CÓDIGOS Y CRIPTOGRAFIA. INFORMÁTICA. DIEGO RUANO 28/9 2022

COTA DE SINGLETON

$d \leq n-k+1$

Th: C código $[n,k,d]_q \Rightarrow n+1 \geq d+k$

$[10,\cancel{6},6]$

DEM: NÓTESE QUE ESTA DEMOSTRACIÓN ES VÁLIDA PARA UN CÓDIGO DE BLOQUE, NO NECESARIAMENTE LINEAL

q^k PALABRAS DE C

$$q\left\{\begin{array}{l} (\quad * \cdots *) \in \mathbb{F}_q^n \\ (\quad * \quad *) \\ \vdots \\ (\quad \underbrace{* \quad *}_{d-1}) \end{array}\right. \rightsquigarrow q\left\{\begin{array}{l} (\quad\quad) \in \mathbb{F}_q^{n-(d-1)} \\ (\quad\quad) \\ \vdots \\ (\ ,\ \ ,\ ) \end{array}\right.$$

BORRAMOS

$\mathbb{F}_q \qquad \mathbb{F}_q$

$q^{n-(d-1)}$ POSIBLES VECTORES

¿SON TODOS DIFERENTES?

SI DOS FUERAN IGUALES LAS PALABRAS CORRESPONDIENTES DE $\mathbb{F}_q^n$ ESTARÍAN A DISTANCIA $\leq d-1$

$d=3$

$(1\ 2\ \cancel{x}\ \cancel{x})$

$(1\ 2\ \cancel{x}\ \cancel{x})$ 2

$$\Rightarrow q^k \leq q^{n-(d-1)} \iff k \leq n-(d-1) \iff$$

$$\iff n+1 \geq k+d$$

CÓDIGOS REED-SOLOMON

Sean $x_1, \ldots, x_n$ elementos diferentes de $\mathbb{F}_q$. Para $k \leq n$ consideramos $\mathbb{P}_k$ el conjunto de polinomios de $\mathbb{F}_q[x]$ de grado menor que k. Un código Reed-Solomon es

$$RS_{k,n} = \{ (f(x_1), \ldots, f(x_n)) \mid f \in \mathbb{P}_k \} \qquad k \leq n$$

Nota: Se tiene que $n \leq q$

Normalmente se toma $n = q$ (maximizar longitud) ó $n = q-1$ para tener una estructura cíclica y $x_i = \alpha^i$ para $\langle \alpha \rangle = \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

Lema: Un código RS es un código lineal

$$c = (f(x_1), \ldots, f(x_n)), \quad c' = (f'(x_1), \ldots, f'(x_n)) \in C$$

$\underset{\mathbb{F}_q}{\lambda} c + \underset{\mathbb{F}_q}{\mu} c' \in C$? $\quad \lambda c + \mu c' = (\lambda f(x_1) + \mu f'(x_1), \ldots, \lambda f(x_n) + \mu f'(x_n))$

$$= ((\lambda f + \mu f')(x_1), \ldots, (\lambda f + \mu f')(x_n)) \in C$$

LEMA: LA DIMENSIÓN DE $RS_{k,n}$ ES k

DEM: $\mathbb{P}_k$ ES UN ESPACIO VECTORIAL DE DIMENSION k SOBRE $\mathbb{F}_q$

BASE: $\{1, x, x^2, \ldots, x^{k-1}\}$

$$ev: \mathbb{P}_k \longrightarrow \mathbb{F}_q^n \qquad \operatorname{Im}(ev) = RS_{k,n}$$

$$f \longmapsto (f(x_1), \ldots, f(x_n))$$

¿ES INYECTIVA? SI $\Rightarrow \dim RS_{k,n} = k$

$\Leftrightarrow f, g \;/\; (f(x_1), \ldots, f(x_n)) = (g(x_1), \ldots, g(x_n))$

$((f-g)(x_1), \ldots, (f-g)(x_n)) = (0, \ldots, 0)$

$(f-g)(x)$ TIENE AL MENOS n RAICES: $x_1, \ldots x_n$

$$\deg(f-g(x)) < k \leq n \Rightarrow f-g=0 \Rightarrow f=g$$

$\mathfrak{M}$: USAMOS

UN POLINOMIO NO NULO DE GRADO m TIENE COMO MUCHO m RAICES

$$f(x_i)=0 \Rightarrow (X-x_i) \mid f$$

$$f=(X-x_i)\cdot \underline{\qquad}$$

Th: LA DISTANCIA MÍNIMA DE UN CÓDIGO $RS_{k,n}$ ES

$$n-k+1$$

$[4,3,2]$

$4+1 \leq 3+2$

POR TANTO SUS PARAMETROS VERIFICAN LA COTA DE SINGLETON Y DECIMOS QUE TENEMOS UN CÓDIGO MDS (MAXIMUM DISTANCE SEPARABLE)

$k+d=$
$k+(n-k+1)=$
$n+1$

DEM:

$$c=(f(x_1),\dots,f(x_n))\in C \quad , \quad \deg(f)<k$$

$c_i=0 \Rightarrow f(x_i)=0 \Rightarrow x_i$ ES UNA RAIZ DE f

$\deg(f)<k \Rightarrow f$ TIENE COMO MUCHO $k-1$ RAICES $\Rightarrow$

$\Rightarrow c$ TIENE COMO MUCHO $k-1$ POSICIONES IGUALES A 0

$\Rightarrow c$ TIENE AL MENOS $n-(k-1)$ POSICIONES $\neq$ DE 0

$\Rightarrow w(c) \geq n-(k-1) = n-k+1$

$\Rightarrow d(C) \geq n-k+1$

$d(C) \leq n-k+1$ $\quad\Big\}\; d(C) = n-k+1 \quad \square$

↳ COTA SINGLETON

$n \leq q$ DESVENTAJA

CODIFICACIÓN

$$m = (m_0, \ldots, m_{k-1}) \in \mathbb{F}_q^k$$

CONSTRUIMOS EL POLINOMIO $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$ DE GRADO MENOR QUE k Y CODIFICAMOS m COMO

$$(m(x_1), \ldots, m(x_n)) \in \mathbb{F}_q^n$$

NO ES UNA CODIFICACIÓN SISTEMÁTICA

EJ: NO HAY CÓDIGOS BINARIOS INTERESANTES

$\mathbb{F}_5$ $n=4$ $k=3$

$x_1 = 1$, $x_2 = 2$

$x_3 = 3$ $x_4 = 4$

$f = 1$ $(1\ 1\ 1\ 1)$

$f = x$ $(1\ 2\ 3\ 4)$

$f = x^2$ $(1\ 4\ 4\ 1)$

$f = x^2 + 1$ $(2\ 0\ 0\ 2)$

$\mathbb{F}_5^3 \to \mathbb{F}_5^4$

$\vec{m} \mapsto \vec{c}$

$RS_{3,4}$ $\vec{m} = (3, 0, 2)$

$m(x) = 3 + 2x^2$ $(3 \cdot 1 + 0 \cdot x + 2 \cdot x^2)$

$\vec{c} = (m(1), m(2), m(3), m(4))$

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

$\{1, x, x^2\}$ BASE DE $\mathbb{P}_3$

$$m(x) = 3 + 2x^2$$

BASE DE C ES
$\{ev(1), ev(x), ev(x^2)\}$

$$\vec{c} = 3 \cdot ev(1) + 2 \cdot ev(x^2)$$

$$= 3 \cdot (1,1,1,1) + 2 \cdot (1,4,4,1)$$

$$= (3,3,3,3) + (2,3,3,2)$$

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

$$G = \begin{array}{cl} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix} & \begin{array}{l} \leftarrow ev(1) \\ \leftarrow ev(x) \\ \leftarrow ev(x^2) \end{array} \end{array}$$

$$c = (3\ 0\ 2) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix} = (0\,1\,1\,0)$$

FÁCILES

$\alpha = 2$ $\quad 2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3$ $\quad \mathbb{F}_5^* = \mathbb{F}_5 \setminus \{0\}$

$2^0 = 2^4$

$\mathbb{F}_5^* = \langle \alpha \rangle = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3\}$

$$\{\alpha^1, \alpha^2, \alpha^3, \alpha^4\}$$

$$\alpha^1 = 2 = x_1, \quad \alpha^2 = 4 = x_2, \quad \alpha^3 = 3 = x_3, \quad \alpha^4 = 1 = x_4$$

$\alpha = 4$ NO VALE: $\quad 4^0 = 1 \quad 4^1 = 4 \quad 4^2 = 1 \quad 4^3 = 4$

PERO SIEMPRE EXISTE UN α CON ESTA PROPIEDAD

DIFÍCILES

$$\mathbb{F}_{16} = \{0\} \cup \underbrace{\{\alpha^1, \alpha^2, \ldots, \alpha^{15}\}}_{} = \langle \alpha \rangle$$

$$\alpha^1 = x_1, \quad \alpha^2 = x_2, \quad \ldots, \quad \alpha^{15} = x_{15}$$

α RAIZ DE $X^4 + X + 1$

$\alpha = [X]$

MATRIZ GENERADORA BASE $\mathbb{P}_k$ $\{1, x, x^2, \dots, x^{k-1}\}$

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & & x_n \\ x_1^2 & & x_n^2 \\ & & \\ x_1^{k-1} & & x_n^{k-1} \end{pmatrix} \begin{array}{l} \leftarrow ev(1) \\ \leftarrow ev(x) \\ \leftarrow ev(x^2) \\ \\ \leftarrow ev(x^{k-1}) \end{array} \quad (*)$$

Si $n = q-1$ y $x_i = \beta^{i-1}$ con $\langle \beta \rangle = \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

α ANTES

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & & \beta^{n-1} \\ \vdots & \beta^2 & & \beta^{2(n-1)} \\ & \vdots & & \\ 1 & \beta^{k-1} & & \beta^{(k-1)(n-1)} \end{pmatrix}_{k \times n} = \Big(\underbrace{\beta^{(i-1)(j-1)}}_{= g_{ij}} \Big)_{\substack{i=1,\dots,n \\ j=1,\dots,n}}$$

FILA $i \rightarrow$

MATRIZ CONTROL

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ \vdots & \beta^2 & \cdots & \beta^{2(n-1)} \\ \vdots & & & \vdots \\ 1 & \beta^{n-k} & & \beta^{(n-k)(n-1)} \end{pmatrix}_{n-k \times n}$$

FILA r

$$\begin{cases} G = (I_k \mid A) \\ H = (-A^T \mid I_{n-k}) \end{cases}$$

$\to$ AQUÍ NO

$(a^b)^c = a^{b\cdot c}$

$a^b \cdot a^c = a^{b+c}$

DEM: $GH^T = 0$ Y TAMAÑOS ADECUADOS

$M = GH^T$

$M = (m_{ir})_{\substack{1 \le i \le n-k \\ 1 \le r \le n}}$

FILA i DE G POR FILA r DE H

$$m_{ir} = \sum_{j=1}^{n} \beta^{(i-1)(j-1)} \beta^{r(j-1)} = \sum_{j=1}^{n} \left(\beta^{i-1+r}\right)^{j-1}$$

$\beta^{(i-1)(j-1)+r(j-1)}$

$$= \underset{\underset{a_1}{\|}}{1} \cdot \frac{\left(\beta^{i-1+r}\right)^n - 1}{\beta^{i-1+r} - 1} = \frac{1-1}{?\neq 0} = \frac{0}{?\neq 0} = 0$$

$\left(\beta^{i-1+r}\right)^n = 1$ (*)

$\beta^{i-1+r} \neq 1$ (*)

$a_n = a_1 s^{n-1}$

$\sum_{j=1}^{n} a_j = a_1 \frac{s^n - 1}{s-1}$, $a_1 = 1$

s RAZÓN

$a^{q-1} = 1$ CIERTO SIEMPRE

$a \neq 0$

$\mathbb{F}_5$ $\underset{1}{\underset{\shortparallel}{2^0}}, 2, \underset{4}{\underset{\shortparallel}{2^2}}, \underset{3}{\underset{\shortparallel}{2^3}}, \underset{1}{\underset{\shortparallel}{2^4}}$ $\boxed{2^4 = 2^{q-1} = 1}$ $\mathbb{F}_5^* = \{2^i \mid i = 0, \dots, q-2\}$

$4, \underset{1}{\underset{\shortparallel}{4^2}}, \underset{4}{\underset{\shortparallel}{4^3}}, \underset{1}{\underset{\shortparallel}{4^4}}$ $4^{q-1} = 1$

$\mathbb{F}_{p^e}$

TAMBIÉN

$\alpha = [x]$ $\alpha^{q-1} = 1$

$$\beta^{i-1+r} \neq 1$$

- $\underset{1}{\underset{\vee\!\shortparallel}{i}} - 1 + \underset{1}{\underset{\vee\!\shortparallel}{r}} > 0$ $\beta^{i-1+r} \geq \beta$ "ALGO MAYOR QUE CERO" $\Rightarrow$ NO ES 1 $(\beta^0 = 1)$

- $i - 1 + r < q - 1$?

$i - 1 + r \leq k - 1 + n - k = n - 1 = q - 2 \Rightarrow i - 1 + r < q - 1$

CALCULAMOS EN SAGE EL EJEMPLO 2.2.3 SOBRE CUERPOS FINITOS Y CODIGOS REED-SOLOMON DEL LIBRO DE JUSTESEN-HØHOLDT

↳ CONCEPTO DE ELEMENTO PRIMITIVO DE UN CUERPO FINITO

EL ELEMENTO β ($\beta \mid \langle\beta\rangle = \mathbb{F}_q^*$) DE LA CLASE DE AYER

$$\mathbb{F}_{11} = \{0, 1, 2, \ldots, 10\}$$

$$\underbrace{[3] = \overline{3} = \{\ldots, -8, 3, 14, 25, \ldots\}}_{3}$$

$F = GF(11)$ ← CUERPO FINITO

GALOIS FIELD

CALCULAMOS EN SAGE LOS EJEMPLOS 4.1.1, 4.1.2 Y 4.2.1 DEL LIBRO JUSTESEN-HØHOLDT SOBRE CÓDIGOS REED-SOLOMON

4.1.1) CALCULAMOS MATRIZ GENERADORA. CODIFICACIÓN

4.1.2) CALCULAMOS MATRIZ DE CONTROL.

4.2.1) DECODIFICAMOS

IMPLEMENTAMOS LOS CÁLCULOS NOSOTROS Y TAMBIÉN PODEMOS EXPLORAR LAS FUNCIONES IMPLEMENTADAS PARA CÓDIGOS REED-SOLOMON EN SAGE

CALCULAMOS EN SAGE LOS EJEMPLOS 2.3.2 Y 2.3.3 SOBRE $\mathbb{F}_4$ Y $\mathbb{F}_{16}$

CALCULAMOS LAS TABLAS CON LAS DISTINTAS FORMAS DE REPRESENTAR UN CUERPO FINITO Y EXPLORAMOS CÓMO ESTÁN IMPLEMENTADOS LOS CUERPOS FINITOS EN SAGE.

EJERCICIOS DEL LIBRO JUSTESEN-HØHOLDT

PROBLEMAS:

2.6.1, 2.6.5 (CUERPOS FINITOS)

4.5.2, 4.5.3 (CÓDIGOS REED-SOLOMON)