Universidad Nacional de Colombia
Facultad de Ciencias
Teoria de Codificación

Edgar Santiago Ochoa Quiroga
María Alejandra Rodríguez Ríos ....

Ejercicio 1
Considere un canal simétrico cuya matriz de distribución de probabilidad tiene como fila permutaciones de la distribución de probabilidad $\{q_1, \ldots, q_n\}$. Pruebe que la capacidad del canal es:

$$\log(n) - H(q_1, \ldots, q_n)$$

Ayuda: Pruebe primero que

$$I(X;Y) \leq \log(n) - H(X|Y)$$

y observe bajo qué condiciones se da la igualdad.
Ejercicio 2
Construya una matriz generadora para un código lineal binario que transforma los mensajes (columna izquierda) escritos en binario en los códigos (columna derecha) mostrados en la siguiente tabla:

z	zG
0	0000000
1	0001110
2	0010101
3	0011011
4	0100011
5	0101101
6	0110110
7	0111000
8	1000111
9	1001001
10	1010010
11	1011100
12	1100100
13	1101010
14	1110001
15	1111111

A) Clasifique el código de acuerdo a la notación $[n, m, d]$.

B) Determine si el mensaje $z = 1011111$ trae errores, en tal caso calcule el síndrome, la coclase y corrija siempre y cuando sea posible.

C) ¿Cuántos errores puede detectar el código? Justifique.

D) ¿Cuántos errores puede corregir el código? Justifique.

Ejercicio 3
Sea C un código lineal $[n, m, d]$ sobre un cuerpo finito $GF(D)$. El código dual de C es el conjunto

$$C^{\perp} = \{x \in GF(D)^n : \langle x, y\rangle = 0, \forall y \in C\}.$$

Demuestre que $C^{\perp}$ es un código lineal de dimensión $n - m$ y que su matriz generadora corresponde a la matriz de verificación de C.

Demostración. Primero tenemos que probar que el código dual es lineal, para esto basta probar que es un subespacio de $GF(D)^n$.
Primero probemos que es cerrado bajo la suma. Sean $x_1, x_2 \in C^{\perp}$, por definición $\langle x_1, y\rangle = 0$ y $\langle x_2, y\rangle = 0$, para cualquier $y \in C$, luego como el producto interno es lineal en cada componente, tenemos que $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle = 0$, así $x_1 + x_2 \in C^{\perp}$. Ahora falta probar que la multiplicación por escalares también es cerrada. Tomemos $\lambda \in GF(D)$, luego si tomamos x_1 igual que en la anterior parte, nuevamente como el producto interno es lineal tenemos que $\langle \lambda x_1, y\rangle = \lambda\langle x_1, y\rangle = 0$. Así como es cerrado para ambas propiedades hemos probado que $C^{\perp}$ es un subespacio y por tanto un código lineal.
Ahora para encontrar la dimensión del código notemos que como C es de dimensión m, existen vectores $g_1, \dots, g_m \in C$, que forman una base para C, tales que

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix}.$$

Es la matriz generadora de C, recordemos que

$$\ker(G) = \{x \in GF(D)^n : Gx^T = 0\}.$$

La idea sera probar que $C^{\perp} = \ker(G)$. Sea $x \in C^{\perp}$, note que

$$Gx^T = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix} x^T = \begin{bmatrix} \langle x, g_1\rangle \\ \vdots \\ \langle x, g_m\rangle \end{bmatrix},$$

Note que esto se tiene por la definición del producto de matrices, Pero como cada $g_i \in C$ y $x \in C^{\perp}$ tenemos que $\langle x, g_i\rangle = 0$ para cada $i = 1, \dots, m$. Así $Gx^T = 0$, luego $x \in \ker(G)$. Esto prueba $C^{\perp} \subseteq \ker(G)$. Para ver la otra contenecia considere $x \in ker(G)$, por definición

$$0 = Gx^T = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix} x^T = \begin{bmatrix} \langle x, g_1\rangle \\ \vdots \\ \langle x, g_m\rangle \end{bmatrix}.$$

De esta manera $\langle x, g_i\rangle = 0$ para cada i, pero recordemos que los g_i forman una base para C, luego dado $y \in C$, existen $\alpha_i \in GF(D)$ tales que $y = \sum_{i=1}^{m} \alpha_i g_i$, y por la linealidad del producto interno

$$\begin{aligned}\langle x, y\rangle &= \left\langle x, \sum_{i=1}^{m} \alpha_i g_i \right\rangle \\ & \sum_{i=1}^{m} \alpha_i \langle x, g_i\rangle \\ &= 0,\end{aligned}$$

así como y era arbitrario, tenemos que $\langle x, y\rangle = 0$ para todo $y \in C$, luego $x \in C^{\perp}$, probando así por la doble contenencia la igualdad de los conjuntos.
Con estos hechos por el teorema de rango-nulidad tenemos que

$$\dim(\ker(G)) + \dim(\mathrm{Im}(G)) = n,$$

Pero recordemos que la dimensión de la imagen de una matriz, es la dimensión del subespacio generado por sus filas, como sus filas generan C y este código tiene dimensión m, tenemos que $\dim(\mathrm{Im}(G)) = m$, luego como $\ker(G) = C^{\perp}$, si reemplazamos en la anterior expresión obtenemos

$$\dim(C^{\perp}) + m = n.$$

Así la dimensión de el código dual es $n - m$. Por ultimo nos falta probar que la matriz de verificacion H para C es la matriz generadora de $C^{\perp}$. Sea $G = [\ I_m \mid P\ ]$, donde P es de tamaño $m \times (n - m)$, la matriz sistemática del código C, recordemos que la matriz de paridad esta dada por $H = [\ -P^T \mid I_{n-m}\ ]$, por un hecho visto en clase sabemos que $\dim(\mathrm{Im}(H)) = n - m$, es decir que la dimensión del espacio generado por sus filas es $n - m$, si podemos probar que las filas de H pertenecen a $C^{\perp}$, por la parte anterior, como la dimensión del espacio fila coincide con la de $C^{\perp}$, habremos terminado. Primero notemos que la matriz G es de tamaño $m \times n$, mientras que H es de tamaño $(n - m) \times n$, así que consideremos el siguiente producto matricial

$$GH^T = [\ I_m \mid P\ ] \left[\begin{array}{c} -P \\ \hline I_{n-m} \end{array}\right]$$

Note que hacemos esto para que las dimensiones coincidan, el resultado serán matrices de tamaño $m \times (n - m)$, pero ademas podemos notar que la primeras m columnas de G son las entradas de la identidad, mientras que las primeras m filas de H^T son las entradas de $-P$, luego pro el producto de matrices en bloque tenemos que

$$[\ I_m \mid P\ ] \left[\begin{array}{c} -P \\ \hline I_{n-m} \end{array}\right] = -I_m P + P I_{n-m} = -P + P = 0.$$

Esto quiere decir que las columnas de H^T son ortogonales a las filas de G, o de manera equivalente, las filas de H son ortogonales a las de G. esto debido a que las entradas del producto matricial son el producto interno usual. Luego como las filas de G son una base para C, por un argumento análogo al hecho en la prueba de $\ker(G) = C^{\perp}$, tenemos que las filas de Hpertenecen a $C^{\perp}$, de esta manera por lo dicho al inicio de la prueba, hemos concluido que la matriz H es la matriz generadora del código dual de C.

Ejercicio 4

Determine las palabras código de $C^{\perp}$, si C es un código lineal binario con matriz generadora

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

Solución. Primero notemos que G es de tamaño 3×5, Asi C es un codigo lineal $[5, 3]$, es decir es un subespacio de $GF(2)^5$. Por el punto probado anteriormente sabemos que la matriz de verificacion H de el codigo C, es la matriz generadora de $C^{\perp}$, pero recordemos que solo podemos construir H si G esta en forma sistematica, y podemos darnos cuenta facilmente que no lo esta, por lo que debemos llevarla a esta forma. Esto se puede hacer por medio de operaciones elementales entre filas

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{F_3 + F_1} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{F_1 + F_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{F_1 + F_3} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Notemos entonces que $G = [\ I_3 \mid P\ ]$, donde $P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$. Como esta forma es la sistematica, podemos construir la matriz H, note que como las entradas pertenecen a $GF(2)$, tenemos que $-P^T = P^T$, luego

$$H = [\ -P^T \mid I_{5-3}\ ] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Como H es la matriz generadora, quiere decir que sus filas generan a el codigo $C^{\perp}$, es decir

$$C^{\perp} = \langle 11010, 10101 \rangle = \{00000, 11010, 10101, 01111\},$$

note que esto quiere decir que $C^{\perp}$ es un codigo $[5, 2]$, esto coincide con lo hallado en el anterior punto.

A) ¿Cuántos errores puede detectar y corregir el código $C^{\perp}$?

Solución. Primero debemos determinar la distancia minima del codigo, recordemos que

$$d_{min}(C^{\perp}) = w_{min}(C) := \min_{z \in C, z \neq 0} \{w(z)\}$$

Ahora note que el peso de las palabras no nulas es

$$w(11010) = 3,$$
$$w(10101) = 3,$$
$$w(01111) = 4.$$

Asi como el peso minimo es 3, tenemos que $C^{\perp}$ es un codigo $[5, 2, 3]$. Recordemos entonces que un codigo puede detectar y corregir patrones con $\left\lfloor \frac{d_{min}(C^{\perp}) - 1}{2} \right\rfloor$, si reemplazamos en la expresion obtenemos que

$$\left\lfloor \frac{d_{min}(C^{\perp}) - 1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1.$$

Es decir que $C^{\perp}$ puede detectar y corregir hasta 1 error.

B) ¿Es el código $C^{\perp}$ mejor que el código C para detectar y corregir errores?

Solución. Para responder esta pregunta debemos determinar la distancia minima de C y ver cuantos errores puede detectar y corregir. Primero como las filas de G son una base para C, tenemos que

$$C = \langle 11100, 01010, 11001 \rangle = \{00000, 11100, 01010, 11001, 10110, 00101, 10011, 01111\}.$$

Luego el peso de cada palabra no nula en el codigo es

$$\begin{aligned} w(11100) &= 3, \\ w(01010) &= 2, \\ w(11001) &= 3, \\ w(10110) &= 3, \\ w(00101) &= 2, \\ w(10011) &= 3, \\ w(01111) &= 4. \end{aligned}$$

Como hay palabras con peso dos tenemos que $d_{min}(C) = 2$, asi la cantidad de errores que puede detectar y corregir es

$$\left\lfloor \frac{d_{min}(C) - 1}{2} \right\rfloor = \left\lfloor \frac{2-1}{2} \right\rfloor = 0.$$

Esto quiere decir que C no puede corregir errores, por lo que $C^{\perp}$ es mejor ya que este puede detectar y corregir patrones con un error, mientras que C no puede.

C) ¿Es C un código perfecto?

Solución. Por lo hallado en la anterior parte sabemos que C es un codigo $[5, 3, 2]$. En este caso nuestros datos son $D = 2, n = 5$ y $d = 2$. Para esto el radio de las esferas esta dado por $t = \lfloor \frac{2-1}{2} \rfloor = 0$, luego tenemos que

$$\mathrm{Vol}_2(0, 5) = \sum_{i=0}^{0} \binom{5}{i} (2-1)^i = 1,$$

Ahora recordemos que $M = |C| = 8$, luego note que

$$8 = M < \frac{D^n}{\mathrm{Vol}_D(t,n)} = \frac{2^5}{\mathrm{Vol}_2(0,5)} = 32.$$

Como no se tiene la igualdad, concluimos que el codigo C no es perfecto.

ʊ̬ʊ

Ejercicio 5
Sea $C \preceq \mathrm{GF}(3)^6$ un código lineal con matriz generadora

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

A) Calcule una matriz sistemática para C.

B) Calcule la correspondiente matriz de verificación.

C) Decodifique el mensaje $z = 001021$. Indique en su hoja de respuesta la coclase correspondiente.

Ejercicio 6
Una fuente F genera símbolos de un alfabeto $\{a, b, c\}$ y se modela como un proceso markoviano $\{X_i\}_{i\in\mathbb{N}}$ con matriz de transición

$$P = \begin{bmatrix} 0.6 & 0.3 & 0.1 \\ 0.2 & 0.5 & 0.3 \\ 0.1 & 0.4 & 0.5 \end{bmatrix}$$

A) Determine la distribución de probabilidad para las variables aleatorias X_i.

B) ¿Cuál es la probabilidad de que la fuente emita la palabra $\mathtt{aabc}$ (considerando que las letras salen de derecha a izquierda, es decir, primero $\mathtt{c}$)?

C) Dibuje el grafo de estados que modela el proceso markoviano.

Ejercicio 7
Resuelva el ejercicio 6.7.6 de las notas de clase.
Considere una fuente binaria con una distribución de probabilidades $\{p(0) = 0.3, p(1) = 0.7\}$ y un canal con matriz de transición:

$$\begin{bmatrix} 0.1 & 0.9 \\ 0.8 & 0.2 \end{bmatrix}$$

Si los símbolos de la fuente son codificados mediante las asignaciones $0 \to 000$, $1 \to 111$, determine una función decodificadora $\delta : \{0,1\}^3 \to \{0,1\}$ con máxima probabilidad de corrección.