# EJEMPLO 6.3.7 MUNUERA-TENA (PAG 78)

$$\left\lfloor \frac{5-1}{2} \right\rfloor$$

$$G = \left( \begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array} \right) \quad 2\times 8 \qquad C\ [\overset{n}{8}, \overset{k}{2}, \overset{d}{5}]_2 \qquad t = 2$$

$\vec{m}\,G = \underbrace{(1,1)}\,G = (\underbrace{1\,1}\,1\,0\,0\,0\,1\,1)$ $\quad 2+6=8=n$

$$H = (-A^T \mid I_{n-k}) = \left( \begin{array}{cc|cccccc} 1 & 0 & 1 & & & & & \\ 1 & 1 & & 1 & & & 0 & \\ 1 & 1 & & & 1 & & & \\ 1 & 1 & & & & 1 & & \\ 0 & 1 & & 0 & & & 1 & \\ 0 & 1 & & & & & & 1 \end{array} \right) \quad 6\times 8$$

$n-k=6$

$C^{\perp}\ [8, 6, 2]$

$C \subset \mathbb{F}_q^{\,n}$

$C^{\perp} \subset \mathbb{F}_q^{\,n}$

$C^{\perp} = \{ \vec{u} \in \mathbb{F}_q^{\,n} \mid \vec{u}\cdot\vec{c} = \vec{0}\ \forall \vec{c} \in C \}$

$C$ H CONTROL MÍNIMO NÚMERO COLUMNAS LINEALMENTE DEPENDIENTE $= d(C)$

TENEMOS 2 BITS DE INFORMACIÓN Y 6 DE REDUNDANCIA Y PODEMOS CORREGIR 2 ERRORES

$$\vec{m} = ( \, , \, ) \in \mathbb{F}_2^2$$

$$\vec{c} = m\vec{G} = (1,1)\left(\begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right) =$$

$$= (1,1,1,0,0,0,1,1)$$

$$\vec{c} \xrightarrow{\text{RUIDO}} \vec{r}$$

$$\vec{r} = (0,0,1,0,0,0,1,1)$$

INTRODUCIMOS DOS ERRORES Y LOS CORREGIMOS

TABLA SÍNDROMES:

TAMAÑO $q^{n-k} = 2^6 = 64$

$H_{(n-k)\times n}$

$S(\vec{x}) \in \mathbb{F}_q^{n-k}$

| SINDROME | LIDER |
|---|---|
| | |

$64 \left\{ \right.$

$$S(\vec{r}) = H\vec{r}^{\,T} = \left(\begin{array}{cc|cccccc} 1 & 0 & 1 & & & & & \\ 1 & 1 & & 1 & & & 0 & \\ 1 & 1 & & & 1 & & & \\ 1 & 1 & & & & 1 & & \\ 0 & 1 & & 0 & & & 1 & \\ 0 & 1 & & & & & & 1 \end{array}\right) \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

TABLA: LIDER $(1\,1\,0\,0\,0\,0\,0\,0)$

DECODIFICACIÓN: $\vec{r}$ − LIDER $= (0\,0\,1\,0\,0\,0\,1\,1) - (1\,1\,0\,0\,0\,0\,0\,0)$

$= \vec{c}$

# POLINOMIO DE PESOS ($d^+$?)

↳ SI CONOCEMOS EL PESO DE TODAS LAS PALABRAS DEL CÓDIGO. ÚTIL CALCULAR PROBABILIDAD DE DECODIFICACIÓN EXITOSA

PARA $i=1,\dots,n$

$$a_i := a_i(C) = \#\{\vec{c} \in C \mid w(\vec{c}) = i\}$$

TENEMOS $a_0 = 1$, $a_1 = a_2 = \dots = a_{d-1} = 0$
$a_d \geq 1$

$d = d(C)$

$$\sum_{i=0}^{n} a_i = q^n$$ ← NÚMERO PALABRAS CÓDIGO

# POLINOMIO DE PESOS DE C

$$W(x) = \sum_{i=0}^{n} a_i x^i \left( = \sum_{\vec{c} \in C} x^{w(\vec{c})} \right)$$

EJ: CÓDIGO HAMMING $[7,4,3]_2$

$$W(x) = 1 + 7x^3 + 7x^4 + x^7$$ POLINOMIO DE PESOS DE C ($\Rightarrow d = 3$)

$$W^\perp(x) = 1 + 7x^4$$ POLINOMIO DE PESOS DE $C^\perp$ ($\Rightarrow d^\perp = 4$)

¿RELACIÓN?

ESCRIBIENDO EL POLINOMIO HOMOGENEIZADO

$$W(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$$

Th: $W^\perp(x,y) = q^{-k} W(y-x, y+(q-1)x)$

↳ DEDUCIMOS LA DISTANCIA MÍNIMA DE $C^\perp$

# UNA APLICACIÓN DEL POLINOMIO DE PESOS

SI $p$ ES LA PROBABILIDAD DE ERROR EN CADA BIT DURANTE LA TRANSMISIÓN EN UN CANAL BINARIO

BINARIO

LA PROBABILIDAD DE ENVIAR UNA PALABRA DEL CÓDIGO Y RECIBIR UNA PALABRA DEL CÓDIGO DIFERENTE (ERROR NO DETECTABLE) ES

$$(1-p)^n \left( W\left(\frac{p}{1-p}\right) - 1 \right)$$

PARA UN CÓDIGO SOBRE $\mathbb{F}_q$ ES:

POLINOMIO HOMOGENEIZADO

$$W\left(1-p, \frac{p}{q-1}\right) - (1-p)^n$$