CÓDIGOS Y CRIPTOGRAFÍA DIEGO RUANO 20/9 2022

RELACIÓN EQUIVALENCIA

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

$$\mathbb{F}_q^n / \sim \; = \mathbb{F}_q^n / C$$ 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: $\vec{u} + C = \vec{v} + C \iff S(\vec{u}) = S(\vec{v})$

EJEMPLO DE RELACIÓN DE EQUIVALENCIA

$\mathbb{Z}/\sim \qquad a \sim b \iff a - b \in n\mathbb{Z}$

$n = 3 \qquad 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

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

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

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

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

$[0] = [3] = [6] \qquad [7] = [10] \qquad 7 + 3\mathbb{Z} = 10 + 3\mathbb{Z}$

DEM: $\vec{u}+C = \vec{v}+C \overset{\text{DEF}}{\iff} \vec{u}-\vec{v} \in C \overset{H \text{ control}}{\iff} H(\vec{u}-\vec{v}) = 0 \iff$

$\overset{H \text{ LINEAL}}{\iff} H\vec{u} = H\vec{v} \overset{\text{DEF}}{\iff} S(\vec{u}) = S(\vec{v})$

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

PROP: CADA CLASE DE $\mathbb{F}_q^n/\mathcal{C}$ 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 $\exists\ \vec{u}, \vec{v} \in \mathbb{F}_q^n$ CON $\vec{u} \neq \vec{v}$ TALES QUE

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

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

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

$$\left.\begin{array}{l} \vec{u} - \vec{v} \in C \\ w(\vec{u} - \vec{v}) < d \end{array}\right\} \lightning \text{ ABSURDO}$$

$\vec{u} \neq \vec{v}$

CONTINUACIÓN DE DECODIFICACIÓN POR SINDROMES

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

$\{\vec{r}-\vec{x} \;/\; \vec{x}\in C\}$ ← TODOS ESTOS VECTORES ESTÁN EN LA MISMA CLASE $\vec{r}+C$

$w(\vec{r}-\vec{x})$ MENOR

$\vec{r}-\underbrace{\vec{x}}_{\in C} \in \vec{r}+C$

MÍNIMO DE $d(\vec{r},\vec{x})$ SE OBTIENE CUANDO $\vec{x}$

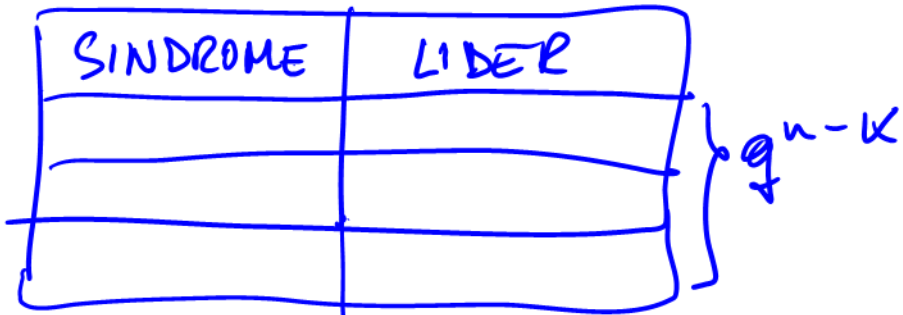
$w(\vec{r}-\vec{x})$ ES EL LÍDER DE LA CLASE

LA DECODIFICACIÓN ES POSIBLE $\Longleftrightarrow$ LA CLASE DEL VECTOR RECIBIDO TIENE LÍDER

ERROR: EL LÍDER DE LA CLASE

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

CONSTRUIMOS TABLA:



1 VEZ Y SE ALMACENA

ALGORITMO DESCODIFICACIÓN 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 DESCODIFICAMOS

3) SI TIENE LÍDER: OUTPUT ES $\vec{r}$ − LÍDER

PUESTO QUE SE DECIDE QUE EL LÍDER ES EL ERROR COMETIDO

↑ HEMOS PROBADO

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 SYEN