MATEMATICA DISCRETA II-2019
PRÁCTICO 4:Códigos de corrección de errores

I): Sea

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

y sea C el código generado por G.
a) ¿Cual es la longitud de C? Cual es su dimensión?
b)Supongamos que desea mandar el mensaje 10101 11010 00111. ¿Cuales son las palabras del código que deberia usar para mandar el mensaje?
c) Dar una matriz de chequeo de C.
d) Calcular $\delta(C)$.
e) Supongamos que se reciben las palabras 100111001, 011100011 y 110000001 ¿ Cuales son las palabras mas probables que se hayan mandado? ¿A que mensaje corresponden?
f) ¿ Que puede concluir si recibe la palabra 001111010?

II): Sea H la matriz de chequeo:

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

y sea C el código asociado a ella.
a) Describir C explicitamente (es decir, dar las palabras que constituyen el código).
b) Calcular $\delta(C)$.
c) Suponga que Ud. recibe la palabra 00111000. Asumiendo que se produjo a lo sumo un error de transmisión, ¿que palabra le fue enviada?
d) Ud. recibe la palabra 11100111. ¿ Que puede concluir?

III): Sea H la matriz de chequeo:

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

y sea C el código asociado a ella.
a) Escribir 5 palabras que esten en C. ¿Cuantas palabras tiene en total C?
b) Calcular $\delta(C)$.
c) Suponga que Ud. recibe la palabra 11100000000011. Asumiendo que se produjo a lo sumo un error de transmisión, ¿que palabra le fue enviada?

IV): Una consultora realizará 65 preguntas a una población. Cada pregunta tendrá como respuestas posibles "Siempre", "Frecuentemente", "De vez en cuando", "Rara Vez", y "Nunca". La compañia quiere codificar esta informacion. (por lo tanto, los datos a codificar son cosas del tipo "pregunta 32, respuesta Frecuentemente"). La encuestadora desea que el código sea capaz de corregir un error por dato y que codifique todos los datos posibles.
a) Diseñe un código lineal que satisfaga esto, dando una matriz de chequeo apropiada del menor tamaño posible.
b) Escriba dos palabras que esten en su código.
c) Tome una de sus palabras de b), y cambiele los dos primeros digitos. Suponga que esa es la palabra que se recibe. Prediga que deducirá la persona que la recibe, de acuerdo con el código diseñado por Ud. Explique bien porqué.

V): Dar un ejemplo de un código lineal C con matriz generadora G tal que $\delta(C)$ NO sea igual a la menor cantidad de unos que aparece en alguna fila de G.

VI): Se tiene un código binario de longitud 16 tal que la distancia minima entre palabras es 7. Dar una cota superior para el numero de palabras del código. Dar una cota superior si ademas se requiere que el código sea lineal.

VII): Sea A el conjunto de códigos de longitud 12 con 512 elementos, B el conjunto de códigos de longitud 12 con 3584 elementos y L el conjunto de códigos de longitud 12 que son lineales.
Probar que $|A| = |B|$ pero $|A \cap L| > |B \cap L|$.

VIII): Estoy pensando en un número natural entre 1 y 2048. Ud debe deducir el número, haciendome a lo sumo 15 preguntas cuyas unicas respuestas posibles sean "Si" o "No", y teniendo en cuenta que yo puedo mentirle una vez.

IX): Si C es un código lineal, probar que el conjunto que consiste en todas las palabras de C de peso par tambien es un código lineal.

X): a) Probar que si C es un código binario perfecto con distancia mínima $\delta = 3$, entonces debe tener la misma longitud y la misma cantidad de elementos que algún código de Hamming. (i.e., debe existir r tal que C tiene longitud $2^r - 1$ y $2^{2^r - r - 1}$ elementos).
b) Sin embargo los de Hamming no son los únicos códigos binarios perfectos con $\delta = 3$: Dado un $r \geq 3$, denotemos por $\oplus$ el XOR (Exclusive OR), por $\vee$ el OR y por $\mathcal{H}_r$ un código de Hamming con parámetro r. Sea $n = 2^r - 1$ y sea C el código:

$$C = \{(x, x \oplus w, x_1 \oplus ... \oplus x_n \oplus (w_1 \vee ... \vee w_n)) | x \in \boldsymbol{Z}_2^n, w \in \mathcal{H}_r\}$$

b1) Probar que C no es lineal. (por lo tanto, no puede ser ningún código de Hamming) (nota: aca usamos que $r \geq 3$ pues para $r = 2$ se tiene $C = \mathcal{H}_3$).
b2) Probar que $\delta(C) = 3$.
b3) Probar que C es perfecto.