CÓDIGOS Y CRIPTOGRAFIA

DIEGO RUANO 13/9 2022

CÓDIGOS DE BLOQUE

UN CÓDIGO DE BLOQUE C ES UN CONJUNTO DE PALABRAS DE LA MISMA LONGITUD

$$C = \{c_1, \dots, c_M\} \quad \text{DONDE} \quad c_i \in \mathbb{F}_q^n$$

EL CODIGO TIENE M PALABRAS DE LONGITUD n

EJEMPLO: CÓDIGO REPETICIÓN
CÓDIGO BIT PARIDAD
CÓDIGO DE HAMMING
} CLASE 7/9

¿CUANTOS ERRORES SE PUEDEN CORREGIR?

DISTANCIA DE HAMMING

↳ NOS VA A DECIR CUANTOS ERRORES PODEMOS DETECTAR Y CORREGIR

DEF: $\vec{x}, \vec{y} \in \mathbb{F}_q^n$ $\quad \vec{x} = (x_1, \dots, x_n)$ $\quad \vec{y} = (y_1, \dots, y_n)$

LA DISTANCIA DE HAMMING ENTRE $\vec{x}$ E $\vec{y}$

$$d(\vec{x}, \vec{y}) = \#\{i / 1 \leq i \leq n, \ x_i \neq y_i\}$$

NÚMERO DE POSICIONES EN LAS QUE DIFIEREN

$$d((1001), (1000)) = 1$$

$$d((1001), (0110)) = 4$$

EN MATEMÁTICAS EL CONCEPTO DE DISTANCIA SIGNIFICA QUE:

$$\begin{cases} \bullet\ d(\vec{x},\vec{y}) \geq 0 \ \text{ y } \ d(\vec{x},\vec{y}) = 0 \iff \vec{x} = \vec{y} \\ \bullet\ d(\vec{x},\vec{y}) = d(\vec{y},\vec{x}) \\ \bullet\ d(\vec{x},\vec{y}) + d(\vec{y},\vec{z}) \geq d(\vec{x},\vec{z}) \end{cases}$$

i • $x_i = z_i$ ✓

• $x_i \neq z_i$ ⇒ APORTA 1 DERECHA

$\begin{cases} x_i = y_i \\ y_i = z_i \end{cases}$ ⇒ APORTA 0 ó 2 IGUALES ⇒ $x_i = z_i$ NO PASA

DEF: LLAMAREMOS DISTANCIA MINIMA DEL CODIGO C A

$$d = d(C) = \min \{ d(\vec{x},\vec{y}) \mid \vec{x},\vec{y} \in C,\ \vec{x} \neq \vec{y} \}$$

DESCODIFICACIÓN - ALGORITMO

RECIBIMOS UNA PALABRA $\vec{r}$

- SI $\vec{r}$ ES DEL CÓDIGO NO HACEMOS NADA
- SI NO ES DEL CÓDIGO DESCODIFICAMOS $\vec{r}$ POR LA PALABRA CÓDIGO MÁS CERCANA (SI ES ÚNICA)

DISTANCIA HAMMING

$$\#\text{ERRORES} = d(\vec{c}, \vec{r})$$

PODEMOS:

a) DETECTAR t ERRORES, $t < d$

b) CORREGIR t ERRORES, $2t < d$

c) CORREGIR s BORRONES, $s < d$

d) (b+c) CORREGIR t ERRORES Y s BORRONES

SI $2t + s < d$

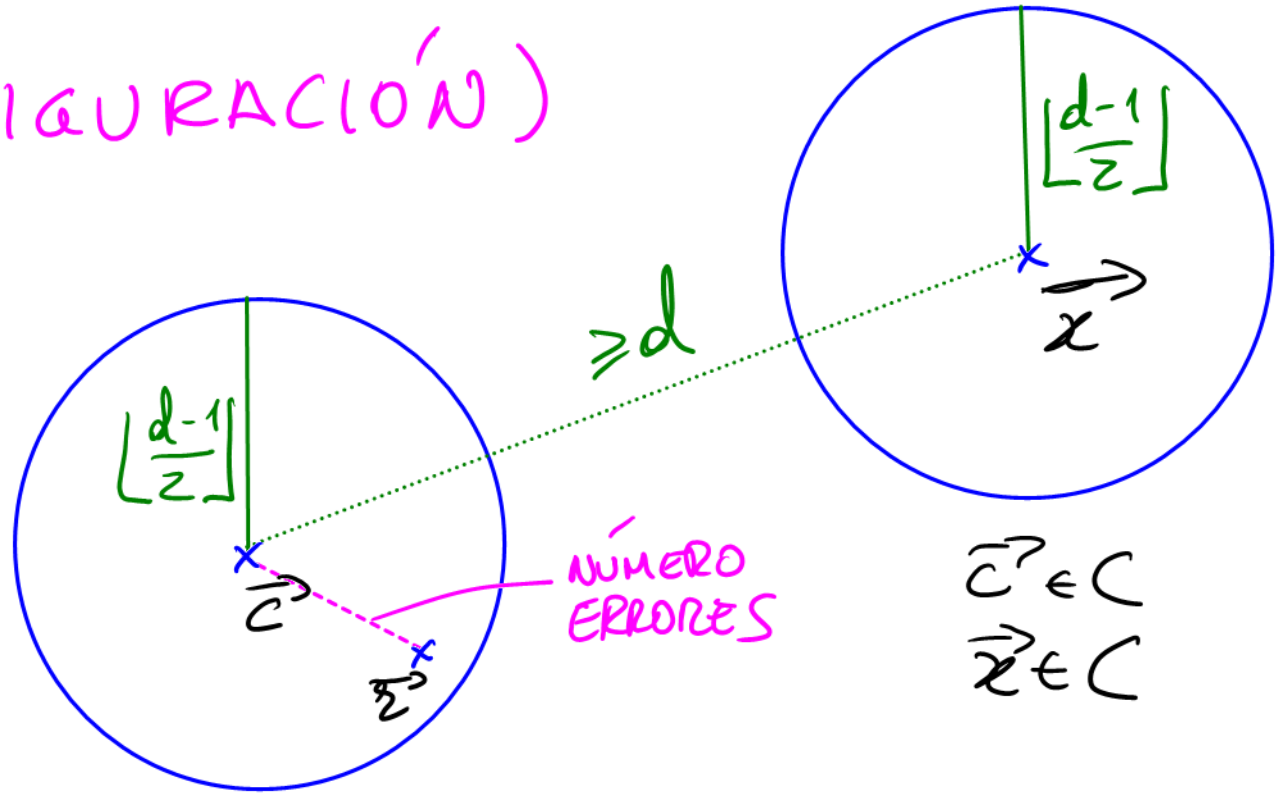
(CUALQUIER CONFIGURACIÓN)

$(0,0,0) \xrightarrow{2} (?\,0\,?)$

2 BORRONES

$(0,0,0) \xrightarrow{3} (1\,0\,1)$

2 ERRORES



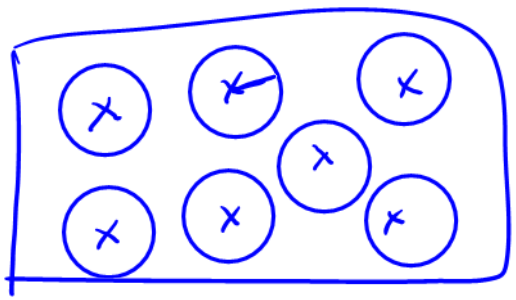
DEMOSTRACIÓN:

a) $\vec{c} \rightsquigarrow \vec{x}$ (RUIDO) $\quad \vec{c}, \vec{x} \in C \;,\; \vec{c} \neq \vec{x}$

NO DETECTAMOS

SÓLO PASA SI HAY $\geq d$ ERRORES

b)



$\mathbb{F}_q^n$

BOLAS:

CENTRO $\vec{x} \in C$

RADIO $< \frac{d}{2}$

BOLAS CON CENTRO UNA PALABRA DEL CÓDIGO Y RADIO $\left\lfloor \frac{d-1}{2} \right\rfloor$ SON DISJUNTAS

$$d(\vec{z}, \vec{c}) < d(\vec{z}, \vec{x}) \quad \forall \vec{x} \neq \vec{c},\ \vec{x} \in C$$

↑ QUEREMOS

$\vec{r}$ VA A ESTAR EN LA BOLA DE CENTRO $\vec{c}$. Y SOLO EN ESA BOLA PORQUE SON DISJUNTAS

RAZONAMOS POR REDUCCIÓN AL ABSURDO: (SUPONEMOS LO CONTRARIO A LO QUE QUEREMOS PROBAR Y LLEGAMOS A UNA CONTRADICCIÓN)

SUPONEMOS QUE $\vec{r}$ ESTÁ EN UNA BOLA DE CENTRO OTRA PALABRA DEL CÓDIGO (DISTINTA DE $\vec{c}$)

$$\exists\, \vec{x} \in C \,,\ \vec{x} \neq \vec{c} \quad \text{TAL QUE}$$

$$d(\vec{r}, \vec{x}) \leq \frac{d-1}{2}$$

$$d(\vec{r},\vec{x}) \leq d(\vec{r},\vec{c}) \leq \frac{d-1}{2}$$

↑ POR HIPÓTESIS

ENTONCES (DESIGUALDAD TRIANGULAR)

$$d(\vec{c},\vec{x}) \leq d(\vec{c},\vec{r}) + d(\vec{r},\vec{x}) \leq d-1 < d$$

$$d(\vec{c},\vec{r}) \leq \frac{d-1}{2} \qquad d(\vec{r},\vec{x}) \leq \frac{d-1}{2}$$

↑ ¡CONTRADICCIÓN!

d ES LA DISTANCIA MÍNIMA

⇒ NO HAY OTRA PALABRA DEL CÓDIGO QUE ESTÉ MÁS CERCA DE $\vec{r}$ QUE $\vec{c}$

⇒ $\vec{c}$ ES LA PALABRA MÁS CERCANA

S PODEMOS SUPONER (SALVO REORDENACIÓN) QUE SE HAN BORRADO LAS PRIMERAS s POSICIONES

$$\vec{x} = (\underbrace{? \; ? \; \dots \; ?}_{s}, x_{s+1}, \dots, x_n) \quad \text{TENEMOS QUE}$$

$$\vec{c} = (c_1, -, c_s, c_{s+1} -, c_n)$$

COINCIDEN EN LAS ÚLTIMAS $n-s$ POSICIONES

SI $\vec{x} \in C$ TAMBIÉN COINCIDE ULTIMAS $n-s$ POSICIONES

$\Rightarrow d(\vec{c}, \vec{x}) \leq s < d$ ABSURDO SI $\vec{x} \neq \vec{c}$

POR LO QUE DECODIFICAMOS POR LA PALABRA DEL CODIGO QUE ES IGUAL EN LAS POSICIONES NO BORRADAS

DEF: SI d ES LA DISTANCIA MÍNIMA DE C DIREMOS QUE C CORRIGE $\left\lfloor \frac{d-1}{2} \right\rfloor$ ERRORES O QUE ES UN CÓDIGO $\left\lfloor \frac{d-1}{2} \right\rfloor$-CORRECTOR

EJ: CANAL EN EL QUE UN SÍMBOLO ES ALTERADO CON PROBABILIDAD p, SE DEBE EMPLEAR UN CÓDIGO QUE CUMPLA AL MENOS QUE

$$\left\lfloor \frac{d-1}{2} \right\rfloor \geq np$$

PORQUE SE ESPERA UNA MEDIA DE np SIMBOLOS INCORRECTOS EN CADA PALABRA

BIBLIOGRAFIA

MUNUERA-TENA : SECCIÓN 6.1
SECCIÓN 4.2

JUSTESE-HØHOLDT : SECCIÓN 1.1
SECCION 1.2

UN POCO DE CAPITULO 5

CAPITULO 2 CUERPOS FINITOS