

RELACIÓN EQUIVALENCIA

$$\vec{u} \sim \vec{v} \Leftrightarrow \vec{u} - \vec{v} \in C$$

$$\mathbb{F}_q^n / \sim = \mathbb{F}_q^n / C \quad \text{ESPACIO COCIENTE CUYOS}$$

ELEMENTOS SON CLASES DE EQUIVALENCIA

$$\vec{u} + C = \{ \vec{u} + \vec{x} \mid \vec{x} \in C \}$$

NÚMERO
ELEMENTOS
TOTAL

$$\# C = q^k \Rightarrow \# \mathbb{F}_q^n / \sim = q^{n-k} = \frac{q^n}{q^k}$$

ELEMENTOS
EN UNA CLASE

$$EJ: \vec{0} + C = C$$

$$PROP: \vec{u} + C = \vec{v} + C \Leftrightarrow S(\vec{u}) = S(\vec{v})$$

EJEMPLO DE RELACIÓN DE EQUIVALENCIA

$$\mathbb{Z}/\sim \quad a \sim b \Leftrightarrow a - b \in n\mathbb{Z}$$

$$n=3 \quad 3\mathbb{Z} = \{ \dots, -9, -6, -3, 0, 3, 6, 9, \dots \}$$

$$7 \sim 10 \quad 7 - 10 = -3 \in 3\mathbb{Z}$$

$$[0] = 0 + 3\mathbb{Z} = \{ \dots, -6, -3, 0, 3, 6, 9, \dots \}$$

$$[1] = 1 + 3\mathbb{Z} = \{ \dots, -5, -2, 1, 4, 7, 10, \dots \}$$

$$[2] = 2 + 3\mathbb{Z} = \{ \dots, -4, -1, 2, 5, 8, 11, \dots \}$$

$$[0] \sim [3] \sim [6]$$

$$[7] \sim [10]$$

$$7 + 3\mathbb{Z} = 10 + 3\mathbb{Z}$$

DEM: $\vec{u} + C = \vec{v} + C \stackrel{\text{DEF}}{\Leftrightarrow} \vec{u} - \vec{v} \in C \stackrel{\text{H control}}{\Leftrightarrow} H(\vec{u} - \vec{v}) = 0 \Leftrightarrow$
 $\stackrel{\text{H LINEAL}}{=} H\vec{u} = H\vec{v} \stackrel{\text{DEF}}{\Leftrightarrow} S(\vec{u}) = S(\vec{v})$

DEF: SI EN UNA CLASE EXISTE UN ÚNICO ELEMENTO DE PESO MÍNIMO, LO LLAMAREMOS EL LÍDER DE SU CLASE

PROP: CADA CLASE DE \mathbb{F}_q^n / \sim TIENE COMO MUCHO UN ELEMENTO DE PESO $\leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$

ES DECIR TODOS LOS VECTORES DE PESO MENOR O IGUAL QUE t SON LÍDERES DE UNA CLASE

DEM: POR RA

SUPONGAMOS QUE $\exists \vec{u}, \vec{v} \in \mathbb{F}_q^{\sim}$ CON $\vec{u} \neq \vec{v}$ TALES QUE

$$a) \vec{u} + \mathbb{C} = \vec{v} + \mathbb{C} \quad \text{y} \quad b) w(\vec{u}) \leq t, w(\vec{v}) \leq t$$

$$a) \vec{u} - \vec{v} \in \mathbb{C}$$

$$w(\vec{u} - \vec{v}) \leq w(\vec{u}) + w(\vec{v}) \stackrel{b)}{\leq} t + t < \frac{d}{2} + \frac{d}{2} < d$$

$$\begin{array}{l} \vec{u} - \vec{v} \in \mathbb{C} \\ w(\vec{u} - \vec{v}) < d \\ \vec{u} \neq \vec{v} \end{array} \Bigg\} \Rightarrow \text{ABSURDO}$$

CONTINUACIÓN DE DECODIFICACIÓN POR SINDROMES

RECIBIDO UN VECTOR \vec{z} , DESCODIFICAR \vec{z} SIGNIFICA ENCONTRAR LA PALABRA DE C MÁS CERCANA A \vec{z} (SIEMPRE QUE ESTA PALABRA SEA ÚNICA)

$\{\vec{z} - \vec{x} \mid \vec{x} \in C\} \leftarrow$ TODOS ESTOS VECTORES ESTÁN EN LA MISMA CLASE $\vec{z} + C$

$w(\vec{z} - \vec{x})$ MENOR $\vec{z} - \underbrace{\vec{x}}_{\in C} \in \vec{z} + C$

MÍNIMO DE $d(\vec{z}, \vec{x})$ SE OBTIENE CUANDO \vec{x} ES EL LÍDER DE LA CLASE $w(\vec{z} - \vec{x})$

LA DECODIFICACIÓN ES POSIBLE \Leftrightarrow LA CLASE DEL VECTOR RECIBIDO TIENE LÍDER

ERROR: EL LÍDER DE LA CLASE

PROPOSICIÓN (DE HACER DOS HOJAS) GARANTIZA QUE SI EL NÚMERO DE ERRORES NO SUPERA LA CAPACIDAD DEL CÓDIGO, ENTONCES LA DECODIFICACIÓN SE PUEDE HACER Y ES CORRECTA

CONSTRUIMOS TABLA:

SINDROME	LÍDER

} q^{n-k}

1 VEZ Y
SE ALMACENA

ALGORITMO DECODIFICACIÓN POR SÍNDROME

RECIBIDO $\vec{r} \in \mathbb{F}_q^n$

- 1) CALCULAR $S(\vec{r})$ Y BUSCARLO EN LA TABLA
 - 2) SI NO TIENE LÍDER: ERROR, NO DECODIFICAMOS
 - 3) SI TIENE LÍDER: OUTPUT ES \vec{r} -LÍDER
- PUESTO QUE SE DECIDE QUE EL LÍDER ES EL ERROR COMETIDO

↑
HEMOS
PROBADO

Como el síndrome es la columna correspondiente a la posición del error y cada líder a lo sumo presenta un único error, por lo tanto se deduce que es 1 la capacidad correctora

EJ

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

$$[6, 3, 3]$$

$$t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$$

SINDROME	LIDER
(0 0 0)	(0 0 0 0 0 0)
(1 1 1)	(1 0 0 0 0 0)
(1 0 1)	(0 1 0 0 0 0)
(1 1 0)	(0 0 1 0 0 0)
(1 0 0)	(0 0 0 1 0 0)
(0 1 0)	(0 0 0 0 1 0)
(0 0 1)	(0 0 0 0 0 1)
(0 1 1)	—

CON OTRO ORDEN
EL EJEMPLO AYER