

Ejercicio 1. (40%) Sea $C \subset \mathbb{F}_2^7$ el código lineal dado por la matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad G : K \times n$$

(a) ¿Cuál es la longitud y la dimensión de C ? $\underbrace{\mathbf{I}}_{\mathbf{P}}$

(b) Codifica el mensaje $(1, 0, 1, 0) \in \mathbb{F}_2^4$ usando el código C .

(c) Calcula una matriz de control del código C . \mathcal{M}

(d) ¿Cuál es la distancia mínima de C ?

a) Longitud: $n = 7$, Dimensión: $K = 4$

b) $\vec{a} = (1, 0, 1, 0)$

$$\begin{array}{ccc} \mathbb{F}_2^4 & \longrightarrow & \mathbb{F}_2^7 \\ \vec{a} & \longleftarrow & \vec{a} \cdot G \end{array}$$

$$(1, 0, 1, 0) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1, 0, 1, 0, 1, 0, 1) \approx$$

c) Matriz de control $[H] = [P^t : I_{n-k}] \rightarrow [H] = [-A^t, I_{m-k}]$

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad P^t = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$I_{n-k} = I_{7-4} = I_3$$

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

d) $d(C)$ (Sobre la matriz de control H)

1) ¿Es columna cs l.v.?

2) Las filas de 0 =>

Como todas las columnas son distintas

$$\Rightarrow d > 1$$

2) Si 2 columnas son l.i?

$$\lambda_1 \begin{bmatrix} \end{bmatrix} + \lambda_2 \begin{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \lambda_i \in \mathbb{F}_2, \quad \lambda_i = 0, 1$$

$$\begin{bmatrix} \end{bmatrix} + \begin{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad \begin{bmatrix} \end{bmatrix} = -\begin{bmatrix} \end{bmatrix} \quad \text{Como estamos en } \mathbb{F}_2 \Rightarrow$$

$$\begin{bmatrix} \end{bmatrix} = \begin{bmatrix} \end{bmatrix}; \quad \text{Como no hay 2 columnas que sean iguales} \Rightarrow d > 2$$

3) Si 3 columnas l.i?

Buscar una columna que sea la suma de las otras 2;

$$\text{Columna}(4) = \text{Columna}(3) + \text{Columna}(7)$$

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}; \quad \text{Por lo tanto} \Rightarrow$$
$$\Rightarrow d \leq 3$$

Finalmente, obtenemos que $\boxed{d \leq 3}$

Ejercicio 2. (40%) Sea C el código lineal binario dado por la matriz de control

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad n=6$$

y que tiene la siguiente tabla de síndromes y líderes:

Síndrome	Líder
(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)	-

- (a) A partir de la tabla de síndromes y líderes, deduce la capacidad correctora del código C .
- (b) Usando la tabla de síndromes y líderes, decodifica las siguientes palabras recibidas de \mathbb{F}_2^6 y menciona cuantos errores se han cometido.
- (0,0,0,1,1,1)
 - (1,0,0,1,0,0)
 - (1,0,0,1,1,1)

a) Como el síndrome es la columna correspondiente a la posición del error y cada líder presenta a (\rightarrow) sumo un único error, por lo tanto, se deduce que la

b) $S(\vec{r}_1) = H \cdot \vec{r}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

Líder = [1, 0, 0, 0, 0, 0]
 $\vec{e} = \vec{r}_1 - \text{líder} = [0, 0, 0, 1, 1, 1] - [1, 0, 0, 0, 0, 0] =$

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

Se ha cometido un error.

$$\bullet S(\vec{r}_2) = H \cdot \vec{r}_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

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

Como el síndrome no tiene

vector r no decodificamos \Rightarrow

\Rightarrow error.

$$\bullet S(\vec{r}_3) = H \cdot \vec{r}_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

$$= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}; L_{\text{der}} = (0, 0, 0, 0, 0)$$

$$\vec{c} = \vec{r}_3 - L_{\text{der}} = (1, 0, 0, 1, 1, 1) - (0, 0, 0, 0, 0) =$$

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

No se ha cometido ningún error.

Ejercicio 3. (20%) Sea C el código Reed-Solomon [10, 3, 8] sobre \mathbb{F}_{11} .

- (a) Calcula cuál es el mayor tamaño de lista que se podría usar para decodificar en lista el código C si se quiere mejorar la capacidad correctora única de C.
- (b) ¿Cuántos errores se pueden corregir si el tamaño de lista es $\ell = 2$?

Pág 11 del 06/10, hasta el valor de ℓ .

$$a) \frac{k}{n} < \frac{1}{\ell+1} + \frac{1}{n}; \quad [10, 3, 8]$$

$$\frac{3}{10} < \frac{1}{\ell+1} + \frac{1}{10}$$

$$\frac{3-1}{10} < \frac{1}{\ell+1} \Rightarrow \frac{2}{10} < \frac{1}{\ell+1}$$

$$2(\ell+1) < 10 \Rightarrow \ell+1 < 5$$

$$\boxed{\ell < 4} \Rightarrow \ell = 3$$

$$b) \tau < n \cdot \frac{\ell}{\ell+1} - \frac{\ell}{2}(k-1)$$

$$\tau < 10 \cdot \frac{2}{2+1} - \frac{2}{2}(3-1)$$

$$\tau < \frac{20}{3} - \frac{2}{2} = \frac{14}{3}$$

$$\tau < \frac{14}{3} - 2 = \frac{8}{3}$$

$$\tau < \frac{14}{3} ; \quad \boxed{\tau = 4}$$

Para $\ell=3$ tambien da 4, algo, por lo que no ganas nada, ya que $\boxed{\tau=4}$

Ejercicio 4. (extra 25%)

me vece la pena ir hasta

$\ell = \dots$ y lo

mejor es decir $\ell=2$
porque $\ell=3$ no mejora

(a) Encuentra un elemento primitivo de \mathbb{F}_7 .

(b) Considera \mathbb{F}_{16} dado por $\mathbb{F}_2[X]/(X^4 + X + 1)$. Y sea $\alpha = x$ un elemento primitivo de \mathbb{F}_{16} .

- Calcula $\alpha^{13} + \alpha^{14}$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α .
- Calcula $(X + X^2)(X^2 + X^3)$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α .

$$f: x^4 + x + 1$$

$$\mathbb{F}_{16}: \alpha = (\alpha_0, \dots, \alpha_{15})$$

0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1

4	0	1	0	0
5	0	1	0	1
F	0	1	1	1
1	0	1	1	1
2	1	0	0	1
9	1	1	0	1
10	1	1	1	1
11	1	1	1	1
12	1	1	0	1
13	1	1	0	0
14	1	1	1	1
15	1	1	1	0

$$13 = 1101$$

$$14 = 1110$$

$$13 = x^3 + x^2 + 1 = \alpha^{13}$$

$$14 = x^3 + x^2 + x = \alpha^{14}$$

$$1) \quad 1101$$

$$+ 1110$$

$$\hline 1011$$

$$= \alpha^{14}$$

$$x^3 + x^2 + 1$$

$$x^3 + x^2 + x$$

$$\left(\begin{array}{l} \vdots \\ - 2x^3 + 2x^2 + x + 1 \end{array} \right)$$

$$a) \text{ en } \mathbb{F}_7 - \{0\} = \mathbb{F}_7^* = \langle 2 \rangle =$$

$$= \{2^0, 2^1, 2^2, 2^3\}$$

$$\mathbb{F}_7 - \{0\} = \{\underbrace{\alpha^0}_{\alpha^{q^n}}, \underbrace{\alpha^1}_{\alpha^q}, \dots, \underbrace{\alpha^{q-2}}_{\alpha^f}\}$$

$$\mathbb{F}_7: \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 1$$

$$\alpha^{q-1} = 1 \quad \quad \quad \{ \alpha^{q+1}, \alpha^{q+2}, \dots, \alpha^{q+q-1} \}$$

$$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 9 = 2 \quad 3^3 = 27 = 6 \quad 3^4 = 81 = 4$$

$3^5 = 5$ Tenemos todos: 1, 2, 3, 4, 5 y 6.

$$\alpha^i \rightsquigarrow i \quad \quad \quad \alpha^{i+j} = \alpha^i \cdot \alpha^j$$

$$b) \mathbb{F}_2[x]/\langle x^4 - x + 1 \rangle = 16 \text{ elementos } 2^4$$

$$\left\{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_i \in \mathbb{F}_2 \right\}$$

$$\mathbb{F}_p[x]/\langle x^m + \dots \rangle = \mathbb{F}_{p^m}$$

$$\alpha = [x]$$

al ser \mathbb{F}_2 \oplus \ominus
es campo

$$\alpha^{13} + \alpha^{14} = x^{14} + x^{13}$$

$x^{14} + x^{11} + x^{10}$

x^{13}

TRUCO

$$x^4 + x + 1 \quad | \quad \overbrace{x^4 + x + 1}^{\oplus}$$

\ominus

$$x^4 = x + 1$$

$$x^8 = x^4 \cdot x^4 \cdot x^4 \cdot x^4 = (x+1) \cdot (x+1) \cdot (x+1) \cdot x^2$$

$$\begin{aligned}
 &= x^2 + 1 \quad (x+1) \cdot x^2 = (x^4 + x^2)(x+1) = \\
 &= (x+1+x^2)(x+1) = \cancel{x^2} + \cancel{x} + x^3 + \cancel{x} + \cancel{4x} = \\
 &\quad x^3 + 1 //
 \end{aligned}$$

$$\begin{aligned}
 x^{13} &= x^4 \cdot x^4 \cdot x^4 \cdot x \\
 &= (x^2 + 1) \cdot (x+1) \cdot x = \\
 &= (x^2 + 1) \cdot (x^2 + x) = \\
 &= x^4 + x^3 + x^2 + x = \\
 &= (\cancel{x+1}) + x^3 + x^2 + \cancel{x} \\
 &= x^3 + x^2 + 1
 \end{aligned}$$

Ejemplo en $\mathbb{F}_3[x]$

$$\begin{aligned}
 F_3 &= \mathbb{F}_3[x] / \langle x^2 + x + 2 \rangle \\
 x^2 + x + 2 &= 0 \\
 x^2 &= -(x+2) \\
 &= -x - 2 = -x + 1
 \end{aligned}$$

$$\begin{aligned}
 x^{13} + x^{14} &= \cancel{x^3} + x^2 + \cancel{x} + 1 + \cancel{x^3} - x^2 \\
 &= (0, 0, 1, 0)
 \end{aligned}$$

$$\begin{array}{l} \left. \begin{array}{l} x^1 \cdot x^{15} \\ - x^{13+14} \end{array} \right\} = x^{22 \text{ mod } 15} = x^{12} \quad \text{FACTIL} \\ b_2 \} \\ (x+x^2)(x^2+x^3) \end{array}$$

$$\begin{array}{l} x^3 + \cancel{x^4} + \cancel{x^5} + x^5 = \\ = x^3 + x \cdot (x+1) \end{array}$$

$$-x^3 + x^2 + x = (0, 1, 1, 1)$$

$$x^4 \left(\cancel{x^4} + x^6 + x \right)$$

$$\alpha = x \quad \alpha^2 = x^2 \quad \alpha^3 = x^3 \quad \alpha^4 = x^4 + x^2 \quad \alpha^5 = x^5 + x^3 + x^2 + x + 1$$

$$\alpha^6 = x^6 \quad \alpha^7 = x^7 + x^5 \quad \alpha^8 = x^8 + x^6 + x^4 + x^2 + x + 1$$

$$\alpha^9 = x^9 + x^7 + x^5 + x^3 + x = x^2 + x$$

Viendo la tabla

$$x^{13} + x^{15} \left(\cancel{x^3 + x^2 + x} + (x^3 + x) \right) = x^2$$

y el β es ver que es $= \alpha^5 \cdot \alpha^6 = x^3 + x^2 + x$