# Teoría de Códigos y Criptografía

Justo Peralta López
Juan Antonio López Ramos

Universidad de Almería
Departamento de Álgebra y Análisis Matemático

## Definición

Sea $r$ un número entero positivo y sea $H$ un $r \times (2^r - 1)$ matriz cuyas columnas son todos los vectores distintas de cero de $V(r, 2)$. Entonces el código que tiene a $H$ como matriz de paridad es un código Hamming binario, al cual notaremos por $Ham(r, 2)$. Este tipo de códigos es un código perfecto con parámetros:

| | |
|---|---|
| Número de bits de paridad: | $r$ |
| Longitud de palabra: | $2^r - 1$ |
| Número de bits de paridad: | $2^r - 1 - r$ |
| Distancia mínima: | 3 |

## Ejemplo

1. El código $Ham(2, 2)$ posee como matriz de paridad $H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$. Este código posee como matriz de generadora $G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$. Es decir, es un código de repetición binario de longitud de palabra 3.
2. $Ham(3, 2)$ posee como matriz de paridad a

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

Se puede comprobar que es un $[7, 4, 3]$-código.

**Teorema**

*Un q-código (no necesariamente lineal) con parámetros* $(n, M, 2t+1)$ *satisface la siguiente ecuación:*

$$M[\sum_{i=0}^{t} \binom{n}{i}(q-1)^i] \leq q^n$$

*Si se verifica la igualdad entonces decimos que el código es perfecto*

**Definición**

Un código $C$ capaz de corregir $t$ errores se dice que es perfecto, si en su array de decodificación aparece como líderes todos los vectores de peso menor o igual que $t$, y ninguno de pesos mayor que $t$.

**Teorema**

*Un código Hamming* $Ham(r, 2)$*,con* $r \geq 2$ *verifica:*

1. *Es un* $[2^r - 1, 2^r - 1 - r, 3]$*-código lineal.*
2. *Es un código perfecto*

1. $Ham(r,2)$ es un código perfecto, los líderes de las clases son $2^r$ vectores del espacio vectorial $V(n,2)$ de pesos menor o igual que 1.
2. Si recibimos la palabra $y = x + e$ donde $x$ es una palabra del código y $e$ es el error cometido, con $w(e) = 1$. Supongamos también que la posición de $e$ distinta de cero es la posición $j$. Entonces

$$S(y) = yH^t = (x+e)H^t = xH^t + eH^t = eH^t = (0\ldots0\overset{j}{1}0\ldots0)H^t = h_j$$

   donde $h_j$ es la $j$-ésima columna de $H$.
3. Si ordenamos las columnas de $H$ de menor a mayor, $h_j$ será la representación de $j$ en binario.

## Decodificación

1. Recibimos la palabra $y$ y calculamos su síndrome $S(y)$.
2. Si $S(y) = 0$ entonces $y$ pertenece al código y no se han cometido errores.
3. Si $S(y) \neq 0$, entonces el síndrome nos indica la posición donde se ha producido el error en binario.

## Ejemplo

Para el código Hamming, $Ham(3, 2)$ con matriz de paridad

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

Si recibimos la palabra $y = 1101011$, $S(y) = 110$. Luego se ha producido un error en la posición 6. Obsérvese que si se produce un error doble, por ejemplo en las posiciones 3 y 7, $S(y) = h_3 + h_7 = (0011 + 0111) = 0100$ y decodificamos incorrectamente.

Definimos una nueva matriz de paridad $H'$ como sigue

$$H' = \begin{bmatrix} 0 & & \\ \vdots & \mathbf{H} & \\ 0 & & \\ 1 & 1 \ \ldots \ 1 & \end{bmatrix}$$

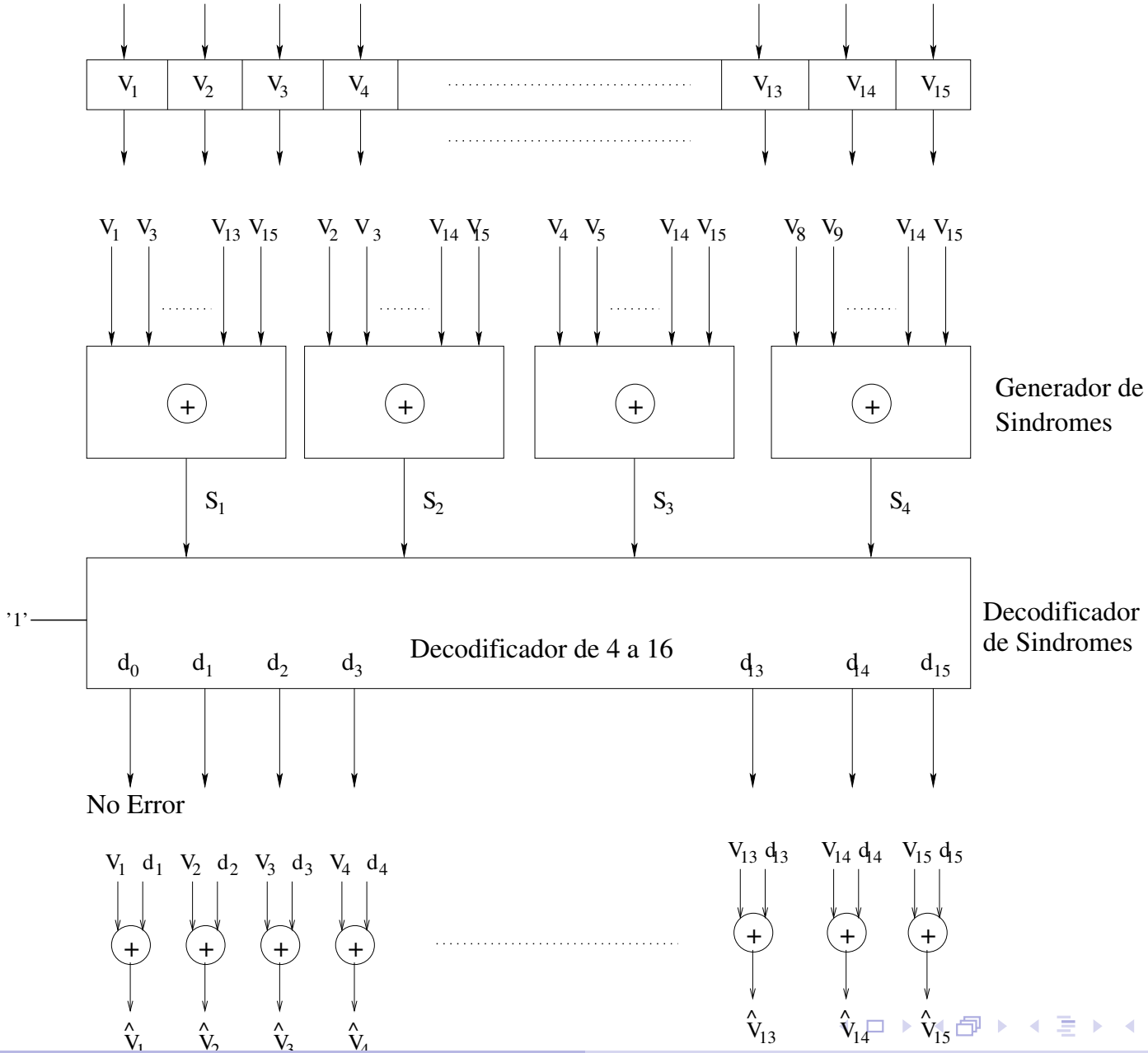
## Ejemplo

La matriz de paridad de un $Ham(4,2)$ viene dado por

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Si $v = v_1 v_2 v_3 v_4 v_5 v_6 v_7 v_8 v_9 v_{10} v_{11} v_{12} v_{13} v_{14} v_{15}$ es la palabra recibida, entonces $S(y) = (s_4, s_3, s_2, s_1)$ con

$$\begin{aligned} s_1 &= v_1 + v_3 + v_5 + v_7 + v_9 + v_{11} + v_{13} + v_{15} \\ s_2 &= v_2 + v_3 + v_6 + v_7 + v_{10} + v_{11} + v_{14} + v_{15} \\ s_3 &= v_4 + v_5 + v_6 + v_7 + v_{12} + v_{13} + v_{14} + v_{15} \\ s_4 &= v_8 + v_9 + v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15} \end{aligned}$$


V1 V2 V3 V4 V13 V14 V15
V1 V3 V13 V15
V2 V3 V14 V15
V4 V5 V14 V15
V8 V9 V14 V15
Generador de Sindromes
S1 S2 S3 S4
'1'
Decodificador de 4 a 16
Decodificador de Sindromes
d0 d1 d2 d3 d13 d14 d15
No Error
V1 d1 V2 d2 V3 d3 V4 d4
V13 d13 V14 d14 V15 d15
V̂1 V̂2 V̂3 V̂4 V̂13 V̂14 V̂15

1. La nueva matriz de paridad para poder detectar errores dobles viene dada por

$$H = \begin{bmatrix} \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \mathbf{0} & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \mathbf{0} & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \mathbf{0} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}$$

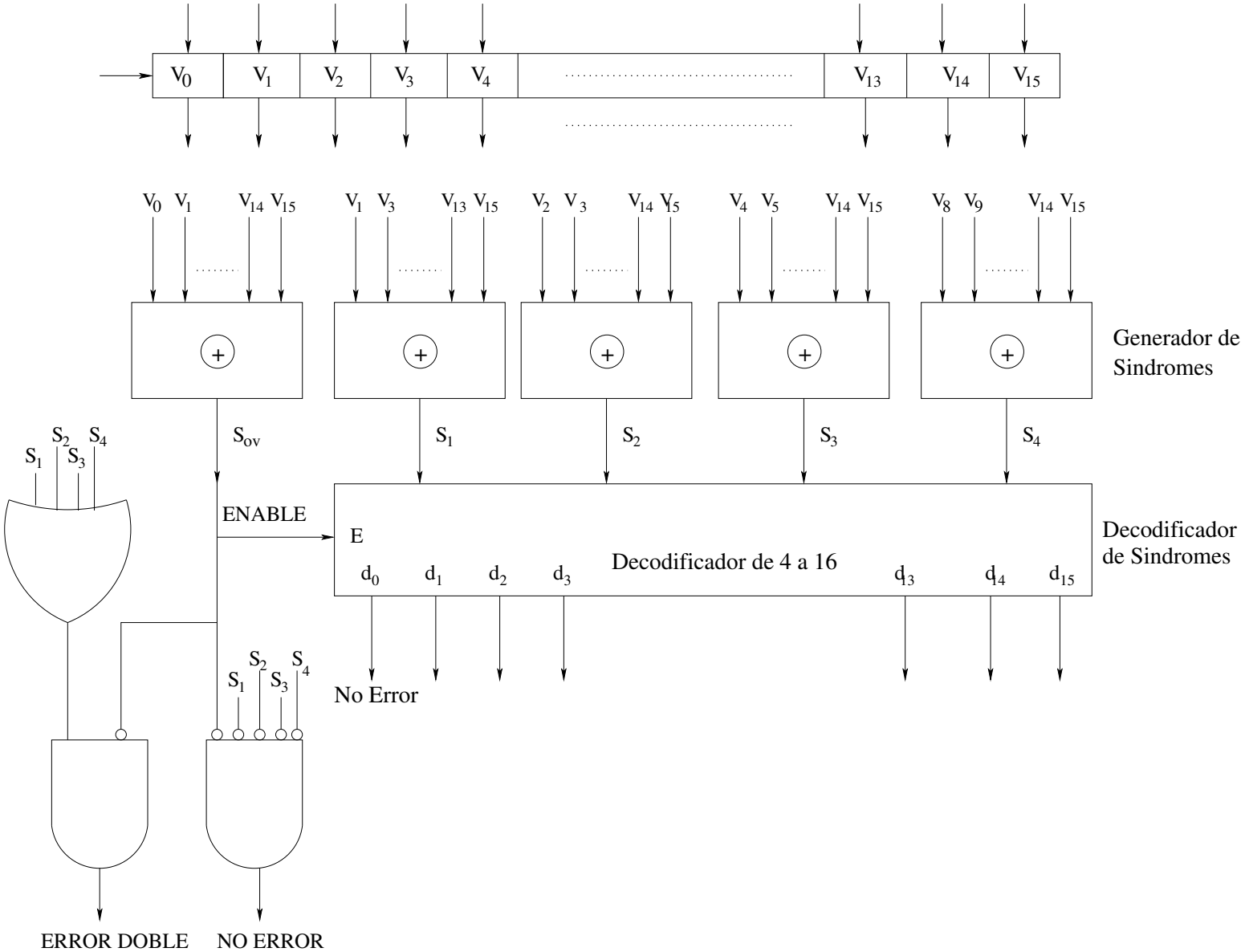
2. Ahora el síndrome posee una ecuación más

$$s_{ov} = v_0 + v_1 + \cdots + v_{15}$$

3. Si recibimos una palabra (de longitud 16) con 2 errores, $s_{ov} = 0$, lo cual nos permitirá la detección de 2 errores o un número par de errores.
4. Hay que tener en cuenta que la palabra recibida ahora es de longitud 16 $v = v_0 v_1 \ldots v_{15}$):

## Decodificación

1. Si $s = 0$, no se ha cometido ningún error.
2. Si $s_{ov} = 1$, entonces un error simple ha ocurrido y la posición viene dada en binario por $(s_4, s_3, s_2, s_1)$ (ej:si $(s_4, s_3, s_2, s_1) = 0101$ entonces ha ocurrido un error en la posición 5).
3. Si $s_{ov} = 0$ y $(s_4, s_3, s_2, s_1) = 0$, un error doble o par ha ocurrido y no se puede


V0 V1 V2 V3 V4 ..... V13 V14 V15
V0 V1 V14 V15
V1 V3 V13 V15
V2 V3 V14 V15
V4 V5 V14 V15
V8 V9 V14 V15
+
Generador de Sindromes
Sov
S1
S2
S3
S4
S1 S2 S3 S4
ENABLE
E
Decodificador de 4 a 16
d0 d1 d2 d3 d13 d14 d15
Decodificador de Sindromes
No Error
S1 S2 S3 S4
ERROR DOBLE
NO ERROR

1. Para obtener un código lineal con distancia mínima 3, basta con encontrar una matriz generadora $H$ con cualquier par de columnas linealmente independiente, es decir, ninguna columna puede ser múltiplo por un escalar de otra y ninguna columna puede ser cero.
2. Para cualquier vector $v$ del espacio vectorial $V(r,q)$, éste posee $q-1$ múltiplos por escalares distintos de cero dados por los conjuntos de la forma $[v] = \{\lambda v | \lambda \in GF(q) \text{y} \lambda \neq 0\}$, con $v \in V(r,q)$. Luego sobre el espacio vectorial $V(r,q)$ se puede definir una partición dado por la clase de equivalencia *ser múltiplo de*, es decir, $u \sim v$ si y sólo si $u = av$ con $a \neq 0 \in GF(q)$ y $u, v \in V(r,q)$. Como hemos visto, cada clase $[v]$ posee $q-1$ elementos, lo que nos da un total de $q^r - 1/q - 1$ clases.
3. A la hora de construir $H$, sólo tenemos que tomar un representante o un elemento de cada clase como columna. Esto nos garantiza que una columna no sea múltiplo de otra, ya que de nor ser así, ambas columnas estarían en la misma clase. De esta forma, $H$ es la matriz de paridad de un código hamming sobre un alfabeto $GF(q)$, al cual notamos por $Ham(r,q)$, con parámetros $[q^r - 1/q - 1, (q^r - 1/q - 1) - r, 3]$.

## Ejemplo

1. Construcción de la matriz de paridad de un $Ham(2,3)$ viene dada por

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

2. La matriz de paridad de un $Ham(2,11)$ viene dado por

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}$$

3. La matriz de paridad de un $Ham(3,3)$ viene dado por

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

## Teorema

*Un $Ham(r, q)$ es un código perfecto capaz de corregir errores simples*

1. Como $Ham(r, q)$ es un código perfecto, los líderes de la tabla de decodificación está formado por todos los vectores de peso menor o igual a 1. Esto quiere decir, sea cual sea el peso del error cometido, siempre decodificaremos como un error de peso 1.
2. Si recibimos la palabra $y = x + e$ con el error $e = (00\ldots0\overset{i}{b}0\ldots0)$, diremos que el error cometido es de peso 1 y magnitud $b$. En este caso, el síndrome viene dado por:

$$S(y) = S(e) = (00\ldots0\overset{i}{b}0\ldots0)H^t = bh_i$$

donde $h_i$ es la $i$-ésima columna de $H$.

## Decodificación

1. Calculamos el síndrome de la palabra recibida $S(y) = yH^t$
2. Si $S(y) = 0$ entonces no hay errores.
3. Si $S(y) \neq 0$ , entonces al ser un código perfecto, $S(y) = bh_i$, y el error cometido es $e = (00\ldots0\overset{i}{b}0\ldots0)$ y decodificamos por $y - e$

## Ejemplo

Sea $H$ la matriz de paridad de un $Ham(2, 5)$, es decir,

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

y $y = 203031$ la palabra recibida. Entonces $S(y) = (2, 3) = 2(1, 4)$ y como $(1, 4)$ es la quinta columna de $H$ el error cometido es $e = 00002$ y decodificamos por $x = y - e = 203034$