna es un múltiplo escalar de cualquier otra columna, sin embargo algún conjunto de tres columnas es linealmente dependiente.

Vamos a construir una matriz de chequeo de paridad con estas propiedades. Primero escogemos cualquier columna diferente de cero $\mathbf{H}_1$ en $V_1 = \mathbb{F}_q^k$, después escogemos cualquier columna diferente de cero $\mathbf{H}_2 \in V_2 = V_1 - \{\alpha\mathbf{H}_1 : \alpha \neq 0\}$, enseguida escogemos cualquier columna diferente de cero $\mathbf{H}_3 \in V_3 = V_1 - \{\alpha\mathbf{H}_1 : \alpha \neq 0\} \cup \{\alpha\mathbf{H}_2 : \alpha \neq 0\}$, continuamos escogiendo columnas diferentes de cero y descartamos todos los múltiplos escalares diferentes de cero de la columna escogida hasta que todas las columnas hayan sido descartadas, esto se realiza en un número finito de pasos, digamos n. Como hay $q^k - 1$ k-tuples distintos de cero en $\mathbb{F}_q^k$ y $|\{\alpha\mathbf{H}_i : \alpha \neq 0\}| = q - 1$ entonces $n(q-1) = q^k - 1$, de ahí que, $n = (q^k - 1)/(q - 1)$. Por otro lado, todo par de columnas $\mathbf{H}_i$ y $\mathbf{H}_j$, $i, j \in \{1, \ldots, n\}$, $i \neq j$ son linealmente independientes pero para cada $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$, $\alpha\mathbf{H}_i \neq \beta\mathbf{H}_j$ entonces $\alpha\mathbf{H}_i - \beta\mathbf{H}_j \neq 0$, de ahí que, $\alpha\mathbf{H}_i - \beta\mathbf{H}_j = \gamma\mathbf{H}_k$ para algún $\gamma \in \mathbb{F}_q \setminus \{0\}$ y $\mathbf{H}_k$, $k \neq i, j$, $k \in \{1, \ldots, n\}$, por consiguiente, $\alpha\mathbf{H}_i - \beta\mathbf{H}_j - \gamma\mathbf{H}_k = \mathbf{0}$, esto es, $\mathbf{H}_i, \mathbf{H}_j, \mathbf{H}_k$ son columnas linealmente dependientes.

En resumen, construimos una matriz de chequeo de paridad con $n = (q^k - 1)/(q - 1)$ columnas, para las cuales ningún par de columnas son linealmente dependientes, pero algún conjunto de tres columnas es linealmente dependiente. La matriz resultante, conocida como *matriz de Hamming de orden k* es la matriz de chequeo de paridad de un $[n, n-k, 3]$ código lineal sobre $\mathbb{F}_q$ con parámetros $n = (q^k - 1)/(q - 1)$, $n - k = (q^k - 1)/(q - 1) - k$ y $d = 3$, que es conocido como un *código q-ario de Hamming de orden k* y es denotado por $\mathcal{H}_q(k)$.

Obsérvese que la elección de las columnas no es única, y así, hay muchas matrices de Hamming diferentes y códigos de Hamming con el mismo conjunto de parámetros. Sin embargo, cualquier matriz de Hamming puede ser obtenida de cualquier otra (con los mismos parámetros) permutando las columnas y multiplicando algunas columnas por escalares diferentes de cero. Por consiguiente, cualesquiera dos códigos de Hamming del mismo tamaño son múltiplos escalares equivalentes.

El Teorema 3.9 se establece de manera análoga para códigos sobre $\mathbb{F}_q$, usando este hecho demostramos el siguiente teorema.

Teorema 5.7. *Los $[n, n-k, 3]$ códigos lineales q-arios de Hamming $\mathcal{H}_q(k)$ son perfectos.*

Demostración. Como $d = 3$ es la distancia mínima del código de Hamming $\mathcal{H}_q(k)$ entonces $\mathcal{H}_q(k)$ puede corregir $t = 1$ o menos errores. Luego $B_1(\mathbf{x}) \cap B_1(\mathbf{y}) = \emptyset$ siempre que $\mathbf{x}, \mathbf{y} \in \mathcal{H}_q(k)$, $\mathbf{x} \neq \mathbf{y}$. Hay un total de q^{n-k} esferas del tipo $B_1(\mathbf{x})$, $\mathbf{x} \in \mathcal{H}_q(k)$ (una por cada palabra-código). Por otro lado, la esfera de radio 1 alrededor de la palabra-código cero contiene a este vector y a los n vectores de peso 1 y sus múltiplos diferentes de cero, es decir, $q-1$, hay un total de $n(q-1)+1$ vectores en $B_1(\mathbf{0})$, esto es, $|B_1(\mathbf{0})| = n(q-1)+1 = [(q^k-1)/(q-1)](q-1)+1 = q^k$. Para cualquier otra palabra-código $\mathbf{x} \in \mathcal{H}_q(k)$, $|B_1(\mathbf{x})| = q^k$ ya que cada vector en la esfera $B_1(\mathbf{x})$, puede ser obtenido sumando $\mathbf{x}$ a un vector en la esfera $B_1(\mathbf{0})$. Así, para cada $\mathbf{x} \in \mathcal{H}_q(k)$, $|B_1(\mathbf{x})| = q^k$. Por lo que,

$$\begin{aligned} |\bigcup_{\mathbf{x}\in\mathcal{H}_q(k)} B_1(\mathbf{x})| &= \sum_{\mathbf{x}\in\mathcal{H}_q(k)} |B_1(\mathbf{x})| \\ &= \sum_{\mathbf{x}\in\mathcal{H}_q(k)} q^k \\ &= \sum_{i=1}^{q^{n-k}} q^k \\ &= q^{n-k}q^k \\ &= q^n \end{aligned}$$

esto es, $|\bigcup_{\mathbf{x}\in\mathcal{H}_q(k)} B_1(\mathbf{x})| = q^n$, en consecuencia, las esferas de Hamming de radio 1 y con centro en las palabras-código cubren el espacio. Por lo tanto, los $[n, n-k, 3]$ códigos lineales q-arios de Hamming $\mathcal{H}_q(k)$ son perfectos. □

Veamos algunos ejemplos de códigos lineales q-arios de Hamming.

Ejemplo 5.8. Sea $\mathbb{F}_3 = \{0, 1, 2\}$ el campo ternario cuyas Tablas de Cayley son:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

y

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

La característica del campo $\mathbb{F}_3$ es 3, esto es, 3 es el menor entero positivo tal que $3a = 0$ para cada $a \in \mathbb{F}_3$. Sea $k = 2$ y tenemos que $q = 3$ entonces $n = (q^k-1)/(q-1) = (3^2-1)/(3-1) = 4$,

de ahí que, $|\mathbb{F}_3^n| = |\mathbb{F}_3^4| = 3^4$ Sean $V_1 = \mathbb{F}_3^2$,

$$\begin{aligned}
\mathbf{c}_1 &= \begin{pmatrix}1\\0\end{pmatrix} \in V_1,\\
\mathbf{c}_2 &= \begin{pmatrix}0\\1\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}\},\\
\mathbf{c}_3 &= \begin{pmatrix}1\\1\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix} \cup \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\},\\
\mathbf{c}_4 &= \begin{pmatrix}1\\2\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix} \cup \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix} \cup \{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\}.
\end{aligned}$$

Tomamos a las columnas $\mathbf{c}_i$'s en el orden $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_1, \mathbf{c}_2$ para formar la matriz de chequeo de paridad estándar

$$H = \begin{pmatrix}1 & 1 & 1 & 0\\ 1 & 2 & 0 & 1\end{pmatrix}$$

de un $[4, 2, 3]$ código lineal ternario de Hamming $\mathcal{H}_3(2)$, cuya matriz generadora estándar es:

$$G = \begin{pmatrix}1 & 0 & -1 & -1\\ 0 & 1 & -1 & -2\end{pmatrix} = \begin{pmatrix}1 & 0 & 2 & 2\\ 0 & 1 & 2 & 1\end{pmatrix}.$$

De manera que toda palabra-código $\mathbf{x} \in \mathcal{H}_3(2)$ se puede escribir como combinación lineal de las filas de la matriz generadora, esto es, para cada $\mathbf{x} \in \mathcal{H}_3(2)$,

$$\mathbf{x} = uG = u_1(1022) + u_2(0121)$$

donde $u_i \in \mathbb{F}_3$, $i \in \{1, 2, 3\}$, hay 3^2 de tales combinaciones lineales, de ahí que, $|\mathcal{H}_2(2)| = 9$. En la Figura 5 enlistamos todas las palabras-código del código lineal ternario de Hamming $\mathcal{H}_3(2)$ con su peso respectivo.

$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$
0000	0	0121	3	0212	3
1022	3	2011	3	1110	3
2220	3	1201	3	2102	3

Figura 5: Palabras-código del código lineal ternario de Hamming $\mathcal{H}_3(2)$

□

Ejemplo 5.9. Sea $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ un campo cuaternario cuyas Tablas de Cayley son:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

y

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Obsérvese que la característica del campo $\mathbb{F}_{2^2}$ es 2 y que se satisface la relación $\alpha^2 + \alpha + 1 = 0$. Además, sea $k = 2$, y tenemos que $q = 2^2$ entonces $n = (q^k - 1)/(q - 1) = (2^4 - 1)/(2^2 - 1) = 5$, de ahí que, $|F_{2^2}^n| = |F_{2^2}^5| = 4^5$. Sean $V_1 = \mathbb{F}_{2^2}^2$,

$$
\begin{aligned}
\mathbf{c}_1 &= \begin{pmatrix}1\\0\end{pmatrix} \in V_1,\\
\mathbf{c}_2 &= \begin{pmatrix}0\\1\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}\alpha^2\\0\end{pmatrix}\},\\
\mathbf{c}_3 &= \begin{pmatrix}1\\1\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}\alpha^2\\0\end{pmatrix}\} \cup \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\\alpha\end{pmatrix}, \begin{pmatrix}0\\\alpha^2\end{pmatrix}\},\\
\mathbf{c}_4 &= \begin{pmatrix}1\\\alpha\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}\alpha^2\\0\end{pmatrix}\} \cup \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\\alpha\end{pmatrix}, \begin{pmatrix}0\\\alpha^2\end{pmatrix}\} \cup \{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}\alpha\\\alpha\end{pmatrix}, \begin{pmatrix}\alpha^2\\\alpha^2\end{pmatrix}\},\\
\mathbf{c}_5 &= \begin{pmatrix}\alpha\\1\end{pmatrix} \in V_1 \setminus \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}\alpha^2\\0\end{pmatrix}\} \cup \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\\alpha\end{pmatrix}, \begin{pmatrix}0\\\alpha^2\end{pmatrix}\} \cup \{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}\alpha\\\alpha\end{pmatrix}, \begin{pmatrix}\alpha^2\\\alpha^2\end{pmatrix}\} \cup\\
&\qquad \{\begin{pmatrix}1\\\alpha\end{pmatrix}, \begin{pmatrix}\alpha\\\alpha^2\end{pmatrix}, \begin{pmatrix}\alpha^2\\1\end{pmatrix}\}.
\end{aligned}
$$

Tomamos a las columnas $\mathbf{c}_i$'s en el orden $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_1, \mathbf{c}_2$ para formar la matriz de chequeo de paridad estándar

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

de un $[5, 3, 3]$ código lineal cuaternario de Hamming $\mathcal{H}_4(2)$, cuya matriz generadora estándar es:

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

De manera que toda palabra-código $\mathbf{x} \in \mathcal{H}_4(2)$ se puede escribir como combinación lineal de las filas de la matriz generadora, esto es, para cada $\mathbf{x} \in \mathcal{H}_4(2)$,

$$\mathbf{x} = uG = u_1(10011) + u_2(0101\alpha) + u_3(001\alpha 1)$$

donde $u_i \in \mathbb{F}_{2^2}$, $i \in \{1, 2, 3\}$, hay 4^3 de tales combinaciones lineales, de ahí que, $|\mathcal{H}_4(2)| = 64$. En la Figura 6 enlistamos todas las palabras-código del código lineal cuaternario de Hamming $\mathcal{H}_4(2)$ con su respectivo peso.

$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$
00000	0	$001\alpha 1$	3	0101α	3	10011	3
$00\alpha\alpha^2\alpha$	3	$0\alpha 0\alpha\alpha^2$	3	$\alpha 00\alpha\alpha$	3	$00\alpha^2 1\alpha^2$	3
$0\alpha^2 0\alpha^2 1$	3	$\alpha^2 00\alpha^2\alpha^2$	3	$0\alpha 10\alpha$	3	$01\alpha\alpha 0$	3
$10\alpha\alpha\alpha^2$	4	$\alpha 010\alpha^2$	3	$1\alpha 0\alpha^2\alpha$	4	$\alpha 10\alpha^2 0$	3
$0\alpha^2 110$	3	$01\alpha^2 01$	3	$10\alpha^2 0\alpha$	3	$\alpha^2 011\alpha$	4
$1\alpha^2 0\alpha 0$	3	$\alpha^2 10\alpha 1$	4	$011\alpha^2\alpha^2$	4	$101\alpha^2 0$	3
$1100\alpha^2$	3	$0\alpha\alpha 11$	4	$\alpha 0\alpha 10$	3	$\alpha\alpha 001$	3
$0\alpha^2\alpha^2\alpha\alpha$	4	$\alpha^2 0\alpha^2\alpha 0$	3	$\alpha^2\alpha^2 00\alpha$	3	$111\alpha\alpha$	5
$\alpha\alpha\alpha\alpha^2\alpha^2$	5	$\alpha^2\alpha^2\alpha^2 11$	5	$\alpha 1111$	5	$1\alpha 11\alpha^2$	5
$11\alpha\alpha^2 1$	5	$\alpha^2 1100$	3	$1\alpha^2 101$	4	$11\alpha^2 10$	4
$1\alpha\alpha 00$	3	$\alpha 1\alpha 0\alpha$	4	$\alpha\alpha 1\alpha 0$	4	$\alpha^2\alpha\alpha\alpha\alpha$	5
$\alpha\alpha^2\alpha\alpha 1$	5	$\alpha\alpha\alpha^2 1\alpha$	5	$1\alpha\alpha^2\alpha 1$	5	$1\alpha^2\alpha 1\alpha$	5
$\alpha 1\alpha^2\alpha\alpha^2$	5	$\alpha\alpha^2 1\alpha^2\alpha$	5	$\alpha^2 1\alpha 1\alpha^2$	5	$\alpha^2\alpha 1\alpha^2 1$	5
$0\alpha\alpha^2\alpha^2 0$	3	$0\alpha^2\alpha 0\alpha^2$	3	$\alpha 0\alpha^2\alpha^2 1$	4	$\alpha\alpha^2 01\alpha^2$	4
$\alpha^2 0\alpha 01$	3	$\alpha^2\alpha 010$	3	$1\alpha^2\alpha^2\alpha^2\alpha^2$	5	$\alpha^2 1\alpha^2\alpha^2\alpha$	5
$\alpha^2\alpha^2 1\alpha\alpha^2$	5	$\alpha\alpha^2\alpha^2 00$	3	$\alpha^2\alpha\alpha^2 0\alpha^2$	4	$\alpha^2\alpha^2\alpha\alpha^2 0$	4

Figura 6: Palabras-código del código lineal cuaternario de Hamming $\mathcal{H}_4(2)$

□

6. Códigos simplex

A continuación se define el concepto de código dual $\mathcal{C}^\perp$ de un código $\mathcal{C}$, los duales de los códigos de Hamming $\mathcal{H}_q(k)$ son llamados *códigos simplex q-arios*.

Definición 6.1. Sean $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ y $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ vectores en $\mathbb{F}_q^n$. El producto escalar de $\mathbf{u}$ y $\mathbf{v}$, se denota por $\mathbf{u} \cdot \mathbf{v}$ y está definido por $\mathbf{u} \cdot \mathbf{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n$. Dos palabras-código $\mathbf{u}$ y $\mathbf{v}$ son ortogonales si $\mathbf{u} \cdot \mathbf{v} = 0$.

Definición 6.2. Si $\mathcal{C}$ es un $\mathbb{F}_q$-código lineal su código dual u ortogonal $\mathcal{C}^\perp$ puede ser definido como el conjunto de vectores que son ortogonales a todas las palabras-código de $\mathcal{C}$, es decir,

$$\mathcal{C}^\perp = \left\{\mathbf{u} \in \mathbb{F}_q^n : \mathbf{u}\cdot\mathbf{v} = 0 \text{ para todo } \mathbf{v} \in \mathcal{C}\right\}.$$

Un $\mathbb{F}_q$-código lineal $\mathcal{C}$ es auto-dual si $\mathcal{C} = \mathcal{C}^\perp$

Teorema 6.3. *Si $\mathcal{C}$ es un $[n,k]$ código lineal sobre $\mathbb{F}_q$ que tiene matriz generadora G y matriz de chequeo de paridad H entonces $\mathcal{C}^\perp$ tiene matriz generadora H y matriz de chequeo de paridad G, además, $\mathcal{C}^\perp$ es un $[n,n-k]$ código lineal sobre $\mathbb{F}_q$.*

Demostración. Sea G la matriz generadora de $\mathcal{C}$ entonces para cada $\mathbf{v} \in \mathcal{C}$, $\mathbf{v} = \sum_{i=1}^k \alpha_i G_i$, donde $\alpha_i \in \mathbb{F}_q$, G_i es la i-ésima fila de G y además, $G_i \in \mathcal{C}$, para $i \in \{1,\ldots,k\}$. Supóngase que $\mathbf{u} \in \mathbb{F}_q^n$ es tal que $\mathbf{u}G^t = \mathbf{0}$ entonces $\mathbf{0} = \mathbf{u}G^t = [\mathbf{u}\cdot G_1 \ \ldots \ \mathbf{u}\cdot G_k]$, de ahí que, $\mathbf{u}\cdot G_i = 0$ para cada $i \in \{1,\ldots,k\}$. Como

$$\mathbf{u}\cdot\mathbf{v} \ = \ \mathbf{u}\cdot(\sum_{i=1}^k \alpha_i G_i) = \sum_{i=1}^k \alpha_i(\mathbf{u}\cdot G_i) = 0$$

i.e., $\mathbf{u}\cdot\mathbf{v} = 0$, tenemos que, $\mathbf{u} \in \mathcal{C}^\perp$. Ahora bien, supóngase que $\mathbf{u} \in \mathcal{C}^\perp$ entonces $\mathbf{u}\cdot G_i = 0$ para cada $i \in \{1,\ldots,k\}$ ya que $G_i \in \mathcal{C}$ pero $G^t = [G_1^t \ \ldots \ G_k^t]$, por consiguiente, $\mathbf{u}G^t = [\mathbf{u}\cdot G_1 \ \ldots \ \mathbf{u}\cdot G_k] = [0 \ \ldots \ 0] = \mathbf{0}$, i.e., $\mathbf{u}G^t = \mathbf{0}$. Por lo tanto, $\mathcal{C}^\perp = \{\mathbf{u} \in \mathbb{F}_q^n : \mathbf{u}G^t = \mathbf{0}\} = \{\mathbf{u} \in \mathbb{F}_q^n : G\mathbf{u}^t = \mathbf{0}\}$. Así, la matriz generadora G del código lineal $\mathcal{C}$ es la matriz de chequeo de paridad del código dual $\mathcal{C}^\perp$. Como $\mathcal{C}^\perp$ es el espacio de soluciones de un sistema lineal homogéneo de k ecuaciones con n indeterminadas cuya matriz asociada al sistema tiene rango k entonces $\mathcal{C}^\perp$ es generado por $n-k$ vectores en $\mathbb{F}_q^n$ linealmente independientes, por consiguiente, $\mathcal{C}^\perp$ es un $[n,n-k]$ código lineal sobre $\mathbb{F}_q$. Por otro lado, como $GH^t = 0$ tenemos que $0 = G[H_1^t \ \ldots \ H_{n-k}^t]$ entonces $GH_i^t = 0$ para cada $i \in \{1,\ldots n-k\}$, de ahí que, $H_i \in \mathcal{C}^\perp$ para cada $i \in \{1,\ldots n-k\}$, pero $rango(H) = n-k = dim\mathcal{C}^\perp$, por consiguiente, las filas de H forman una base para $\mathcal{C}^\perp$, esto es, H es una matriz generadora de $\mathcal{C}^\perp$. Así la matriz de chequeo de paridad H del código lineal $\mathcal{C}$ es la matriz generadora del código dual $\mathcal{C}^\perp$, con lo cual queda demostrado el teorema. □

Definición 6.4. El código dual del código lineal q-ario de Hamming $\mathcal{H}_q(k)$ es llamado un código simplex q-ario.

Por el Teorema anterior, el código simplex q-ario del $[n,n-k,3]$ código lineal q-ario de Hamming $\mathcal{H}_q(k)$ es un $[n,n-(n-k)] = [n,k]$ código lineal.

Ejemplo 6.5. El código binario de Hamming $\mathcal{H}_2(r)$ es un $[2^r-1, 2^r-1-r, 3]$ código lineal entonces el código simplex binario $\mathcal{H}_2(r)^\perp$ es un $[2^r-1, r]$ código lineal, cuya matriz generadora es la matriz de chequeo de paridad H_r del código $\mathcal{H}_2(r)$ dada en la Definición 4.1.

Ejemplo 6.6. El código binario simplex $\mathcal{H}_3^{\perp}$ del $[7,4,3]$ código binario de Hamming $\mathcal{H}_3$ del Ejemplo 3.20 es un $[7,3]$ código lineal cuya matriz generadora es la matriz de chequeo de paridad H_3 dada por (21).

En la Figura 7 enlistamos las palabras-código del código $\mathcal{H}_3^{\perp}$ con su peso respectivo.

$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$
0000000	0	1010101	4	0110011	4	1100110	4
0001111	4	1011010	4	0111100	4	1101001	4

Figura 7: Palabras-código del código simplex binario del código de Hamming $\mathcal{H}_3$

□

Ejemplo 6.7. Sea el $[4,2,3]$ código lineal de Hamming ternario $\mathcal{H}_3(2)$ del Ejemplo 5.8, el $[4,2]$ código simplex ternario $\mathcal{H}_3(2)^{\perp}$ del código $\mathcal{H}_3(2)$ tiene como matriz generadora a la matriz de chequeo de paridad de $\mathcal{H}_3(2)$, a saber,

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

En la Figura 8 enlistamos las palabras-código del código $\mathcal{H}_3(2)^{\perp}$ con su peso respectivo.

$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$
0000	0	1201	3	2102	3
1110	3	2011	3	0212	3
2220	3	0121	3	1022	3

Figura 8: Palabras-código del código simplex ternario del código de Hamming $\mathcal{H}_3(2)$

□

Ejemplo 6.8. Sea el $[5,3,3]$ código lineal de Hamming cuaternario $\mathcal{H}_4(2)$ del Ejemplo 5.9, el $[5,2]$ código simplex cuaternario $\mathcal{H}_4(2)^{\perp}$ del código $\mathcal{H}_4(2)$ tiene como matriz generadora a la matriz de chequeo de paridad de $\mathcal{H}_4(2)$, a saber,

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

En la Figura 9 enlistamos las palabras-código del código $\mathcal{H}_4(2)^{\perp}$ con su peso respectivo.

Los pesos de las palabras-código distintas de cero de los códigos simplex q-arios de los Ejemplos 6.6, 6.7 y 6.8 son $4 = 2^{k-1}$, $(k = 3)$, $3 = 3^{k-1}$, $(k = 2)$ y $4 = 4^{k-1}$, $(k = 2)$, respectivamente.

$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$	$\mathbf{x}$	$wt(\mathbf{x})$
00000	0	$1\alpha101$	4	$11\alpha10$	4	$\alpha\alpha^2\alpha0\alpha$	4
$\alpha\alpha\alpha^2\alpha0$	4	$\alpha^2 1\alpha^2 0\alpha^2$	4	$\alpha^2\alpha^2 1\alpha^2 0$	4	$0\alpha^2\alpha^2 11$	4
$\alpha^2\alpha01\alpha$	4	$\alpha^2 0\alpha\alpha 1$	4	$011\alpha\alpha$	4	$1\alpha^2 0\alpha\alpha^2$	4
$10\alpha^2\alpha^2\alpha$	4	$\alpha011\alpha^2$	4	$\alpha10\alpha^2 1$	4	$0\alpha\alpha\alpha^2\alpha^2$	4

Figura 9: Palabras-código del código simplex cuaternario del código de Hamming $\mathcal{H}_4(2)$

□

7. Conclusiones

En este capítulo de libro de divulgación se introducen los conceptos básicos de la Teoría de Códigos Lineales Detectores-Correctores de Errores a través del código binario de Hamming $\mathcal{H}_3$, se definen los códigos binarios de Hamming y se describen sus parámetros, posteriormente se construyen los códigos q-arios de Hamming perfectos y se describen sus códigos duales llamados códigos simplex q-arios.

Bibliografía

[1] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, (2003).

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, (1977).

[3] R. J. McEliece, *The Theory of Information and Coding*, Encyclopedia of Mathematics and its Applications, Vol. 86, Cambridge, (2004).

[4] S. Roman, *Coding and Information Theory*, Springer-Verlag, (1992).

[5] J. H. van Lint, *Introduction to Coding Theory*, 2nd ed., Springer-Verlag, (1992)

Facultad de Ciencias Físico Matemáticas, BUAP
Avenida San Claudio y 18 Sur, Colonia San Manuel,
Puebla, Pue. C.P. 72570
clopez@fcfm.buap.mx