Teoría de Códigos
Tarea 1

Rubí Rojas Tania Michelle

3 de abril de 2020

1. Construye el campo $\mathbb{F}_{16}$. También da sus tablas de suma y multiplicación.

   Solución: En el anillo $\mathbb{Z}_2$ existe el polinomio irreducible $f(x) = x^4 + x + 1$. Tenemos que

$$\mathbb{F}_{16} = \mathbb{Z}_2[x]/(x^4 + x + 1) \tag{1}$$

donde los elementos de $\mathbb{F}_{16}$ son:

$$\begin{aligned} \mathbb{F}_{16} &= \{ax^3 + bx^2 + cx + d \ : \ a, b, c, d \in \mathbb{Z}_2\} \\ &= \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1, x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, \\ &\quad x^3 + x^2 + x, x^3 + x^2 + 1, x^3 + x^2 + x + 1\} \end{aligned}$$

Etiquetamos cada uno de los elementos de $\mathbb{F}_{16}$ de la siguiente manera:

- $g_0(x) = 0$
- $g_1(x) = 1$
- $g_2(x) = x$
- $g_3(x) = x + 1$
- $g_4(x) = x^2$
- $g_5(x) = x^2 + 1$
- $g_6(x) = x^2 + x$
- $g_7(x) = x^2 + x + 1$
- $g_8(x) = x^3$
- $g_9(x) = x^3 + 1$
- $g_{10}(x) = x^3 + x$
- $g_{11}(x) = x^3 + x + 1$
- $g_{12}(x) = x^3 + x^2$
- $g_{13}(x) = x^3 + x^2 + x$
- $g_{14}(x) = x^3 + x^2 + 1$
- $g_{15}(x) = x^3 + x^2 + x + 1$

Su respectiva tabla de suma es:

$+$	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_0	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_1	g_1	g_0	g_3	g_2	g_5	g_4	g_7	g_6	g_9	g_8	g_{11}	g_{10}	g_{14}	g_{15}	g_{12}	g_{13}
g_2	g_2	g_3	g_0	g_1	g_6	g_7	g_4	g_5	g_{10}	g_{11}	g_8	g_9	g_{13}	g_{12}	g_{15}	g_{14}
g_3	g_3	g_2	g_1	g_0	g_7	g_6	g_5	g_4	g_{11}	g_{10}	g_9	g_8	g_{15}	g_{14}	g_{13}	g_{12}
g_4	g_4	g_5	g_6	g_7	g_0	g_1	g_2	g_3	g_{12}	g_{14}	g_{13}	g_{15}	g_8	g_{10}	g_9	g_{11}
g_5	g_5	g_4	g_7	g_6	g_1	g_0	g_3	g_2	g_{14}	g_{12}	g_{15}	g_{13}	g_9	g_{11}	g_8	g_{10}
g_6	g_6	g_7	g_4	g_5	g_2	g_3	g_0	g_1	g_{13}	g_{15}	g_{12}	g_{14}	g_{10}	g_8	g_{11}	g_9
g_7	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_0	g_{15}	g_{13}	g_{14}	g_{12}	g_{11}	g_9	g_{10}	g_8
g_8	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{14}	g_{13}	g_{15}	g_0	g_1	g_2	g_3	g_4	g_6	g_5	g_7
g_9	g_9	g_8	g_{11}	g_{10}	g_{14}	g_{12}	g_{15}	g_{13}	g_1	g_0	g_3	g_2	g_5	g_7	g_4	g_6
g_{10}	g_{10}	g_{11}	g_8	g_9	g_{13}	g_{15}	g_{12}	g_{14}	g_2	g_3	g_0	g_1	g_6	g_4	g_7	g_5
g_{11}	g_{11}	g_{10}	g_9	g_8	g_{15}	g_{13}	g_{14}	g_{12}	g_3	g_2	g_1	g_0	g_7	g_5	g_6	g_4
g_{12}	g_{12}	g_{14}	g_{13}	g_{15}	g_8	g_9	g_{10}	g_{11}	g_4	g_5	g_6	g_7	g_0	g_2	g_1	g_3
g_{13}	g_{13}	g_{15}	g_{12}	g_{14}	g_{10}	g_{11}	g_8	g_9	g_6	g_7	g_4	g_5	g_2	g_0	g_3	g_1
g_{14}	g_{14}	g_{12}	g_{15}	g_{13}	g_9	g_8	g_{11}	g_{10}	g_5	g_4	g_7	g_6	g_1	g_3	g_0	g_2
g_{15}	g_{15}	g_{13}	g_{14}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_1	g_2	g_0

mientras que su tabla de multiplicación es:

$\cdot$	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0
g_1	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_2	g_0	g_2	g_4	g_6	g_8	g_{10}	g_{12}	g_{13}	g_3	g_1	g_7	g_5	g_{11}	g_{15}	g_9	g_{14}
g_3	g_0	g_3	g_6	g_5	g_{12}	g_{15}	g_{10}	g_9	g_{11}	g_8	g_{14}	g_{13}	g_7	g_1	g_4	g_2
g_4	g_0	g_4	g_8	g_{12}	g_3	g_7	g_{11}	g_{15}	g_6	g_2	g_{13}	g_{10}	g_5	g_{14}	g_1	g_9
g_5	g_0	g_5	g_{10}	g_{15}	g_7	g_2	g_{14}	g_8	g_{13}	g_{11}	g_4	g_1	g_9	g_3	g_{12}	g_6
g_6	g_0	g_6	g_{12}	g_{10}	g_{11}	g_{14}	g_7	g_1	g_5	g_3	g_9	g_{15}	g_{13}	g_2	g_8	g_4
g_7	g_0	g_7	g_{13}	g_9	g_{15}	g_8	g_1	g_6	g_{14}	g_{10}	g_3	g_4	g_2	g_{12}	g_5	g_{11}
g_8	g_0	g_8	g_3	g_{11}	g_6	g_{13}	g_5	g_{14}	g_{12}	g_4	g_{15}	g_7	g_{10}	g_9	g_2	g_1
g_9	g_0	g_9	g_1	g_8	g_2	g_{11}	g_3	g_{10}	g_4	g_{14}	g_5	g_{12}	g_6	g_7	g_{15}	g_{13}
g_{10}	g_0	g_{10}	g_7	g_{14}	g_{13}	g_4	g_9	g_3	g_{15}	g_5	g_8	g_2	g_1	g_6	g_{11}	g_{12}
g_{11}	g_0	g_{11}	g_5	g_{13}	g_{10}	g_1	g_{15}	g_4	g_7	g_{12}	g_2	g_9	g_{14}	g_8	g_6	g_3
g_{12}	g_0	g_{12}	g_{11}	g_7	g_5	g_9	g_{13}	g_2	g_{10}	g_6	g_1	g_{14}	g_{15}	g_4	g_3	g_8
g_{13}	g_0	g_{13}	g_{15}	g_1	g_{14}	g_3	g_2	g_{12}	g_9	g_7	g_6	g_8	g_4	g_{11}	g_{10}	g_5
g_{14}	g_0	g_{14}	g_9	g_4	g_1	g_{12}	g_8	g_5	g_2	g_{15}	g_{11}	g_6	g_3	g_{10}	g_{13}	g_7
g_{15}	g_0	g_{15}	g_{14}	g_2	g_9	g_6	g_4	g_{11}	g_1	g_{13}	g_{12}	g_3	g_8	g_5	g_7	g_{10}

2. Construye una matriz generadora para el código $RS(4, 11)$.

   SOLUCIÓN: Una matriz generadora para $RS(4, 11)$ es

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

3. Supón que recibes la palabra $y = (10, 1, 2, 2, 2, 10, 7, 2, 9, 3, 7) \in \mathbb{F}_{11}^{11}$. Decodifica la palabra usando el algoritmo de Gao, sabiendo que la palabra es del código $RS(4, 11)$.

4. Construye una base para $\mathcal{L}_k$ de tal manera que la matriz generadora del código $RS(k, q)$ sea de la forma

$$\begin{bmatrix} I_k & P \end{bmatrix} \tag{2}$$

   donde I_k es la matriz identidad $k \times k$ y P es una matriz $k \times (q - k)$.

5. Demuestra que el número de subespacios vectoriales de $\mathbb{F}_q^n$ de dimensión i es:

$$\mathcal{G}(n, i) = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{i-1})}{(q^i - 1)(q^i - q) \cdots (q^i - q^{i-1})} \tag{3}$$

   para $i = 1, .., n$.

6. Demuestra que $RS(k, q)_q^{\top} = RS(q - k, q)$.

   Demostración. $\square$

7. Demuestra que si C es un código MDS, entonces $C^{\top}$ también es MDS.

   Demostración. Supongamos que C es un código MDS. $\square$

8. Resuelve los siguientes ejercicios

a) Encuentra la matriz generadora G del código Simplex $S(3,2)$.

SOLUCIÓN: Sabemos que el código $S(3,2)$ tiene

$$\begin{aligned}\frac{q^k-1}{q-1} &= \frac{2^3-1}{2-1} \\ &= \frac{8-1}{1} \\ &= 7\end{aligned}$$

subespacios de dimensión 1. Por lo tanto,

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

b) Supongamos que un mensaje es enviado bajo el código $H(3,2)$. Verifica si el mensaje $r = 1010001$ es correcto.

SOLUCIÓN: Sabemos que $H(3,2) = [7,4,3]_2$ y que una matriz de verificación para $H(3,2)$ es cualquier matriz generadora para $S(3,2)$. Así, la matriz obtenida en el inciso anterior es una matriz de verificación para nuestro código $H(3,2)$.

El mensaje r se puede ver como un vector

$$x = (1,0,1,0,0,0,1) \in \mathbb{F}_2^7$$

Ahora, calculamos el síndrome de x.

$$\begin{aligned} S(y) &= G \cdot x^t \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \end{aligned}$$

Como $S(y) = (0,1,0)^t \neq 0$ entonces podemos concluir que hubo errores de transmisión. Notemos que $(0,1,0)^t$ corresponde a la segunda columna de G, por lo que sabemos que la segunda coordenada es incorrecta. Por lo tanto, la palabra envíada fue

$$r' = (1,1,1,0,0,0,1)$$