CÓDIGOS Y CRIPTOGRAFÍA DIEGO RUANO 14/9 2022

CÓDIGO BLOQUE $C = \{\vec{c}_1, \ldots, \vec{c}_M\} \;/\; \vec{c}_i \in \mathbb{F}_q^n$

ES PRÁCTICO DOTAR A UN CÓDIGO DE BLOQUE DE MÁS ESTRUCTURA:

UN (n,k)-CÓDIGO LINEAL ES UN SUBESPACIO K-DIMENSIONAL DE $\mathbb{F}_q^n$

SE TIENE QUE $\vec{x}+\vec{y} \in C$ y $\lambda \vec{x} \in C$, $\forall \vec{x},\vec{y} \in C$ $\forall \lambda \in \mathbb{F}_q$

NOTA: $\vec{0}$ SIEMPRE ES UN ELEMENTO DE UN CÓDIGO LINEAL

NOTA: EL NÚMERO DE PALABRAS EN C ES q^k

CÓDIGO: $C \subset \mathbb{F}_2^4$

$$\left\{ \begin{matrix} (0011), & (1,0,1,0), & (1,0,0,1), & (0,1,0,1) \\ (1,1,0,0), & (1,1,1,1), & (0,1,1,0), & (0,0,0,0) \end{matrix} \right\}$$

ES UN CÓDIGO DE BLOQUE DE LONGITUD 4 CON 8 PALABRAS

¿ES LINEAL? ✓

¿COMO CODIFICAMOS?

$$\mathbb{F}_2^3 \longrightarrow C$$

$$8 = 2^3 \Rightarrow 3 \text{ BITS} \qquad (x,y,z) \longmapsto ?$$

AYUDA: MATRIZ GENERATRIZ O GENERADORA

UNA MATRIZ GENERADORA DE $C \subseteq \mathbb{F}_q^n$ ES UNA MATRIZ DE UNA APLICACIÓN LINEAL INYECTIVA $f: \mathbb{F}_q^k \longrightarrow C$

ES DECIR, A UNA MATRIZ $k \times n$ CUYAS FILAS SON UNA BASE DE C

NOTA: EN TEORÍA DE CÓDIGOS ES TRADICIÓN MULTIPLICAR POR LA IZQUIERDA

UNA MATRIZ GENERADORA NO ES ÚNICA ¿POR QUÉ?

↳ HAY TANTAS COMO BASES DE C

UNA MATRIZ GENERADORA G PROPORCIONA UN CÓDIGO ($\mathrm{Im}(G)$) Y TAMBIÉN UNA CODIFICACIÓN

$$C = \{\vec{a}G \mid \vec{a} \in \mathbb{F}_q^k\}$$

$\vec{a}$ VECTOR FILA

EL MENSAJE $\vec{a} \in \mathbb{F}_q^k$, SE CODIFICA EN $\vec{a}G \in \mathbb{F}_q^n$

EJ:

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^4$$
$$\vec{a} \longmapsto \vec{a}G$$

¿RELACIÓN CON EJEMPLO ANTERIOR?

PARÁMETROS FUNDAMENTALES DE UN CÓDIGO

$$[\underset{\substack{\uparrow \\ \text{LONGITUD}}}{n}, \underset{\substack{\uparrow \\ \text{DIMENSIÓN}}}{k}, \underset{\substack{\uparrow \\ \text{DISTANCIA MÍNIMA}}}{d}]_q$$

PARA COMPARAR O PARA TENER UNA IDEA REAL DE LOS PARÁMETROS DE UN CÓDIGO TAMBIÉN SE CONSIDERA

$$R(C) = \frac{k}{n} \qquad \delta(C) = \frac{d(C)}{n}$$

DIMENSIÓN Y DISTANCIA RELATIVA

CODIFICACIÓN SISTEMÁTICA

$\vec{a} \in \mathbb{F}_q^{k}$, $\quad \vec{a}G = (\underset{\text{INFORMACIÓN}}{\vec{a}}, \underset{\text{CONTROL}}{\vec{z}}) \quad \vec{z} \in \mathbb{F}_q^{n-k}$

ASÍ EL ÚLTIMO PASO DE DESCODIFICACIÓN ES AUTOMÁTICO.

$$G = (I_k, A) = {}_{k}\left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & A \\ 0 & & 1 & \end{array}\right]_{k} \qquad \text{FORMA ESTANDARD}$$

(columnas: $\underbrace{\quad}_{k}$ | $\underbrace{\quad}_{n-k}$)

C ES SISTEMÁTICO SI POSEE UNA MATRIZ GENERADORA DE FORMA ESTANDARD

DEF: DIREMOS QUE DOS CÓDIGOS C_1, C_2 SON EQUIVALENTES SI EXISTE UNA PERMUTACIÓN σ DEL CONJUNTO $\{1, \ldots, n\}$ TAL QUE

$$C_2 = \{\sigma(c) \mid c \in C_1\}$$

PROPOSICIÓN: TODO CÓDIGO ES EQUIVALENTE A UNO SISTEMÁTICO

DEMOSTRACIÓN: FORMA ESCALONADA REDUCIDA DE LA MATRIZ G Y REORDENAR COLUMNAS

EJ ANTES:

$$G' = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

MATRIZ DE CONTROL

$$\text{SUBESPACIO VECTORIAL} \begin{cases} \text{SISTEMA GENERADORES} \\ \text{ECUACIONES IMPLÍCITAS} \end{cases}$$

DEF: UNA MATRIZ H ES UNA MATRIZ DE CONTROL DEL CÓDIGO C SI $\forall \vec{x} \in \mathbb{F}_q^n$

$$\vec{x} \in C \iff H\vec{x}^t = \underset{n-k}{\vec{0}^t}$$

$$\begin{array}{cc} G & H \\ k \times n & (n-k) \times n \\ \text{RANGO } k & \text{RANGO } n-k \end{array}$$

EJ: $H = (1\ 1\ 1\ 1)$

↳ EJ ANTERIOR

PROPOSICIÓN: $GH^t = 0$

$k \times (n-k)$-MATRIZ DE CEROS

$G = (I_k, A) \Rightarrow H = (-A^T, I_{n-k})$

ES UNA MATRIZ DE CONTROL

$$w_H(\vec{x}) = \{ i \mid 1 \leq i \leq n,\ x_i \neq 0 \} = d(\vec{x}, \vec{0})$$

↳ NORMA

PESO MÍNIMO DE C

$$w(C) = \min \{ w_H(\vec{c}) \mid \vec{c} \in C,\ \vec{c} \neq \vec{0} \}$$

EN CODIGOS LINEALES $d(C) = w(C)$

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

$$w(C) = \min\{ w(\vec{x}) \mid \vec{x} \in C \;,\; \vec{x} \neq \vec{0} \}$$

$\leq$ EN GENERAL

$$d(\vec{x},\vec{y}) = d(\vec{x}-\vec{y},\vec{0}) = w(\underbrace{\vec{x}-\vec{y}})$$

$$\vec{x}-\vec{y} \in C$$

$$w(\vec{x}) = d(\vec{x},\vec{0})$$

¿CÓMO SE CALCULA $d(C)$?

PROP: C CON MATRIZ DE CONTROL H Y DISTANCIA MÍNIMA d

$d \geq r \iff r$ COLUMNAS CUALQUIERA DE H SON LINEALMENTE INDEPENDIENTES

COROLARIO: MENOR NÚMERO DE COLUMNAS LINEALMENTE DEPENDIENTES DE H ES IGUAL A d

NOTA: MÉTODO NO COMPUTACIONALMENTE EFICIENTE

DEM

SUP. r COLUMNAS DE H LINEALMENTE DEPENDIENTES
(1)
$$H\vec{x}^T = \vec{0} \quad \text{CON} \quad \vec{x}$$ VECTOR COEFICIENTES COMBINACIÓN LINEAL

$$\Rightarrow \vec{x} \in C \,, \quad w(\vec{x}) \leq \vec{r} \Rightarrow d(C) \leq \vec{r}$$

SUP. r COLUMNAS CUALQUIERA DE H SON
(2) LINEALMENTE INDEPENDIENTES

$$\text{SI } \vec{x} \in C \Rightarrow H\vec{x}^T = \vec{0} \Rightarrow w(\vec{x}) > r$$

$$\Rightarrow d(C) > r$$

DEM (DESPACIO) (1)

$\vec{v}_1, \dots, \vec{v}_k$ SON LINEALMENTE DEPENDIENTES SI EXISTEN $x_1, \dots, x_k \in \mathbb{F}_q$ CON $(x_1, \dots, x_k) \neq (0, \dots, 0)$, TALES QUE

$$x_1\vec{v}_1 + \dots + x_k\vec{v}_k = \vec{0}$$

$$H\vec{x}^t = \vec{0} \iff$$

$$\begin{pmatrix} \boxed{h_1} & \cdots & \boxed{h_n} \end{pmatrix} \cdot \vec{x}^t = \vec{0} \iff x_1 \boxed{h_1} + \dots + x_n \boxed{h_n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\boxed{h_{i_1}}, \dots, \boxed{h_{i_r}}$ LINEALMENTE DEPENDIENTES $\Rightarrow \exists\, x_{i_1}, \dots, x_{i_r} \,/\, x_{i_1}\boxed{h_{i_1}} + \dots + x_{i_r}\boxed{h_{i_r}} = \vec{0}$

SEA $x_i = 0$ SI $i \neq i_1, \dots, i_r \Rightarrow x_1 \boxed{h_1} + \dots + x_n \boxed{h_n} = \vec{0} \Rightarrow$

$$\Rightarrow H\vec{x}^t = \vec{0} \Rightarrow \vec{x} \in C \Rightarrow w(\vec{x}) \leq r \Rightarrow d(C) \leq r \;\square$$

(2) $\vec{x} \in C$, $\vec{x} \neq 0$ $\Rightarrow H\vec{x} = \vec{0} \Rightarrow x_1 \boxed{h_1} + \dots + x_n \boxed{h_n} = \vec{0}$

SI $w(\vec{x}) \leq r \Rightarrow \underset{\neq 0}{x_{i_1}} \boxed{h_{i_1}} + \dots + \underset{\neq 0}{x_{i_{w(\vec{x})}}} \boxed{h_{i_{w(\vec{x})}}} = \vec{0}$

$\Rightarrow$ HAY r COLUMNAS LINEALMENTE DEPENDIENTES

$\lightning$ ABSURDO $\Rightarrow w(\vec{x}) > r \Rightarrow d(C) > r$ $\square$

EJ:

$$\underset{n-k}{H} = \overset{n}{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}$$

¿$[n, k, d]_2$?

$[7, 4, \ ]_2$

G $k \times n$

H $n-k \times n$

• ¿1 columna cualquiera es linealmente independiente?

Sí, todas son diferentes de $\vec{0}$. $d > 1$

• ¿2 columnas cualquiera son L.I.?

$$\lambda_1 \boxed{} + \lambda_2 \boxed{} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \lambda_i \in \mathbb{F}_2 \Rightarrow \lambda_1 = \lambda_2 = 1$$

$$\boxed{} + \boxed{} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \boxed{} = -\boxed{} \Leftrightarrow \boxed{} = \boxed{}$$

NO HAY DOS COLUMNAS IGUALES $d > 2$

$\Rightarrow$ 2 COLUMNAS CUALQUIERA SON L.I.

- ¿3 COLUMNAS CUALQUIERA SON L.I?

3 PRIMERAS

$$\begin{pmatrix}0\\0\\1\end{pmatrix}+\begin{pmatrix}0\\1\\0\end{pmatrix}+\begin{pmatrix}0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

$d \le 3$

POR TANTO

$$d(C) = 3$$