

MATEMATICA DISCRETA II-2023
1er PRACTICO DE CÓDIGOS

I): En cada uno de los codigos siguientes, encontrar el numero de errores que pueden ser detectados/corregidos.

a) $C = \{0000000, 1111110, 1010100, 0101010\}$

b) $C = \{0000000, 1111111, 1111000, 0000111\}$

c) $C = \{000000000, 111111111, 111100000, 000011111, 101010101, 010101010\}$

II): Se tiene un código binario de longitud 8 tal que la distancia minima entre palabras es 5. Dar una cota superior para el número de palabras del código. Dar una cota superior si ademas se requiere que el código sea lineal.

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

IV): Probar que todo código binario lineal con parametros $(n, k, \delta) = (23, 11, 7)$ es perfecto.

V): Sea

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

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?

VI): Sea H la matriz de chequeo:

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

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?

VII): 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

VIII): Sea H la matriz de chequeo:

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

y sea C el código asociado a ella.

a) Escribir 5 palabras que esten en C . ¿Cuántas 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?

IX):

Sea C el código con matriz de chequeo:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & a & b \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & c & d \end{bmatrix}$$

Escribir dos palabras no nulas que esten en C , decir cuántas palabras tiene en total C , calcular $\delta(C)$, justificando y, si se recibe la palabra 1000000000000111, y se asume que se produjo a lo sumo un error de transmisión, determinar la palabra enviada si esto es posible o indicar porqué no si no se puede. Las respuestas pueden depender de cuales valores toman $a, b, c, d \in \{0, 1\}$, si es así, ud. debe indicarlo y dar todas las respuestas posibles.

X): 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.

XI): 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 compañía quiere codificar esta información. (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 estén en su código.

c) Tome una de sus palabras de b), y cambie los dos primeros dígitos. 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.

XII): Si tenemos un código de Hamming de 5 filas con la columna i -ésima igual a la representación binaria de i , contando columnas de izquierda a derecha y representando números con el bit menos significativo arriba, y llega la palabra

$$w = 0000101001000010000001000000001$$

calcular cual es la palabra mas probable enviada.

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

XIV): Probar que si C es un código binario que corrige un error pero no corrige 2, entonces C es perfecto si y solo si existe r tal que C tiene longitud $2^r - 1$ y $2^{2^r - r - 1}$ elementos.

XV): Vimos arriba que un código binario perfecto que corrija un error debe tener longitud $2^r - 1$ y $2^{2^r - r - 1}$ elementos. En el teórico vimos que para cada $r \geq 2$ existe un código lineal que corrige un error con esos parametros. (los códigos de Hamming) ¿Existe alguno no lineal? La respuesta es si: Dado un $r \geq 2$, sea $n = 2^r - 1$, sea C el código:

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

a) Probar que la longitud de C es $2^{r+1} - 1$.

b) Probar que C tiene $2^{2^{r+1} - (r+1) - 1}$ elementos.

c) Probar que $\delta = 3$ (por lo tanto por a) y b), C será perfecto). (damos una ayuda, pero lo pueden probar como quieran)

c1) Probar que $0 \in C$.

c2) Dar un $\alpha \in C$ con $d(\alpha, 0) = 3$. (esto y c1) prueba que $\delta \leq 3$).

c3) Probar que $\delta \geq 3$ probando que $d(\alpha, \beta) \geq 3 \forall \alpha, \beta \in C$, observando que si $\alpha = (x, x \oplus w, x_1 \oplus \dots \oplus x_n \oplus (w_1 \vee \dots \vee w_n))$ y $\beta = (y, y \oplus v, y_1 \oplus \dots \oplus y_n \oplus (v_1 \vee \dots \vee v_n))$, entonces se pueden hacer los siguientes casos:

c3i) $x \neq y, w = v, x_1 \oplus \dots \oplus x_n = y_1 \oplus \dots \oplus y_n$

- c3ii) $x \neq y, w = v, x_1 \oplus \dots \oplus x_n \neq y_1 \oplus \dots \oplus y_n$.
 - c3iii) $x = y, w \neq v$.
 - c3iv) $x \neq y, w \neq v, x \oplus w = y \oplus v$.
 - c3v) $x \neq y, w \neq v, d(x \oplus w, y \oplus v) \geq 2$.
 - c3vi) $x \neq y, w \neq v, d(x \oplus w, y \oplus v) = 1$.
- d) Probar que C no es lineal.

.

XVI): En la isla de los caballeros y los picaros (recordar que los caballeros siempre dicen la verdad y los picaros siempre mienten) hay una mesa con 2048 llaves. Una de esas llaves abre la puerta de una habitación donde, del otro lado, hay oro, diamantes, la pocima de la salud eterna, y una maquina transdimensional que calcula $\chi(G)$ en $O(m)$. Las otras 2047 llaves destruirán la habitación si ud. la usa para abrirla, además de infectarle a control remoto cualquier computadora en la cual Ud. alguna vez quiera hacer algo. (incluyendo las computadoras de los autos).

Para ayudarle a elegir la llave, 15 habitantes de la isla están dispuestos a responderle preguntas, cuyas respuestas sean ‘SI’ o ‘NO’. Una vez que uno de ellos ya haya respondido, no puede volver a preguntarle (a ese habitante). Cada uno sabe cual es la llave, y estudiaron teoría de códigos, PERO NO saben quienes de entre esos 15 son caballeros y quienes picaros. Un decimosexto habitante de la isla le dice:

“Si soy caballero, entonces entre esas 15 personas hay a lo sumo un solo picaro”
 ¿Como puede hacerle preguntas a las 15 personas para encontrar la llave?