Relación Ejercicios

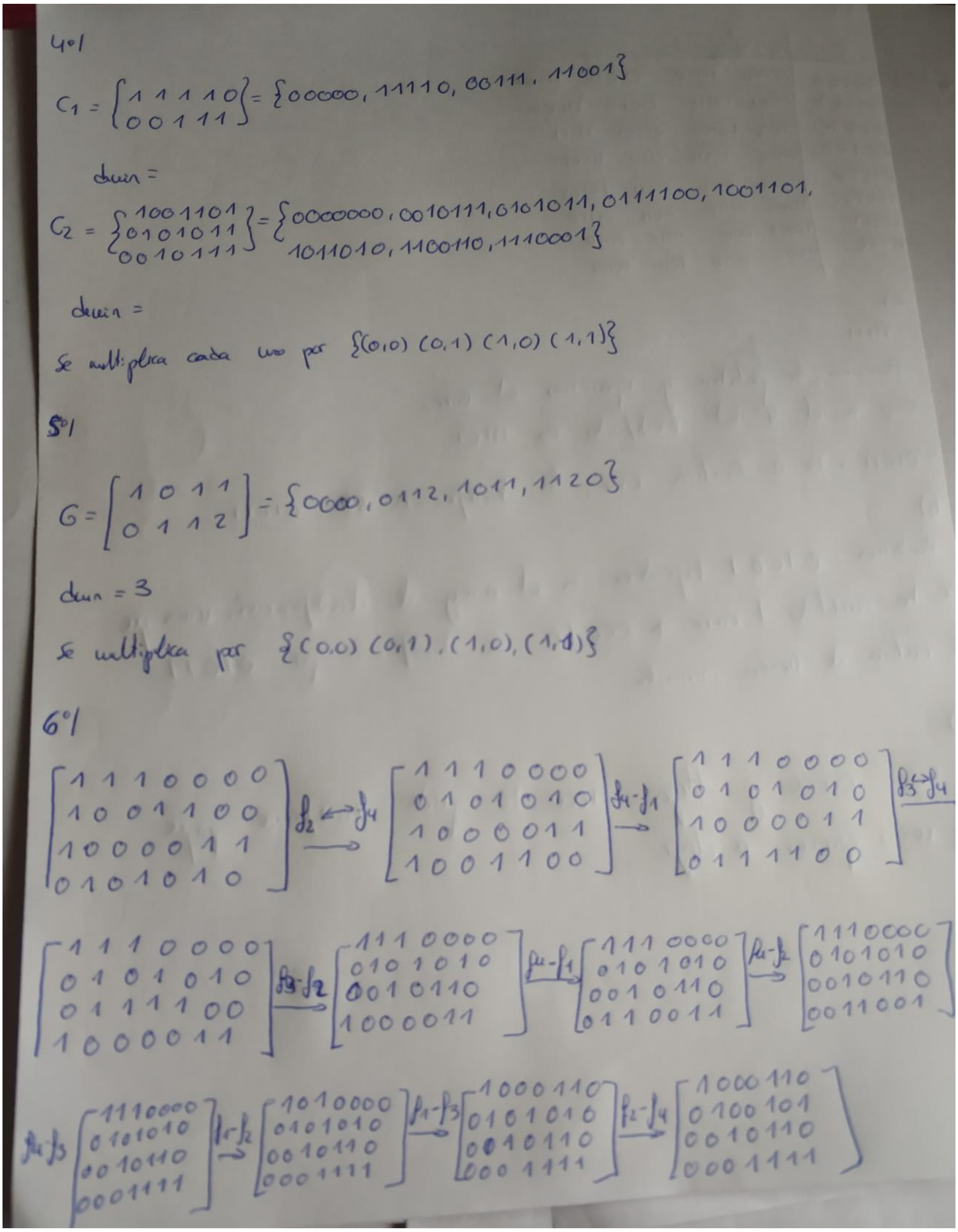
Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

Relación Códigos Lineales



4º)

$$C_1 = \begin{Bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{Bmatrix} = \{00000, 11110, 00111, 11001\}$$

dmin =

$$C_2 = \begin{Bmatrix} 1001101 \\ 0101011 \\ 0010111 \end{Bmatrix} = \{0000000, 0010111, 0101011, 0111100, 1001101, 1011010, 1100110, 1110001\}$$

dmin =

Se multiplica cada uno por $\{(0,0)\ (0,1)\ (1,0)\ (1,1)\}$

5º)

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix} = \{0000, 0112, 1011, 1120\}$$

dmin = 3

Se multiplica por $\{(0,0)\ (0,1), (1,0), (1,1)\}$

6º)

$$\begin{bmatrix} 1&1&1&0&0&0&0 \\ 1&0&0&1&1&0&0 \\ 1&0&0&0&0&1&1 \\ 0&1&0&1&0&1&0 \end{bmatrix} \xrightarrow{f_2 \leftrightarrow f_4} \begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1 \\ 1&0&0&1&1&0&0 \end{bmatrix} \xrightarrow{f_4 - f_1} \begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1 \\ 0&1&1&1&1&0&0 \end{bmatrix} \xrightarrow{f_3 \leftrightarrow f_4}$$

$$\begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 0&1&1&1&1&0&0 \\ 1&0&0&0&0&1&1 \end{bmatrix} \xrightarrow{f_3 - f_2} \begin{bmatrix} 1110000 \\ 0101010 \\ 0010110 \\ 1000011 \end{bmatrix} \xrightarrow{f_4 - f_1} \begin{bmatrix} 1110000 \\ 0101010 \\ 0010110 \\ 0110011 \end{bmatrix} \xrightarrow{f_4 - f_2} \begin{bmatrix} 1110000 \\ 0101010 \\ 0010110 \\ 0011001 \end{bmatrix}$$

$$\xrightarrow{f_4 - f_3} \begin{bmatrix} 1110000 \\ 0101010 \\ 0010110 \\ 0001111 \end{bmatrix} \xrightarrow{f_1 - f_2} \begin{bmatrix} 1010000 \\ 0101010 \\ 0010110 \\ 0001111 \end{bmatrix} \xrightarrow{f_1 - f_3} \begin{bmatrix} 1000110 \\ 0101010 \\ 0010110 \\ 0001111 \end{bmatrix} \xrightarrow{f_2 - f_4} \begin{bmatrix} 1000110 \\ 0100101 \\ 0010110 \\ 0001111 \end{bmatrix}$$

Ejercicios 4,5 y 6 Relación códigos lineales.

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

7º/

e	e + C			
00000	00000	10110	01011	11101
00001	00001	10111	01010	11100
00010	00010	10100	01001	11111
00100	00100	10010	01111	11001
01000	01000	11110	00011	10101
10000	10000	00110	11011	01110
10001	10001	00111	11010	01110
11000	11000	01110	10111	00101

a)

- 11111

Buscamos la palabra y reparamos el error.

Error en el 4º bit. Decodificado es 11101.

- 01011 → No se localiza error, la decodificación es 01011

b)

Recibimos 01001. Fijándonos en el array de decodificación, vemos que se ha cometido 1 error → 00010 se decodificaría por 01011. Se realiza de manera incorrecta.

c)

Se envía 00000 y llega 11000. No puede decodificarse porque hay varias opciones a elegir.

Ejercicio 7 Relación códigos lineales.

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

9º)

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

a)

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix} f_2 - 2f_1 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} f_1 - f_2 \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix}$$

b)

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

c)

e	S(e)
0000	00
0001	01
0002	02
....	
2121	

$$\overbrace{2\begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}1\\2\end{pmatrix} + 2\begin{pmatrix}1\\0\end{pmatrix} + 1\begin{pmatrix}0\\1\end{pmatrix}}^{2121} = \begin{pmatrix}2\\2\end{pmatrix} + \begin{pmatrix}1\\2\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} + \begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}2\\2\end{pmatrix}$$

S(1000) = 22

$$\overbrace{1\begin{pmatrix}1\\1\end{pmatrix} + 2\begin{pmatrix}1\\2\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}2\\1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} = 00}^{1201} \quad S(0000)$$

2222

$$2\begin{pmatrix}1\\1\end{pmatrix} + 2\begin{pmatrix}1\\2\end{pmatrix} + 2\begin{pmatrix}1\\0\end{pmatrix} + 2\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}2\\2\end{pmatrix} + \begin{pmatrix}2\\1\end{pmatrix} + \begin{pmatrix}2\\0\end{pmatrix} + \begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = 01$$

S(0001)

Ejercicio 9 Relación códigos lineales.

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

(10) $[8,4]$ $GF(2)$

$P_6 = M_1 + M_2 + M_4$

$P_7 = M_1 + M_3 + M_4$

$P_8 = M_1 + M_2 + M_3$

$P_9 = M_2 + M_3 + M_4$

Matriz generadora

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

Matriz de paridad

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

$d_{min} = 8.$

Ejercicio 10 Relación códigos lineales.

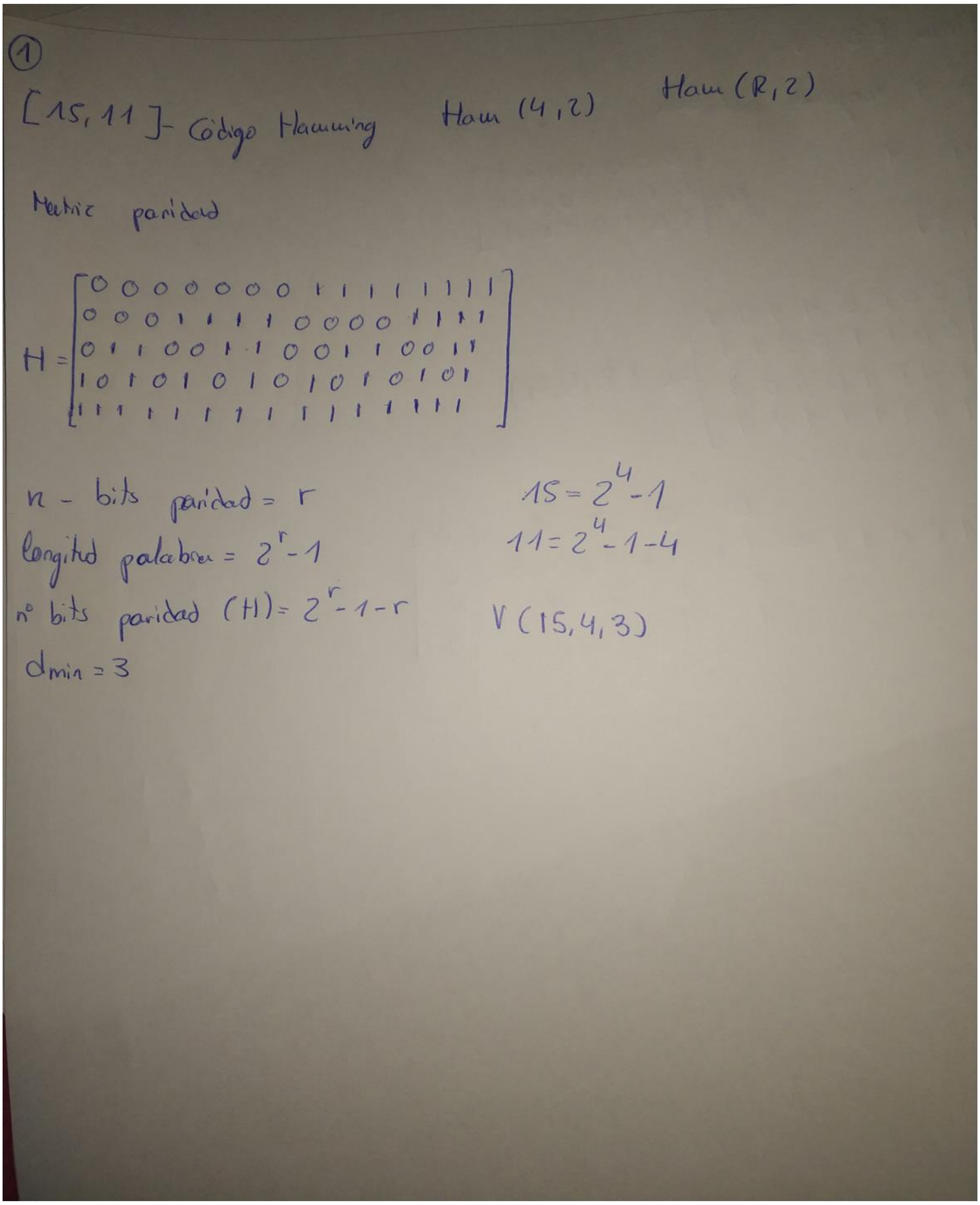
Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

Relación Hamming



1

[15, 11] - Código Hamming   Ham (4, 2)   Ham (R, 2)

Matriz paridad

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

n - bits paridad = r $15 = 2^4 - 1$

longitud palabra = $2^r - 1$ $11 = 2^4 - 1 - 4$

nº bits paridad (H) = $2^r - 1 - r$ V (15, 4, 3)

$d_{min} = 3$

Ejercicio 1 Relación Hamming

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

③ Ham (3,2)

$2^3-1 = 7$ longitud palabra

$2^3-1-4 = 4$

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

$V(7,4,3)$

$$H' = \begin{bmatrix} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix} \rightarrow (8,4,4)$$

$$00110011 \Rightarrow \begin{matrix}0\\1\\0\\1\end{matrix} + \begin{matrix}0\\1\\1\\1\end{matrix} + \begin{matrix}1\\1\\0\\1\end{matrix} + \begin{matrix}1\\1\\1\\1\end{matrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

$$11100000 \Rightarrow \begin{matrix}0\\0\\0\\1\end{matrix} + \begin{matrix}0\\0\\1\\1\end{matrix} + \begin{matrix}0\\1\\0\\1\end{matrix} = \begin{bmatrix}0\\1\\1\\1\end{bmatrix}$$

$$01110000 \Rightarrow \begin{matrix}0\\0\\1\\1\end{matrix} + \begin{matrix}0\\1\\0\\1\end{matrix} + \begin{matrix}0\\1\\1\\1\end{matrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$11000000 \Rightarrow \begin{matrix}0\\0\\0\\1\end{matrix} + \begin{matrix}0\\0\\1\\1\end{matrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

Ejercicio 3 Relación Hamming

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**

5º/

GF(5)

$$\begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}$$

Para calcular la mínima distancia vamos a comprobar cuantas columnas son linealmente independientes.

Todas las columnas son linealmente independientes. Por tanto la distancia mínima es $d=3$

6º/

GF(3)

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

Para calcular la mínima distancia, vamos a calcular si alguna columna es linealmente dependiente de otras.

~~Como~~ Analizando cada columna, llegamos a la conclusión de que la columna {2 0 1} es linealmente dependiente. Se obtiene de la suma e la columna {2 2 2} y {0 1 2}.

mo mínimo $d = 3$.

Ejercicio 5 y 6 Relación Hamming

Miguel Santiago Cervilla

Firmado digitalmente por Miguel Santiago Cervilla
Fecha: 2018.11.28 22:08:57 +01'00'

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Grado Ingeniería Informática Curso **2018/19**