

Notas para práctico 2

1. Elementos del cuerpo como potencias de α

i	α^i
0	1
1	α
2	α^2
3	$\alpha + 1$
4	$\alpha^2 + \alpha$
5	$\alpha^2 + \alpha + 1$
6	$\alpha^2 + 1$

2. Matriz de chequeo de paridad

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} & \alpha^{24} \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix}$$

3. Palabra recibida

$$\begin{aligned} \mathbf{y} &= \alpha + (\alpha^2 + \alpha + 1)x + \alpha^2 x^2 + (\alpha^2 + \alpha)x^3 + \alpha^2 x^4 + (\alpha^2 + 1)x^5 \\ &= \alpha + \alpha^5 x + \alpha^2 x^2 + \alpha^4 x^3 + \alpha^2 x^4 + \alpha^6 x^5 \end{aligned}$$

4. Inicialización para algoritmo de Euclides

- $a(x) = x^4$ $b(x) = (\alpha + 1) + \alpha x + (\alpha^2 + \alpha + 1)x^2$.
- $r_{-1} = x^4$, $r_0(x) = (\alpha + 1) + \alpha x + (\alpha^2 + \alpha + 1)x^2$.
- $s_{-1} = 1$, $s_0 = 0$.
- $t_{-1} = 0$, $t_0 = 1$.