Parcial Álgebra Abstracta y Codificación

Oscar Andrés Gómez Hernández

Noviembre 2020

Este parcial fue desarrollado en compañía de Rodrigo Castillo y Carlos Muños

1. Primer Punto.

Sea C el código lineal de longitud 9, cuya matriz de control es

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

a) Encuentre la dimensión de C.

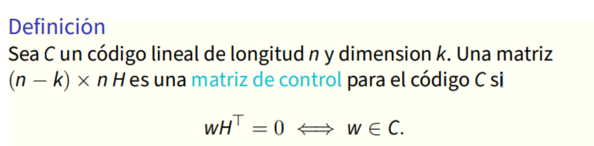

Figura 1: Tomada de: Clase 26 - Diapositiva 3

Sabemos que C tiene longitud 9 y que H es una matriz 4x9 entonces teniendo en cuenta la definición, $n-k=4$, $9-k=4$ y $5=k$ por lo que la dimensión de C es 5.

b) Encuentre la distancia mínima de C.

Encontramos la matriz generadora de C, sabiendo que G=(I_k A) y que H= $(-A^T\ I_{n-k})$, entonces podemos deducir que

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{2}$$

Luego teniendo en cuenta a G, podemos hacer a mano la inspección de la distancia entre cada una de las filas de G, dándonos cuenta que la distancia mínima de esta es 3.

c) Calcule los síndromes correspondientes a errores que C puede corregir.

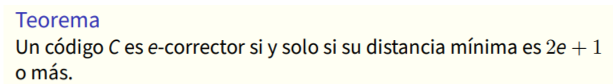

Figura 2: Tomada de: Clase 24 - Diapositiva 8

Teniendo en cuenta el teorema, vemos que el código Ces 1-corrector porque su distancia mínima es 3, entonces 2e+1=3, 2(1)+1=3
Ahora como el código es 1-corrector tenemos dos casos a la hora de calcular los síndromes de C:
*Si el síndrome es igual a 0, esto nos dice que no hay error en la palabra.
*Si el síndrome no es igual a 0 se dará una representación de un número binario que al pasarlo a decimal nos dirá la posición en la que se encuentra el error en la palabra.

d) Diga si 000110011 $\in$ C o no
Hallamos la matriz de H^T

$$H^T = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3}$$

Para saber si la palabra pertenece a C, la multiplicaremos por H^T si el resultado es 0000 significa que la palabra pertenece al código, de otra manera la palabra no pertenece a C.
$(000110011)H^T = 1100$, por lo que la palabra $\notin$ C.

e) Decodifique 110101101
Tomemos el la palabra dada y multipliquémosla por H^T para hallar su respectivo síndrome. $(110101101)H^T = 0111$ por lo que podemos ver que esto es la transpuesta de la tercera columna de H, por lo que el error es 001000000, ahora usando la definición de $w = c + r$, despejamos para poder hallar c, por lo que tenemos $c = 110101101 - 001000000$, entonces $c = 1111011011$.

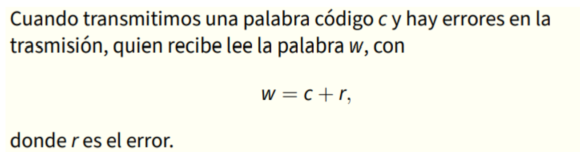

Figura 3: Tomado de: Clase 26 - Diapositiva 2

2. Segundo Punto.

Sea $g(x)$ el generador de un código cíclico de longitud 15 sobre $\mathbb{Z}_2$. Demuestre que $g(1) = 0$ si y solo si todas las palabras del código tienen un peso par.

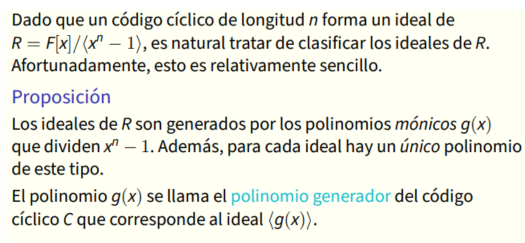

Figura 4: Tomado de: Clase 27 - Diapositiva 7

$\Rightarrow$ Sea $g(x)$ el polinomio generado, por la proposición sabemos que $g(x)$ es mónico y corresponde al ideal de $\langle g(x)\rangle$, entonces es un ideal de $R = \mathbb{Z}_2/\langle X^{15} - 1\rangle$, luego el polinomio quedaría $g(x) = c_0 + c_1X + c_2X^2 + ... + c_{14}X^{14}$, luego $g(1) = 0$, lo que nos da:
$g(1) = c_0 + c_1X + c_2X^2 + ... + c_{14}X^{14} = 0$
$g(1) = c_0 + c_1 + c_2 + ... + c_{14} = 0$, luego como $c_i \in \mathbb{Z}_2$ y además note que $c_i \in C$, así vemos que C tiene peso par.

$\Leftarrow$ Esta parte de la demostración es análoga a la anterior.

3. Tercer Punto.

Sea $F = \{0, 1, \omega, \bar{\omega}\}$ el campo finito con 4 elementos. Las operaciones en F siguen de estas reglas:

$$1 + 1 = 0, \qquad 1 + \omega = \omega^2 = \bar{\omega}$$

a) Escriba las tablas de operaciones en F.

$+$	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$
1	1	0	$\bar{\omega}$	ω
ω	ω	$\bar{\omega}$	0	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0

$.$	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	0	$\bar{\omega}$	1	ω

b) Sea C el código lineal sobre F cuya matriz generadora es la siguiente:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & \bar{\omega} & \omega \end{pmatrix} \tag{4}$$

Encuentre el peso mínimo de C y una matriz de control para C

Notemos que el peso mínimo de G es 4 hallando la distancia mínima entre las filas, luego como C es un código lineal el peso mínimo de C también es 4.

Sabemos que G=(I_k A) y que la matriz de control es igual a H = $(-A^T\ I_{n-k})$ entonces al hacer $-A^T$ nos da

$$\begin{pmatrix} -1 & -1 & -1 \\ -1 & -\omega & -\bar{\omega} \\ -1 & -\bar{\omega} & -\omega \end{pmatrix} \tag{5}$$

Ahora por la tabla de operación de la suma podemos deducir que 1 = -1, $\omega = -\omega$ y $\bar{\omega} = -\bar{\omega}$, por lo que la matriz de control seria:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \omega & \bar{\omega} & 0 & 1 & 0 \\ 1 & \bar{\omega} & \omega & 0 & 0 & 1 \end{pmatrix} \tag{6}$$

c) Demuestre que ningún código (no necesariamente lineal) sobre un alfabeto de 4 símbolos con la misma longitud y distancia mínima de C puede tener más palabras códigos que C.

La cantidad de palabras que C tiene es 64 palabras, luego por la cota del singulete tenemos que $\mid C \mid \leq q^{n-d+1}$, por lo que $\mid C \mid \leq 4^{6-4+1} = 64$ por lo tanto ningún código tiene mas palabras códigos que C.

4. Cuarto punto.

Sea H una matriz de control para el código lineal C sobre $\mathbb{Z}_2$ de longitud n y dimensión k. Construimos un nuevo código C' de longitud $n+1$ en la siguiente manera. Si $c_0c_1...c_{n-1} \in C$ entonces $c_0c_1...c_{n-1}c_n \in C'$

con

$$c_n = c_0 + c_1 + ... + c_{n-1}$$

Encuentre la dimensión, distancia mínima y matriz de control de C' en función de los mismos para C

Como a C' se le añade un símbolo a la longitud, más no se le añaden palabras, note que la dimensión de C y C' es la misma, por lo tanto la dimensión de C' es k.

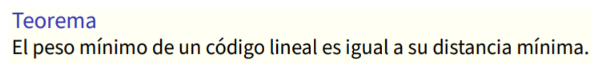

Figura 5: Tomado de: Clase 25 - Diapositiva 5

Para hallar la distancia mínima de C' usaremos el teorema, entonces tenemos dos casos:
*Caso 1: Peso de C es par, como C tiene una cantidad par de 1's y c_n es la suma del código añadimos un 0, dándonos cuenta de que esto no afecta el peso de C' por lo que si el peso de C es par, la distancia mínima de C' es igual a la de C.
*Caso 2: Peso de C es impar, en este caso sumamos una cantidad impar de 1's por lo que añadiremos un 1 a la suma de c_n, por lo que la distancia mínima de C' cuando C es impar, es la distancia mínima de $C + 1$.

Ahora buscaremos una matriz de control para C' Sabemos que $(C_0..C_{n-1})H^T = 0$, luego $C_0..C_n \in C'$ y $c_n = c_0 + c_1 + ... + c_{n-1}$, luego tenemos que $C'H'^T$ también debe ser igual a cero, por lo que debemos buscar que agregarle a la matriz H para poder cumplir con la igualdad, entonces tomamos H^T y le agregamos una columna de 1's al final y una fila de 0's al final hasta la posición $nXn-1$, de tal manera que entrada nXn sea un 1 también, al momento de hacer la transpuesta de esta nueva matriz generaremos a H', en la cual las primeras filas y columnas serán iguales a las de H y la ultima columna serán 0's hasta la posición $n-1Xn$ y la ultima fila serán 1's, teniendo así también en la posición nXn un 1.

Todos las capturas puestas en el parcial fueron tomadas de las diapositivas del curso.

Referencias

[CAM08] Peter J. Cameron. *Introduction to Algebra.*. Oxford University Press, Oxford, second edition 2008.