Parcial 3 de algebra abstracta

Rodrigo Castillo (junto a Carlos y Oscar)

19 de noviembre de 2020

1. Sea c el código lineal de longitud 9 cuya matriz de control es:

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

Figura 1: matriz de control

1.1. a : encuentre la dimensión de C

sabemos que si C es un código lineal de longitud n y dimensión k , una matrix $n-k \times nH$ es una matriz de control para el código C si $wH^T \iff w \in C$
sabemos que C tiene longitud 9
H es una matriz 4×9
por lo tanto $n - k = 4$
$9 - k = 4$
$k = 5$
por lo tanto $dim(C) = 5$

1.2. encuentre la distancia mínima de C

para este punto necesitamos la matris generadora de C , tenemos que $G = (I_k A)$ y que $H = (-A^T I_{n-k})$ luego ...

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

con G podemos ver que la distancia mínima es 3

1.3. calcule los sindromes correspondientes a errores de C que puede corregir

sabemos que un código es $e-corrector$ **si su distancia mínima es** $2e+1$ **como mínimo** por lo tanto, como la distancia mínima de C es 3 , entonces es $1corrector$ (pues $1+1+1=3$)
como el código es $1-corrector$ se tiene que:
si el síndrome es igual a 0 , no hay error en la palabra
si el sindrome $\neq$ 0 , se tiene que la representación será un número binario que representa la posición del error

1.4. diga si $000110011 \in C$ o no

lo primero que hicimos fue calcular la matrix H^T

$$H^T = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2}$$

multiplicaremos la palabra por H^T , si el resultado es 0000 **significa que la palabra pertenece a** C
$000110011 \cdot H^T = 1100$ **luego tenemos que** $000110011 \notin C$

1.5. decodifique 110101101

sea la palabra 110101101 , la multiplicaremos por H^T
$110101101 \cdot H^T = 0111$, luego el error es 001000000 , ahora , usando $\omega = c + r$ se tiene que $c = 1111011011$

2. Punto 2

2.1. sea $g(x)$el generador de un codigo ciclico de longitud 15 sobre Z_2 demuestre que $g(1) = 1 \iff$ todas las palabras del código tienen un peso par

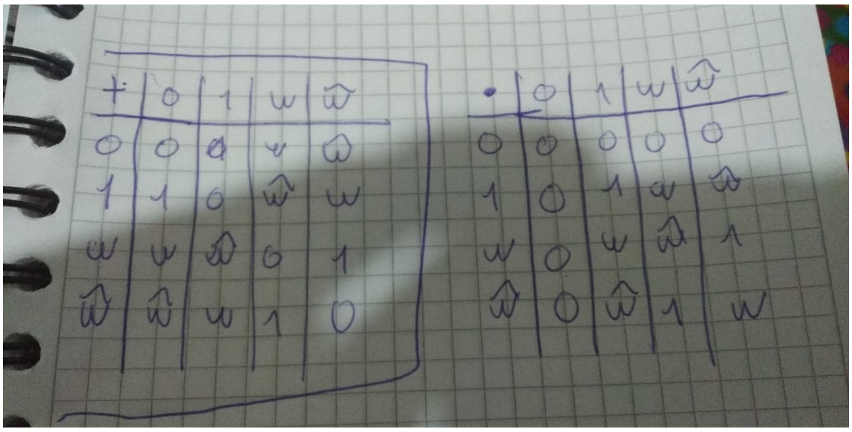
sea $g(x)$ un generador de un código cíclico de longitud 15 sobre Z_2
se tiene entonces que $g(x)$ corresponde al ideal de $\langle g(x) \rangle$, luego es un ideal de $Z_2/\langle X^{15}-1 \rangle$, por lo que
$g(x) = c_0 + c_1X + x_2X^2 + ... + c_{14}X^{14}$
$g(1) = 0$
$g(1) = c_0 + c_1X + c_2X^2 + ... + c_{14}X^{14} = 0$
$g(1) = c_0 + c_1 + c_2 + ... + c_{14} = 0$
como $c_i \in Z_2$ y además $c_i \in C$ entonces C tiene peso par
la demostración de la otra parte de la equivalencia es análoga

3. Punto 3

3.1. sea $\mathbf{F} = \{0, 1, \omega, \hat{\omega}\}$ el campo finito con 4 elementos , las operaciones en F siguen de estas reglas...

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

3.1.1. escriba las tablas de operaciones en F



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

$\cdot$	0	1	ω	$\hat{\omega}$
0	0	0	0	0
1	0	1	ω	$\hat{\omega}$
ω	0	ω	$\hat{\omega}$	1
$\hat{\omega}$	0	$\hat{\omega}$	1	ω

Figura 2: tablas de operaciones

nota: por alguna razón latex no me dejaba importar la libería para hacer una tabla

3.1.2. encuentre el peso minimo de C y una matriz de control para C

el peso mínimo de G es 4

, esto lo sabemos por la distancia mínima entre las filas
como C es lineal, el peso mínimo de de C es igual al peso mínimo de GJ que también es 4
$G = (I_k A)$, $H = -A^T I_{n-k}$, entonces al hacer $-A^T$ nos da la matriz ...

$$\begin{pmatrix} -1 & -1 & -1 \\ -1 & -\omega & -\hat{\omega} \\ -1 & -\hat{\omega} & -\omega \end{pmatrix} \tag{3}$$

haciendo uso de la tabla de operacion de la suma podemos saber que $1 = -1, \omega = -\omega$, podemos decir que matriz de control H es :

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \omega & \hat{\omega} & 0 & 1 & 0 \\ 1 & om\hat{e}ga & \omega & 0 & 0 & 1 \end{pmatrix} \tag{4}$$

3.1.3. demuestre que ningun codigo sobre un alfabeto de 4 simbolos con la misma longitud y distancia mínima de C puede tener mas palabras códigos que C

C tiene 64 palabras, luego
sabemos que C cumple la cota del singulete , luego $|C| <= 4^3$ luego $C <= 64$ luego no hay un código que sea tenga mas palabras códigos que C(pues C tiene 64 palabras)

4. PUNTO 4

sea H una matriz de control para el código lineal C sobre Z_2 de longitud n y dimension 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 minima y matriz de control de C' en función de los mismos para C
como C' es C mas la añadidura de un simbolo a la longitud sabemos que la dimensión de C es k
Sabemos por teorema dado en clase que **el peso minimo de un codigo lineal es su distancia minima** , por lo que en el caso de este ejercicio se tiene que ...
si el peso de C es par , como C tiene una cantidad par de $1'syc_n$ es la suma del código añadimos un 0. dandonos cuenta de que esto no afecta el peso de C' por que si el peso de C es par, la distancia minima de C' será igual a la de C
si el peso de C es impar en , sumamos una cantidad impar de $1's$, entonces añadiremos un 1 a la suma de c_n , por lo que la distancia minima de C' cuando C es impar , la distancia mínima es $C + 1$
Matriz de control :
Sabemos que $(C_0...C_{n-1}H^T = 0)$, por lo tanto $C_0...C_n \in C'$, además , $c_n = c_0+c_1+...+c_{n-1}$ tenemos que $C'H'^T$ debe ser igual a 0 , por lo que debemos lograr que al agregarle la matriz H siga cumpliendo la igualdad.
para esto tomaremos H^T y le agregaremos una columna de $1's$ al final
luego una fila de $0's$ al final hasta la posición $nXn - 1$ de manera que la entrada nXn sea un 1 también
al momento de hacer la transpuesta de esta nueva matriz generaremos a H' , matriz en la cuál las primeras filas y columnas serán iguales a las de H y a la ultima columna serán $0's$ hasta la posición $n - 1Xn$ y la ultima fila será $0s$ teniendo así en la posición nXn un 1 . De esta manera generaremos una matriz H que al multiplicarla con la matriz descrita arriba, obtendremos 0 y por lo tanto esta matriz será una matriz de control para el código C