Comunicación de datos
Curso 2016/17, Problemas # 4

1. Dados dos vectores binarios de longitud n, $\mathbf{x}, \mathbf{y} \in \mathcal{L}_n$, se define su intersección como el vector cuyo elemento i-ésimo vale 1 si y sólo si $\mathbf{x}$ e $\mathbf{y}$ tienen simultáneamente un 1 en la posición i:

$$\mathbf{x} \cap \mathbf{y} \triangleq (x_1 y_1, \ldots, x_n y_n).$$

Demuestre la igualdad

$$p_H(\mathbf{x} + \mathbf{y}) = p_H(\mathbf{x}) + p_H(\mathbf{y}) - 2p_H(\mathbf{x} \cap \mathbf{y}).$$

Utilizando esta igualdad, pruebe que en un código lineal:

a) La suma de dos palabras del código de peso par es otra palabra del código de peso par y el subconjunto de palabras del código de peso par es un código lineal.

b) La suma de dos palabras del código de peso impar es una palabra del código de peso par.

c) La suma de una palabra del código de peso par con una palabra del código de peso impar produce una palabra del código de peso impar.

d) O bien todas las palabras del código son de peso par o bien la mitad son de peso par y la otra mitad son de peso impar. Como corolario, pruebe que el subconjunto de palabras del código de peso par es un código lineal $[n, k]$ o $[n, k-1]$.

e) O bien todas las palabras del código tienen un 0 en la coordenada $1 \leq j \leq n$ o bien la mitad tienen un 1 y la otra mitad un 0. Como corolario de esta proposición, pruebe que el subconjunto de palabras del código con un 0 en la coordenada j o bien es un código lineal $[n, k]$ o bien es un código lineal $[n, k-1]$.

f) La distancia entre dos palabras del mismo peso es par.

2. La matriz de comprobación de paridad de un código lineal binario es

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

a) Calcule la distancia del código.

b) Construya una tabla de decodificación por síndrome.

3. Sea H la matriz de comprobación de paridad de un código Hamming binario $[15, 11]$. Considérese el código lineal $\mathcal{C}$ cuya matriz de comprobación de paridad es la obtenida al eliminar de H todas las columnas con un número par de unos. Sin escribir las palabras de $\mathcal{C}$:

a) Indique los parámetros del código y muestre que su distancia es 4.

b) Demuestre que todas las palabras del código no nulas tienen un número par de unos.

c) ¿Cuántos errores de peso Hamming 4 son detectables? ¿Cuál es la probabilidad de no detectar un error cuando $\mathcal{C}$ se utiliza para transmitir sobre un canal binario simétrico con probabilidad de error de bit p?

d) Si de toda palabra del código se borra un bit de paridad, ¿qué código se obtiene?

4. Sea G_1 una matriz generadora de un código lineal $[n_1, k_1]$ con distancia d_1 y sea G_2 una matriz generadora de un código lineal $[n_2, k_2]$ con distancia d_2. Encuentre los parámetros (longitud, dimensión y distancia) y caracterice, si es posible, las palabras de los códigos cuyas matrices generadoras son las siguientes:

a)

$$\begin{pmatrix} & & G_1 & & \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix}$$

b)

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

c) Si $k_1 = k_2 = k$, muestre que el código lineal de matriz generadora $(G_1|G_2)$ tiene parámetros $[n_1 + n_2, k]$ y distancia $d \geq d_1 + d_2$.

5. Para el código $\mathcal{C}$ que tiene por matriz generadora a

$$G = \left(\begin{array}{c|cccccc} & 1 & 0 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 1 & 1 & 1 \\ & 1 & 1 & 1 & 0 & 1 & 1 \\ I_6 & 1 & 1 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

se pide:

a) Probar que la distribución de pesos es simétrica, $A_i = A_{12-i}$.

b) Hallar la distribución de pesos.

c) Hallar la distribución de pesos de los errores corregibles.

6. La matriz

$$G = \left(\begin{array}{c|cccccc} & 0 & 0 & 0 & 1 & 1 & 1 \\ I_4 & 0 & 1 & 1 & 0 & 1 & 0 \\ & 1 & 0 & 1 & 0 & 0 & 1 \\ & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right)$$

es generadora de un código lineal binario $[10, 4]$.

a) ¿Cuál es la distancia del código?

b) Calcule el número de vectores de error de peso $i = 1, 2, \dots, 10$ que se pueden corregir si se aplica el método de decodificación por síndrome.

c) Suponga que el canal de transmisión no tiene memoria y que se produce un error de transmisión. A la vista de las ecuaciones de comprobación de paridad, deduzca un método de decodificación capaz de corregir los errores simples sin construir la tabla de síndromes.

7. Sea $\mathcal{C}$ el código binario definido por la matriz de comprobación de paridad

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

a) ¿Cuáles son la longitud, dimensión y distancia de $\mathcal{C}$?

b) Escriba una matriz generadora de $\mathcal{C}$.

c) ¿Cuál es el mayor entero t tal que el código es capaz de corregir cualquier patrón hasta t errores?

d) Si se recibe el vector 101010101 ¿cuál será la salida de un decodificador de máxima verosimilitud?

8. Considere el código lineal binario $\mathcal{C}$ con matriz de comprobación de paridad

$$H = \begin{pmatrix} H_4 & 0 \\ 0 & H_4 \end{pmatrix}$$

en donde H_4 es matriz de comprobación de paridad del código Hamming binario $[15, 11]$.

a) Indique la longitud, la dimensión y la distancia de $\mathcal{C}$.

b) Demuestre que $\mathcal{C}$ sólo puede corregir errores simples y dobles. ¿Cuántos dobles?

c) La distribución de pesos del código Hamming es $A_0 = A_{15} = 1$, $A_3 = A_{12} = 35$, $A_4 = A_{11} = 105$, $A_5 = A_{10} = 168$, $A_6 = A_9 = 280$, $A_7 = A_8 = 435$. La distribución de pesos de $\mathcal{C}$ viene dada por la fórmula $B_i = \sum_{j=0}^{i} A_j A_{i-j}$. Calcule el número de palabras de peso mínimo de $\mathcal{C}$.

9. Considere la colección $\mathcal{C}_r$ de códigos lineales binarios definidos por matrices de comprobación de paridad de la forma

$$H_r = \begin{pmatrix} I_r & B_{r\times m} \end{pmatrix} \qquad r \geq 2$$

en donde I_r es la matriz identidad $r \times r$ y $B_{r\times m}$ es una matriz que tiene por columnas vectores distintos de peso 2 de forma que ninguna de sus filas es nula.

a) ¿Cuáles son la longitud y la dimensión mínimas de un código de la familia $\mathcal{C}_r$? ¿Cuáles la longitud y la dimensión máximas? Indique qué matrices corresponden a cada caso.

b) La distancia de cualquiera de los códigos de $\mathcal{C}_r$ es 3. Calcule el número de palabras de peso 3 del código de longitud máxima. Ídem para uno cualquiera de los de longitud mínima.

10. Se define la sucesión de matrices

$$\mathcal{H}_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathcal{H}_m = \begin{pmatrix} 1 \;\; \dots \;\; 1 & 1 \;\; \dots \;\; 1 \\ \mathcal{H}_{m-1} & \overline{\mathcal{H}}_{m-1} \end{pmatrix}$$

en donde $\overline{\mathcal{H}}_{m-1}$ es la matriz complementaria de $\mathcal{H}_{m-1}$ ($0 \mapsto 1$ y $1 \mapsto 0$). Considérese la matriz $\mathcal{H}_m$ como matriz de comprobación de paridad de un código lineal binario $\mathcal{D}_m$, para cualquier $m \geq 2$.

a) Indique razonadamente la longitud y dimensión de $\mathcal{D}_m$.

b) Explique: para $m \geq 2$, todos los códigos $\mathcal{D}_m$ tienen la misma distancia. Calcúlela.

c) Demuestre que la tabla de síndromes de estos códigos $\mathcal{D}_m$ sólo contiene vectores de peso menor o igual que dos. ¿Cuántos errores simples y dobles se pueden corregir?

d) Muestre que si $\mathbf{u}$ y $\mathbf{v}$ son palabras de $\mathcal{D}_{m-1}$ entonces el vector $(\mathbf{u}, \mathbf{v})$ que se forma concatenando ambas es una palabra del código $\mathcal{D}_m$. Use la igualdad $\mathbf{x}\overline{P} = \mathbf{x}(P + J)$, donde J es una matriz binaria con todos sus elementos iguales a 1, válida para todos los vectores $\mathbf{x}$ y matrices P binarias de las dimensiones apropiadas.

e) Deduzca del apartado anterior que, si $\{B_i\}$ es la distribución de pesos de $\mathcal{D}_m$ y $\{A_i\}$ es la de $\mathcal{D}_{m-1}$ entonces $B_i \geq \sum_j A_j A_{i-j}$.

11. Sean $\mathcal{H}_r$ y $\mathcal{H}_s$ los códigos Hamming binarios de r y s bits de redundancia, respectivamente, y sean H_r y H_s sus matrices de comprobación de paridad. Recuerde que los códigos Hamming tienen distancia 3 y corrigen únicamente los errores simples.

a) Obtenga la distancia del código que tiene por matriz de comprobación de paridad

$$\begin{pmatrix} H_r & 0 \\ 0 & H_s \end{pmatrix}.$$

b) Obtenga también su distribución de pesos de errores corregibles.

12. El código Hamming binario extendido $\overline{\mathcal{H}}_r$ es el de matriz de comprobación de paridad

$$\overline{H}_r = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 \\ & & & & & 0 \\ & & & & & \vdots \\ & & H_r & & & 0 \end{pmatrix}, \qquad r \geq 2$$

en donde H_r denota la matriz de comprobación de paridad del código Hamming binario con r símbolos de redudancia. $\overline{\mathcal{H}}_r$ se obtiene añadiendo a las palabras un símbolo de paridad par.

a) ¿Qué longitud, dimensión y distancia tiene $\overline{\mathcal{H}}_r$?

b) Deduzca que $\alpha_0 = 1$, $\alpha_1 = 2^r$ y $\alpha_2 = 2^r - 1$ es la distribución de pesos de los errores corregibles.

c) Muestre que $\mathbf{1} \in \overline{\mathcal{H}}_r$.

d) Escriba explícitamente la matriz $\overline{H}_3$ y úsela para decodificar el vector $1110\ldots0$.

13. Para cualquier $r > 3$, sea H_r la matriz de comprobación de paridad de un código Hamming binario con r bits de redundancia. Considérense las matrices $H_{r,\text{par}}$ y $H_{r,\text{impar}}$ formadas, respectivamente, por las columnas de peso par (impar) de H_r como las de comprobación de paridad de dos nuevos códigos, $\mathcal{P}_r$ e $\mathcal{I}_r$.

a) Indique razonadamente la longitud, dimensión y distancia de $\mathcal{P}_r$ e $\mathcal{I}_r$.

b) ¿Puede $\mathcal{P}_r$ corregir algún error doble? ¿Puede $\mathcal{I}_r$ corregir algún error doble?

c) ¿Cuántas palabras de peso 3 tiene $\mathcal{P}_r$? ¿Cuántas palabras de peso 3 tiene $\mathcal{I}_r$?

14. Si H_r denota la matriz de comprobación de paridad de un código Hamming binario $[2^r-1, 2^r-r-1]$, considérense los códigos con matriz de comprobación

$$T_{2r+1} = \begin{pmatrix} & H_r & & & & & \\ 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \\ & & & & & H_r & \end{pmatrix}.$$

a) Obtenga la longitud, dimensión y distancia del código correspondiente a T_{2r+1}.

b) Sean $\mathbf{s}_1, \mathbf{s}_2$ vectores binarios no simultáneamente nulos de longitud r. Muestre que el síndrome $(\mathbf{s}_1, 0, \mathbf{s}_2)$ es la suma de dos columnas de T_{2r+1}. Si estos son los únicos síndromes correspondientes a errores dobles corregibles, ¿cuántos hay?

c) ¿Es $11\ldots1$ (para la longitud apropiada) una palabra de estos códigos?

15. Sean I_m la matriz identidad de orden m y J_m la matriz $m \times m$ con todos los elementos iguales a uno. Considere el código binario con matriz de comprobación de paridad

$$H_m = \begin{pmatrix} I_m & J_m + I_m \end{pmatrix}.$$

Por ejemplo, para $m = 4$

$$H_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Pero H_4 define un código muy pequeño y nosotros queremos más. Suponga que m es un número grande.

a) Encuentre la distancia del código definido por H_m. Dé un argumento claro.

b) Averigüe cuántos errores de peso dos es capaz de corregir este código. Compruebe que, si m es grande, son corregibles la mitad de los errores dobles, aproximadamente.