

Facultad de Ciencias, UNAM
Teoría de Códigos
Tarea 1

Rubí Rojas Tania Michelle

6 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

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

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:

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

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:

·	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 $RS(4, 11)$.

SOLUCIÓN: Aplicamos el algoritmo de Gao

- i) Sea $p_0(x) = x^{11} - x$ y $p_1(x) = 10 + x + 2x^2 + 2x^3 + 2x^4 + 10x^5 + 7x^6 + 2x^7 + 9x^8 + 3x^9 + 7x^{10}$
 ii) Aplicamos el algoritmo extendido de euclides a p_0 y a p_1 deteniéndonos cuando el grado del residuo $p_m(x)$ es menor que $\frac{q+k}{2} = \frac{11+4}{2} = 7$.
4. Construye una base para \mathcal{L}_k de tal manera que la matriz generadora del código $RS(k, q)$ sea de la forma

$$\begin{bmatrix} I_k & P \end{bmatrix} \quad (2)$$

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:

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

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

Demostración. Sabemos que un subespacio de dimensión k se especifica dando k vectores linealmente independientes $\{v_1, v_2, \dots, v_k\} \in V = \mathbb{F}_q^n$. El vector v_1 puede ser elegido como cualquier vector distinto de cero en V , por lo que hay $q^n - 1$ opciones para v_1 . Dado v_1, v_2 se puede elegir como cualquier vector que no se encuentre en el subespacio generado por v_1 . Como este subespacio tiene q elementos, entonces hay $q^n - q$ opciones para v_2 . Siguiendo de esta manera, tenemos que dados v_1, v_2, \dots, v_i con $i < k$, entonces hay $q^n - q^i$ opciones para v_{i+1} . Así, el número de conjuntos de k vectores linealmente independientes en V es

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}) \quad (4)$$

Como hay muchos conjuntos k linealmente independientes que generan el mismo subespacio, entonces debemos dividir la expresión anterior entre el número de k conjuntos que generan el mismo subespacio (i.e. el número de bases para un subespacio de dimensión k).

Así, aplicando la expresión (4) al caso especial en que $n = k$, tenemos que cada subespacio de dimensión k de V tiene

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}) \quad (5)$$

bases. Por lo tanto, el número de subespacios de dimensión k de V es

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

□

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

Demostración. Notemos que tanto $RS(k, q)$ como $RS(q - k, q)$ tienen dimensiones complementarias, así que es suficiente mostrar que son ortogonales.

Tenemos que el código $RS(k, q)$ es generado por X^i , con $i < k$; y el código $RS(q - k, q)$ es generado por X^j , con $j < q - k$. El producto punto correspondiente a las palabras de código es $S = \sum_u u^{i+j}$. Sea $m = i + j$. Notemos que $m \leq q - 2$. Hay algunos $0 \neq c \in \mathbb{F}_q$ tales que $c^m \neq 1$, ya que el polinomio $X^m - 1$ de grado m debería de tener $q - 1 > m$ raíces, lo cual es imposible.

Como $c^m S = S$, entonces cu

□

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

Demostración. Supongamos que C es un código MDS con una matriz generadora G con columnas c_i , donde $i \in \{1, 2, \dots, n\}$. Entonces G es una matriz de $k \times n$, y por hipótesis tenemos que cada combinación lineal de los renglones tiene un peso de Hamming de al menos $n - k + 1$. Por una proposición vista en clase, sabemos que C^\top tiene una matriz de verificación de paridad G^T . Como $C = [n, k, n - k + 1]$, entonces debemos mostrar que la distancia mínima de C^\top es igual a $n - (n - k) + 1 = k + 1$, es decir, $C^\top = [n, n - k + 1, k + 1]$ (esto significa que cada subconjunto de k columnas de la matriz generadora G es linealmente independiente).

Procedemos por contradicción. Supongamos que algunas k columnas de G son linealmente dependientes. Sea H la submatriz de $k \times k$ formada por estas columnas. Como las columnas son linealmente dependientes, entonces el rango de H es menor que k debido a que los renglones de H tienen alguna dependencia lineal. Por lo tanto, existe una combinación lineal de los renglones de H que suma 0, por lo que podemos usar esta misma combinación lineal en los renglones de G cuya suma tiene al menos k ceros, lo cual implicaría que tiene un peso de Hamming $\leq n - k$. Pero como cualquier combinación lineal de los renglones de G en un código MDS debe tener un peso de Hamming al menos $n - k + 1$, entonces tenemos una contradicción.

Por lo tanto, C^\top es un código MDS .

□

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 .

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

Como $S(x) = (0, 1, 0)^t \neq 0$ 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. Entonces el vector error es

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

Por lo tanto, la palabra enviada fue

$$\begin{aligned}
 z &= x - e \\
 &= (1, 0, 1, 0, 0, 0, 1) - (0, 1, 0, 0, 0, 0, 0) \\
 &= (1, 1, 1, 0, 0, 0, 1)
 \end{aligned}$$