MATEMATICA DISCRETA II-2016
PRÁCTICO 7:Códigos de corrección de errores

I): 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.

II): 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 $|A \cap L| > |B \cap L|$.

III): 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?
b) Dar una matriz de chequeo de C.
c) Calcular $\delta(C)$.
d) Supongamos que se reciben las palabras 100111001 y 110000001 ¿ Cual es son las palabras mas probables que se hayan mandado? ¿A que mensaje corresponden?
e) ¿ Que puede concluir si recibe la palabra 001111010? ¿ y si recibe la palabra 011100011?

IV): 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?

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): 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?

VII): 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 $r \geq 2$, 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)
b2) Probar que $\delta(C) = 3$.
b3) Probar que C es perfecto.

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): Una empresa necesita codificar un millón de palabras. Desea que el código sea capaz de corregir un error.
a) Supongamos que Ud. desea diseñar un código lineal por medio de una matriz de chequeo que satisfaga esto. ¿ Cual es el menor tamaño que debe tener la matriz?
b) Escriba una matriz que satisfaga las condiciones, del tamaño dado en a).
c) Escriba dos palabras de peso menor o igual a 6 que esten en su código y una palabra de peso mayor o igual a 15 que este en su código.
d) Tome una de sus palabras de b), y cambiele los dos primeros digitos. (si es un 1, escriba 0 y viceversa) 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 por qué.

X): 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.

XI): Dados los siguientes polinomios $g(x)$, junto con la longitud n, sea C el código de longitud n generado por $g(x)$. Dar la dimension de C, una matriz de chequeo de C con la identidad a izquierda, probar que $g(x)$ divide a $x^n + 1$ hallar el polinomio chequeador y en cada caso, elejir dos palabras no nulas de la dimension adecuada, y codificarlas, usando ambos metodos enseñados en clase.

a) $g(x) = 1 + x^2 + x^3$; $n = 7$. b) $g(x) = 1 + x + x^4$; $n = 15$
(los anteriores generan códigos de Hamming)
c) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$; $n = 15$.
(este genera un código que corrige 2 errores)
d) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$; $n = 23$.
(nota: este ultimo genera el código **Golay**. Corrige 3 errores, pues tiene $\delta = 7$. (no hace falta que pruebe esto)).

XII): Probar que el código Golay dado en el ejercicio anterior es perfecto.

XIII):
a) ¿Cuántos códigos binarios de longitud n hay? (con al menos 2 palabras)
b) ¿Cuántos códigos binarios de longitud 3 con exactamente 5 palabras hay?
c) ¿Cuántos de esos códigos son lineales?
d) ¿Cuántos códigos binarios de longitud 3 con exactamente 4 palabras hay?
e) ¿Cuántos de esos códigos son lineales?
f) ¿Cuántos de esos códigos son cíclicos?

XIV): $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ con $n = 15$ genera un código de longitud 15 que corrije 2 errores. Use el algoritmo de "error trapping" para corregir los errores de las siguientes palabras:
a) 001000001110110 b) 110010011110111 c) 001111101001001
d) 001000000110000 e) 110001101000101 f) 001001000100110

XV): Sean C_1, C_2 códigos cíclicos con generadores g_1, g_2. Probar que $C_1 + C_2$ tambien es cíclico y tiene generador $\text{mcd}(g_1, g_2)$.