TINF

Apuntes de clase

Apuntes y exámenes ETSIT UPM

Si alguna vez estos apuntes te sirvieron de ayuda, piensa que tus apuntes pueden ayudar a muchas otras personas.

Comparte tus apuntes en simplyjarod.com

① ENTROPÍA

1. Incertidumbre y Entropía

Entropía = Incertidumbre = $H(X)$

$$H(X) = \sum_{\forall x \in X} p(x) \cdot \log_2\left(\frac{1}{p(x)}\right) \quad ; \quad H(X) \geq 0$$

Entropía conjunta = $H(X,Y)$

$$H(X,Y) = \sum_{\forall x \in X} \sum_{\forall y \in Y} p(x,y) \cdot \log_2\left(\frac{1}{p(x,y)}\right)$$

Entropía condicionada = $H(Y/X)$

$$H(Y/X) = \sum_{\forall x \in X} p(x) \cdot H(Y/X=x) = \sum_{\forall x \in X} \sum_{\forall y \in Y} p(x,y) \cdot \log_2\left(\frac{1}{p(y/x)}\right)$$

si X e Y son independientes: $H(Y/X) = H(Y)$

Regla de la cadena:

$$H(X,Y) = H(Y,X) = H(X) + H(Y/X) = H(Y) + H(X/Y)$$

si X e Y son independientes: $H(X,Y) = H(X) + H(Y)$

$$H(X,Y/Z) = H(X/Z) + H(Y/X,Z)$$

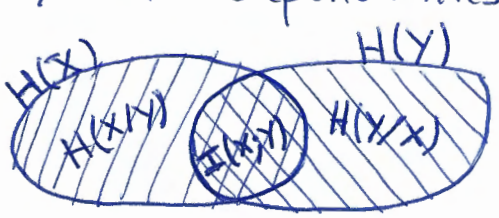
2. Información mutua

$$I(X;Y) = I(Y;X) = H(X) - H(X/Y) = H(Y) - H(Y/X)$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

$$I(X;X) = H(X)$$

si X e Y son independientes: $H(X/Y) = H(X) \Rightarrow I(X,Y) = 0$



Entropía relativa o diferencial

Medida de "distancia" entre dos distribuciones de probabilidad de una misma variable aleatoria

- $D(p \| q) = \sum_{\forall x \in \mathcal{X}} p(x) \cdot \log_2\left(\frac{p(x)}{q(x)}\right)$; $D(p\|q) \geq 0$

  $D(p\|q) = 0 \Leftrightarrow p(x) = q(x)$

  $D(p\|q) \neq D(q\|p)$

"distancia" = ineficiencia de asumir que la distribución correcta es q cuando en realidad es p.

- $I(X;Y) = D(p(x,y) \| p(x) \cdot p(y))$

3. Reglas de la cadena para n variables

$$H(X_1, X_2, X_3, \dots, X_n) = \sum_{i-1}^{n} H(X_i / X_{i-1}, \dots, X_1)$$

↳ $H(X_1, X_2, X_3) = H(X_1) + H(X_2/X_1) + H(X_3 / X_2, X_1)$

$$H(X_1, \dots X_n / Y) = \sum_{i-1}^{n} H(X_i / X_{i-1}, \dots X_1, Y)$$

$$I(X_1, \dots X_n ; Y) = \sum_{i-1}^{n} I(X_i ; Y / X_{i-1}, \dots, X_1)$$

$$D(p(y/x) \| q(y/x)) = \sum_{\forall x} p(x) \sum_{\forall y} p(y/x) \cdot \log_2\left(\frac{p(y/x)}{q(y/x)}\right)$$

$$D(p(x,y) \| q(x,y)) = D(p(x) \| q(x)) + D(p(y/x) \| q(y/x))$$

4. Desigualdad de Jensen

sea $f(x)$ cóncava: $E[f(x)] \geq f(E[x])$

si $f(x)$ convexa: $\leq$

$D(p(x) \| q(x)) \geq 0$

- $I(X;Y) = D(p(x,y) \| q(x,y)) \geq 0$
- $H(X) \leq \log_2(|\mathcal{X}|)$; $|\mathcal{X}|$ = nº elementos en el rango de X

  " = " $\Leftrightarrow$ X tiene una distribución uniforme

En promedio:

$$H(X/Y) = \sum_y p(y) \cdot H(X/Y=y) \leq H(X)$$

$$H(X_1, X_2, \dots, X_n) = \sum_{i=1}^{n} H(X_i / X_{i-1}, X_{i-2}, \dots, X_1) \leq \sum_{i=1}^{n} H(X_i)$$

5. Teorema del proceso de información

$$I(X;Y) \geq I(X;Z) \quad ; \quad Z = f(Y)$$

Nunca una manipulación más inteligente de los datos va a mejorar la información mutua entre las v.a.

si $X \to Y \to Z$ tienen una relación markoviana:

$$\begin{cases} I(X; Y/Z) \leq I(X;Y) \\ I(X; Z/Y) = 0 \end{cases}$$

② MARKOV

1. Modelos markovianos de fuentes

La equipartición asintótica establece que bastan $n \cdot H(X)$ bits para describir n v.a. independientes.

Proceso Estocástico = Secuencia de v.a. indexadas por t

Proceso Estocástico Estacionario: invariante al trasladar el origen de tiempos

Proceso con memoria limitada (de Markov de orden m):
↳ sólo los m valores anteriores del proceso tienen influencia en el siguiente valor

proceso markoviano de orden 1: su pasado no importa si sabemos el presente

↳ $P\{X_n = x_n / X_1, X_2, \dots X_{n-1}\} = P\{X_n = x_n / X_{n-1}\}$

cadena estocástica = proceso estocástico sobre un espacio muestral discreto

cadena de markov de orden m = proceso de Markov de orden m sobre un $\mathcal{X}$ discreto

cadena de markov homogénea = probab. de transición estacionarias
$(p\{X_{L+1}=j / X_L=i\} = P\{X_2=j / X_1=i\})$

matriz Π: $p_{ij} = P\{X_{n+1}=j / X_n=i\}$

$\mu^{n+1} = \mu^n \cdot \Pi$; $\mu^n = \mu^1 \cdot [\Pi]^{n-1}$

probabilidad de cambiar del estado i al j en n saltos: $P_{ij}^{(n)}$

probab. de estar en el mismo estado i tras n saltos: $P_{ii}^{(n)}$

- un estado i será periódico de periodo L si $P_{ii}^{(n)} = 0 \; ; \; n \neq L$
- una cadena será periódica si todos los estados tienen mismo L
- un estado es transitorio si tras pasar por él X veces no se vuelve a pasar por ese estado nunca más
- si ningún estado es transitorio $\Rightarrow$ la cadena será irreducible

[si cadena homogénea, aperiódica e irreducible:

↳ $\exists \vec{\mu}^A \; ; \; \vec{\mu}^A = \vec{\mu}^A \cdot \Pi$

si $\vec{\mu}^n = \vec{\mu}^A \Rightarrow \vec{\mu}^{n+1} = \vec{\mu}^A$ } $\vec{\mu}^{n+L} = \vec{\mu}^A \quad \forall L$

2. Tasa de Entropía

Tasa de Entropía = $H(\mathcal{X})$ = tasa de crecimiento de la entropía conjunta

$$H(\mathcal{X}) = \lim_{n\to\infty} \frac{1}{n} H(X_1, X_2, \ldots, X_n)$$

$$H'(\mathcal{X}) = \lim_{n\to\infty} H(X_n / X_{n-1}, X_{n-2}, \ldots X_1)$$

} en proc. estacionarios $H(\mathcal{X}) = H'(\mathcal{X})$

en una cadena de Markov de orden 1 estacionaria:

$$H(\mathcal{X}) = \sum_i \mu_i \cdot H(\text{fila } i \text{ de } \Pi)$$

③ COMPRESIÓN

1. Tipos de Códigos

La entropía establece el límite inferior de bits/símbolo necesarios para codificar una fuente.

→ **Código Bloque**: asigna una secuencia fija de símbolos del alfabeto código a cada palabra fuente

→ **Código No Singular**: cada palabra fuente tiene una palabra código diferente.

→ **Código unívocamente descodificable**: su extensión es No sing.

extensión: concatenación de palabras

$$\left.\begin{array}{l} x_1 \xrightarrow{C(\cdot)} C(x_1) \\ x_2 \xrightarrow{C(\cdot)} C(x_2) \end{array}\right\} \xrightarrow{\text{extensión}} x_1 \cdot x_2 \xrightarrow{C(\cdot)} C(x_1 \cdot x_2) = C(x_1) \cdot C(x_2)$$

→ **Código prefijo (o instantáneo)**: no existe palabra código que sea prefijo de otra.

$$\text{código prefijo} \in \text{código unívoc. descodif.} \in \text{código NO singular}$$

2. Desigualdad de Kraft

código prefijo sobre alfabeto D-ario: $\sum_i D^{-l_i} \leq 1$

- **Teorema de McMillan**:

  cualquier código unívocamente descodificable debe cumplir la desigualdad de Kraft

3. Códigos óptimos : 1er + 1ma Shannon

código prefijo óptimo: minimiza la longitud media de las palabras código

$$\text{longitud media} = L = \sum_i p_i \cdot l_i$$

$$L_{\substack{\text{mínima}\\\text{matemática}}} = \sum_i p_i \cdot \log_D\left(\frac{1}{p_i}\right) = H_D(X)$$

como l_i debe ser un número entero:

$$L_{\substack{\text{mínima}\\\text{posible}}} = \sum_i p_i \cdot \underbrace{\left\lceil \log_D\left(\frac{1}{p_i}\right)\right\rceil}_{l_i} \geq H_D(X) \quad ; \quad L = H_D(X) \Leftrightarrow p_i = D^{-l_i}$$

$$l_i = \left\lceil \log_D\left(\frac{1}{p_i}\right)\right\rceil$$

$$\Downarrow$$

Shannon: $\quad H_D(X) \leq L \leq H_D(X) + 1$

4. Fuentes sin memoria

a) Codificación Huffman: (binaria)

Sea: $\mathcal{X} = \{A, B, C, D, E, F\}$ y $p(x) = \{0{,}15 , 0{,}26, 0{,}09 , 0{,}25 , 0{,}11 , 0{,}14\}$

X	p(x)	p'(x)	p''(x)	p'''(x)	p''''(x)	C(x)
B	0'26 →	0'26 →	0'29 →	0'45 →	0'55 |0	01
D	0'25 →	0'25 →	0'26 →	0'29 |0	0'45 |1	10
A	0'15 →	0'2 →	0'25 |0	0'26 |1		000
F	0'14 →	0'15 |0	0'2 |1			001
E	0'11 |0	0'14 |1				110
C	0'09 |1					111

es prefijo y óptimo

→ ordenación decreciente de p(x)
→ asignación de '0' y '1' a los menos probables
→ sumar las 2 p(x) más bajas y reordenar p'(x)
→ seguir el camino de derecha a izquierda para obtener el código

b) Ensayo de Sardinas - Patterson:

Sea C el conjunto de todas las palabras código del código a probar

Definimos $C_0 = C$

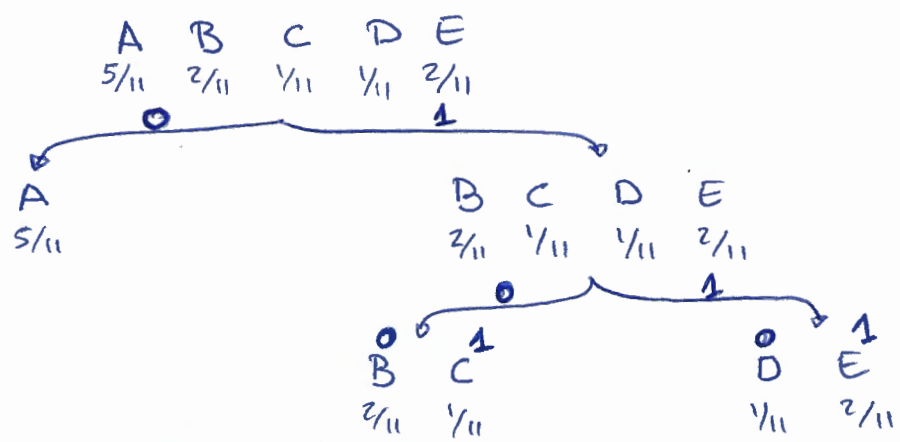
para $n > 0$ definimos:

$$C_n = \{ w \in X^* / uw = v \text{ con } u \in C,\ v \in C_{n-1} \}$$

$$C_\infty = C_1 \cup C_2 \cup C_3 \cup \dots$$

C será unívocamente descodificable si C y C_∞ son disjuntos

c) Código alfabético de Fano:



A = 0
B = 100
C = 101
D = 110
E = 111

→ se divide en dos grupos, siendo las probabilidades acumuladas de cada grupo lo más próximas posibles

d) Código de Shannon - Elías - Fano:

x	p(x)	F(x)	$\tilde{F}(x)$	$\tilde{F}(x)$ binario	l(x)	c(x)
A	0'25	0'25	0'125	0,001	3	001
B	0'5	0'75	0'5	0, 10	2	10
C	0'125	0'875	0'8125	0, 1101	4	1101
D	0'125	1	0'9375	0, 1111	4	1111

$$\tilde{F}(x) = \sum_{t<x} p(t) + \frac{1}{2} p(x)$$

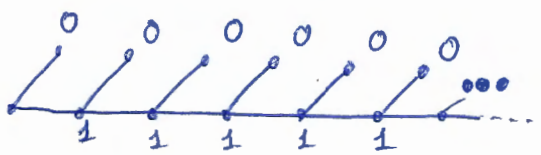
$$l(x) = \left\lceil \log_b \left(\frac{1}{p(x)} \right) \right\rceil + 1 \quad \Rightarrow \quad L < H(X) + 2$$

5. Fuentes con memoria

Codificación Run-Length (fuentes infinitas)

la fuente genera el mismo simbolo de forma repetida con elevada probabilidad.

construcción del código prefijo:

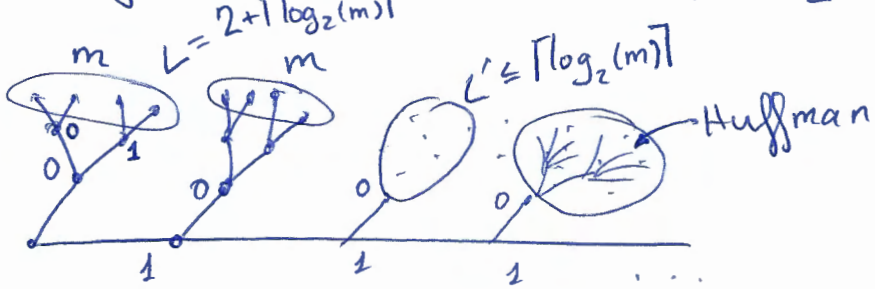


x	p(x)	c(x)	l(x)
1	1/2	0	1
2	1/4	10	2
3	1/8	110	3
4	1/16	1110	4
5	1/32	11110	5
⋮	⋮	⋮	⋮

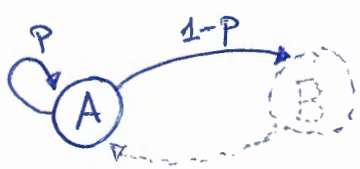
$$L = \sum \frac{1}{2^i} \cdot i = 2 = H(X)$$

↑ óptimo

codificación de $G(p)$ con $p^m = \frac{1}{2}$



Aplicación:



$(p \gg 1-p)$

genera secuencias de longitud ℓ

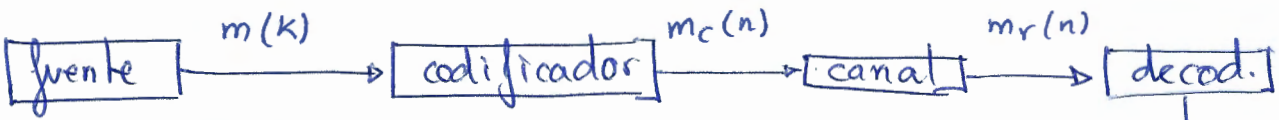
$$L = \frac{1}{1-p} \Rightarrow p = \frac{L-1}{L}$$

codificaremos buscando $p^m \approx \frac{1}{2}$

Códigos de Protección Contra Errores

- → códigos lineales
- → códigos cíclicos

situación de partida:



$m(K)$: mensaje generado por la fuente de longitud k

$m_c(n)$: mensaje codificado

$m_r(n)$: mensaje recuperado después de la transmisión

$\hat{m}(K)$: mensaje recuperado y decodificado (listo para la aplicación)

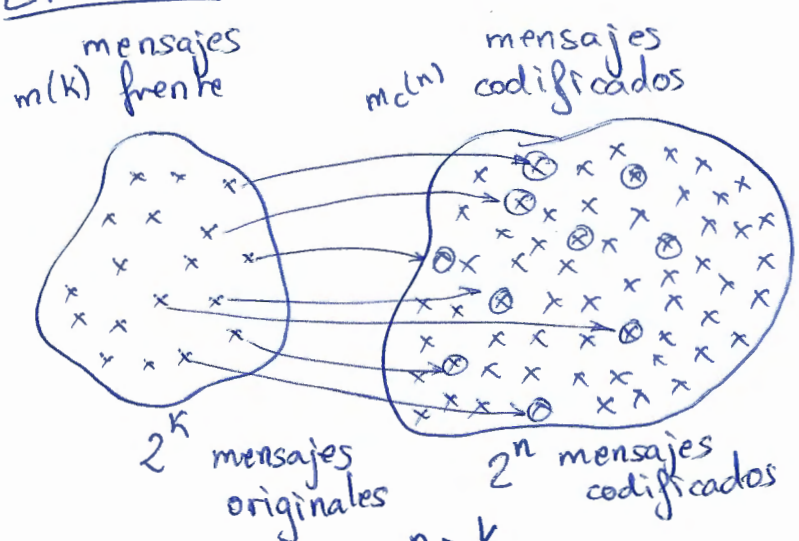
Teorema de Codificación de Canal:

siempre que: $\frac{K}{n} < C$; C = Capacidad del canal

se puede llegar a: $P(\hat{m}(K) \neq m(K)) < \varepsilon$; $\varepsilon \downarrow\downarrow$

↳ la probabilidad de que el mensaje recuperado y decodificado difiera del original sea pequeña

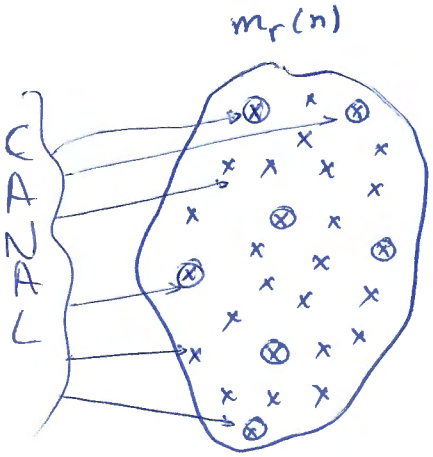
EMISOR:



Deberemos elegir 2^K mensajes codificados y asignar a cada mensaje original un mensaje codificado

RECEPTOR:

Por ruido, interferencias... es posible recibir un mensaje diferente al original



En el momento que recibamos un mensaje de los NO escogidos, habremos detectado un error introducido en el mensaje por el canal. Quizás podamos corregirlo.

El peor caso sería recibir una palabra perteneciente al código pero diferente a la original. En ese caso tenemos un error indetectable.

Algebra binaria:

Partiendo de la base de que tenemos un alfabeto binario $\Rightarrow \{0,1\}$ definimos:

SUMA:

+	0	1
0	0	1
1	1	0

PROD:

·	0	1
0	0	0
1	0	1

$\{0,1\}$ es un cuerpo de Galois: $GF(2)$ [Galois Field]

Sea G un conjunto de elementos.

G es grupo si y sólo si:

- → tiene definida una operación binaria $*$
- → $*$ es asociativa: $(a * (b * c) = (a * b) * c)$
- → $\exists e \in G \; ; \; \forall a \in G \Rightarrow a * e = e * a = a$
- → $\forall a \in G, \; \exists a' \in G \Rightarrow a * a' = e$

G es un grupo conmutativo si:

→ es grupo y $\forall a, b \in G$, $a * b = b * a$

Sea F un conjunto de elementos con dos operaciones definidas: + y ·

F es cuerpo si y sólo si:

→ F es grupo conmutativo bajo la operación +

→ El conjunto de elementos $\neq 0$ de F es grupo conmutativo bajo la operación ·

→ $a \cdot (b+c) = a \cdot b + a \cdot c$

Si el alfabeto es finito, se denomina Cuerpo de Galois de dimensión n ; n = nº de elementos del alfabeto

Luego: $\{0, 1\}$ es un Cuerpo de Galois de dimensión 2

Propiedades de los CG(n):

→ El conjunto V_n formado por todas las tuplas

$\vec{v} = (v_1, v_2, \ldots, v_n)$ $v_i \in GF(2)$

junto con las operaciones: $\begin{cases} +: \vec{v} = \vec{u} + \vec{w} \; ; \; v_i = u_i + w_i \\ \cdot: \lambda \cdot \vec{u} = \vec{w} \; ; \; w_i = \lambda \cdot u_i \end{cases}$

es un espacio vectorial sobre GF(2)

↳ el número de elementos de V_n es 2^n

↳ la dimensión de V_n es n

→ $S \subseteq V_n$ es subespacio vectorial si y sólo si:

- elemento neutro $\in S$
- $\forall \vec{u}, \vec{v} \in S \Rightarrow \vec{u} + \vec{v} \in S$
- Si $\vec{u} \in S \Rightarrow \lambda \cdot \vec{u} \in S$

→ Dado un conjunto de vectores $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n$ se dice que son linealmente independientes si:

$$\forall c_i \Rightarrow c_1\vec{v}_1 + c_2\vec{v}_2 + \dots + c_n\vec{v}_n \neq 0$$

excepto $c_1 = c_2 = \dots = c_n = 0$

→ El conjunto $\{\vec{g}_1, \vec{g}_2, \dots, \vec{g}_n\}$ genera el espacio V_n si:

$$\forall \vec{v} \in V_n \Rightarrow \vec{v} = \sum_{i=1}^{n} c_i \vec{g}_i$$

→ En todo V_n, $\exists \{\vec{g}_1, \dots, \vec{g}_n\} \subseteq V_n$ linealmente independientes que generan V_n:
su cardinal es la dimensión de V_n

→ Si $k < n$ y $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k\} \subseteq V_n$ son linealmente independientes entonces:

$S = \{\vec{u}\,;\, \vec{u} = \sum_{i=1}^{k} c_i \cdot \vec{v}_i\}$ es subespacio vectorial de dimensión k

→ Se define la operación producto interior:

$$\vec{u} \cdot \vec{v} = u_1 v_1 + u_2 v_2 + \dots + u_n v_n$$

→ Se dice que dos vectores son ortogonales si

$$\vec{u} \cdot \vec{v} = 0$$

→ Sea S un subespacio vectorial de dimensión k de V_n
Sea S_d el conjunto de vectores $\subseteq V_n$; $\forall \vec{u} \in S$, $\forall \vec{v} \in S_d$

entonces: $\vec{u} \cdot \vec{v} = 0 \Rightarrow S_d$ es subespacio dual de S de dimensión $(n-k)$

Clasificación de códigos:

- Lineal
  - Bloque
    - cíclico / No cíclico
    - sistemáticos / No sistemáticos
  - convolucionales
- No lineal

Códigos Lineales

Para codificar necesitamos:

- ↳ elegir el conjunto de palabras código (subespacios vectoriales)
- ↳ asignación de palabra fuente a palabra código

Un código de longitud n y 2^k palabras código, es lineal $C(n,k)$ si sus 2^k palabras código forman un subespacio vect. de dimensión k del espacio vectorial V_n sobre $GF(2)$

Ej: $C(7,4) \Rightarrow k=4,\ n=7$

palabras fuente ($k=4$)		palabras código ($n=7$)	
0000	1000	0000000	1101000
0001	1001	1010001	0111001
0010	1010	1110010	0011010
0011	1011	0100011	1001011
0100	1100	0110100	1011100
0101	1101	1100101	0001101
0110	1110	1000110	0101110
0111	1111	0010111	1111111

Matriz G = Matriz Generadora (del código lineal)

Como $C(n,k)$ es un subespacio vectorial de dimensión k entonces: $\exists$ k vectores linealmente independientes $\{\vec{g}_0, \vec{g}_1, \dots \vec{g}_{k-1}\}$ con $\vec{g}_i \in C$ donde $\forall \vec{v} \in C$: $\vec{v} = u_0\vec{g}_0 + u_1\vec{g}_1 + \dots + u_{k-1}\vec{g}_{k-1}$

$$\boxed{\vec{v} = \vec{u} \cdot G}$$

$$(v_0, v_1, v_2 \dots v_{n-1}) = (u_0, u_1, \dots u_{k-1}) \begin{pmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix} \begin{matrix} \leftarrow \vec{g}_0 \\ \leftarrow \vec{g}_1 \\ \\ \\ \leftarrow \vec{g}_{k-1} \end{matrix}$$

Dado un $\vec{u}$ (fuente) será codificado como $\vec{v}$ (código)

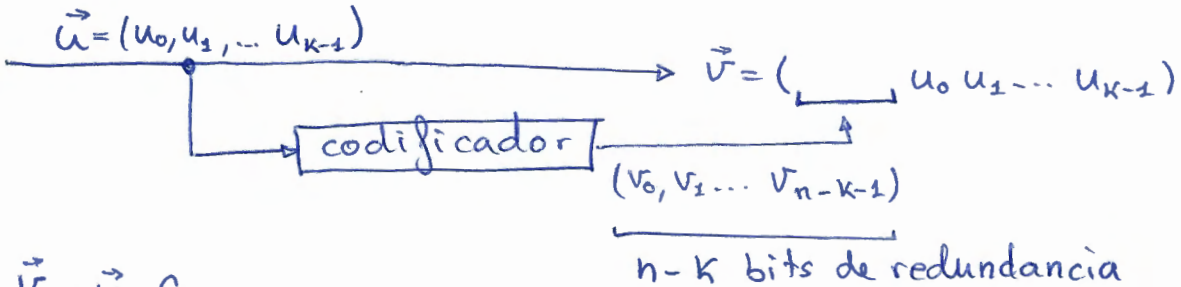
Ej: para el ejemplo anterior, cogemos $k=4$ vectores linealmente independientes:

$$G = \begin{pmatrix} 1\,1\,0 & 1\,0\,0\,0 \\ 0\,1\,1 & 0\,1\,0\,0 \\ 1\,1\,1 & 0\,0\,1\,0 \\ 1\,0\,1 & 0\,0\,0\,1 \end{pmatrix} \quad ; \quad \vec{V} = \vec{u} \cdot G$$

por ejemplo: $\vec{u} = 0101 \Rightarrow \vec{V} = 1100101$

Estructuración sistemática

Escogiendo la matriz G de modo que a su derecha quede una submatriz identidad, obtendremos una palabra código $\vec{v}$ que contendrá los mismos bits que $\vec{u}$ en sus últimas posiciones (muy útil en la práctica)



$$\vec{V} = \vec{u} \cdot G$$

$$G = \begin{pmatrix} \vec{g}_0 \\ \vec{g}_1 \\ \vdots \\ \vec{g}_{k-1} \end{pmatrix} = \begin{pmatrix} p_{00}\ p_{01} \dots p_{0\,n-k-1} & 1\,0\,0 \dots 0 \\ p_{10}\ p_{11} \dots p_{1\,n-k-1} & 0\,1\,0 \dots 0 \\ \vdots & \\ p_{k-1,0}\ p_{k-1,1} \dots p_{k-1,n-k-1} & 0\,0\,0 \dots 1 \end{pmatrix} = (P \,|\, I_k)$$

Ej: Código paridad simple: $C(6,5)$: añade { 1 si nº impar de "1" ; 0 si nº par de "1" }

G será de tamaño:
6 columnas
5 filas

$$G = (P \,|\, I_k) = \begin{pmatrix} 1 & 1\,0\,0\,0\,0 \\ 1 & 0\,1\,0\,0\,0 \\ 1 & 0\,0\,1\,0\,0 \\ 1 & 0\,0\,0\,1\,0 \\ 1 & 0\,0\,0\,0\,1 \end{pmatrix}$$

si añadimos { 1 si nº par de "1" ; 0 si nº impar de "1" } imposible $\Rightarrow$ No lineal

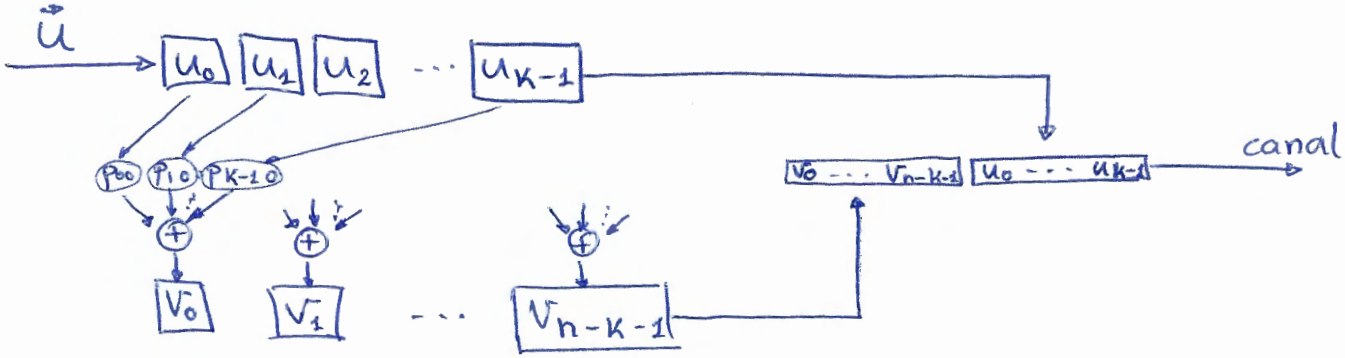
Ej: Ecuaciones de comprobación:

si $G(7,4) \Rightarrow G = \left(\begin{array}{c|ccc} 110 & 1000 \\ 011 & 0100 \\ 111 & 0010 \\ 101 & 0001 \end{array}\right)$

$\vec{v} = \vec{u} \cdot G \Rightarrow (v_0\, v_1\, v_2\, v_3\, v_4\, v_5\, v_6) = (u_0\, u_1\, u_2\, u_3) \cdot G$

$$\begin{cases} v_0 = u_0 + u_2 + u_3 \\ v_1 = u_0 + u_1 + u_2 \\ v_2 = u_1 + u_2 + u_3 \end{cases} \qquad \begin{array}{l} v_3 = u_0 \\ v_4 = u_1 \\ v_5 = u_2 \\ v_6 = u_3 \end{array}$$

Diseño del codificador:



Matriz H: Matriz de comprobación de paridad

$\vec{u}$ → codif. → $\vec{v}$ → canal → $\vec{r}$ → ¿$\vec{r} \in G$?

Para toda matriz $G_{K \times n}$ con K filas linealmente independientes

$\exists$ H de dimensión $(n-K) \times n$ con $n-K$ filas lin. indep. que cumple:

- ↳ cualquier vector generado por las filas de G es ortogonal a las filas de H
- ↳ cualquier vector ortogonal a las filas de H es generado por las filas de G

$$\boxed{\vec{r} \cdot H^t = 0 \iff \vec{r} \in G}$$

La matriz generadora H genera un código llamado código dual de G (C_d); $C_d(n, n-k)$

$$\left.\begin{array}{l}\forall \vec{v} \in C \\ \forall \vec{w} \in C_d\end{array}\right\} \Rightarrow \vec{v} \cdot \vec{w} = 0$$

Cálculo de H:

partiendo de la $G_{sistemática}$: $G_{sist} = (P \,|\, I_k)$

$$H = (I_{n-k} \,|\, P^t)$$

Ej $C(7,4) \longrightarrow G = \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1000 \\ 0 & 1 & 1 & 0100 \\ 1 & 1 & 1 & 0010 \\ 1 & 0 & 1 & 0001 \end{array}\right) \leftarrow \vec{g}_3$

$P \qquad I_4$

$\Downarrow$

$$H = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1011 \\ 0 & 1 & 0 & 1110 \\ 0 & 0 & 1 & 0111 \end{array}\right) \leftarrow \vec{h}_3$$

$I_3 \qquad P^t$

$$\vec{g}_3 \cdot \vec{h}_3 = g_3 + h_3 = 1 + 1 = 0$$

Síndrome:

$$\xrightarrow{\vec{u}} \text{codif.} \xrightarrow{\vec{v}} \text{canal} \xrightarrow{\vec{r}} \text{decod.}$$

$$\vec{r} \Rightarrow \vec{r} \cdot H^t = \begin{cases} = \vec{0} \Rightarrow \begin{cases} \text{sin error} \\ \text{error indetectable} \end{cases} \\ \neq \vec{0} \Longrightarrow \text{error en el canal} \end{cases}$$

vector síndrome $= \vec{s} = \vec{r} \cdot H^t$

vector error $= \vec{e} \Rightarrow \vec{r} = \vec{v} + \vec{e}$

$$\vec{s} = \vec{r} \cdot H^t = (\vec{v} + \vec{e}) \cdot H^t = \vec{v} \cdot H^t + \vec{e} \cdot H^t = \vec{0} + \vec{e} \cdot H^t$$

$$\vec{s} = \vec{e} \cdot H^t = \begin{cases} = \vec{0} \begin{cases} \text{NO error} \Rightarrow \vec{e} = 0 \\ \text{error indetectable} \Rightarrow \vec{e} \in C \end{cases} \\ \neq \vec{0} : \text{error en canal} \end{cases}$$

serán más probables los errores con sólo 1 único "1" que con muchos "1":

Ecuaciones de comprobación:

$$\vec{S} = \vec{r} \cdot H^t$$

$$\begin{cases} S_0 = r_0 + r_{n-k} \cdot p_{00} + r_{n-k+1} p_{10} + \dots + r_{n-1} \cdot p_{k-1,0} \\ S_1 = \\ \vdots \\ S_{n-k-1} = r_{n-k-1} + r_{n-k} \cdot p_{0,n-k-1} + \dots + r_{n-1} \cdot p_{k-1,n-k-1} \end{cases}$$

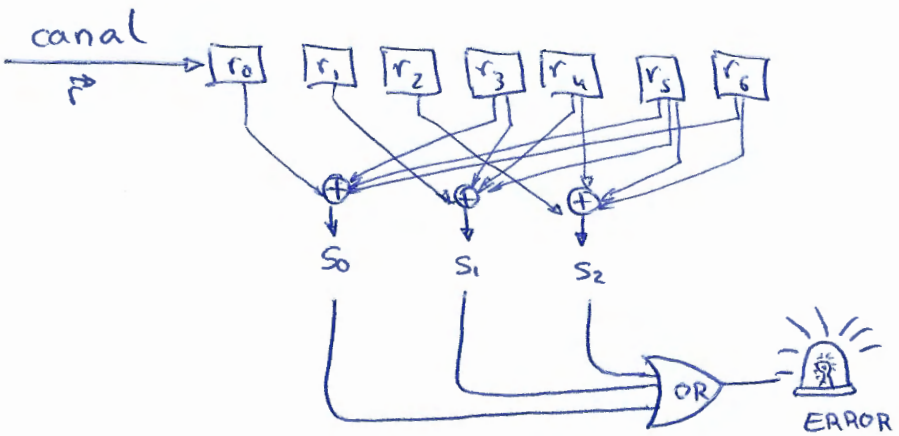
Ej $G(7,4)$

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

$$\vec{S} = \vec{r} \cdot H^t = (r_0\, r_1\, r_2\, r_3\, r_4\, r_5\, r_6) \begin{pmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \\ 1\,1\,0 \\ 0\,1\,1 \\ 1\,1\,1 \\ 1\,0\,1 \end{pmatrix}$$

$$\begin{cases} S_0 = r_0 + r_3 + r_5 + r_6 \\ S_1 = r_1 + r_3 + r_4 + r_5 \\ S_2 = r_2 + r_4 + r_5 + r_6 \end{cases}$$

Diseño del decodificador:



Si el síndrome no es nulo, podremos intentar despejar $\vec{e}$ de $\vec{S}_1 = \vec{e} \cdot H^t$, siendo $\vec{S}_1, \vec{S}_2$ los vectores de diferentes errores. Lo malo es que en el sistema obtenemos más incógnitas que ecuaciones.

Ej $\vec{v} = (1001011)$, $\vec{r} = (1001001)$

$$\vec{s} = \vec{r} \cdot H^t = (1001001) \cdot \begin{pmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 101 \end{pmatrix} = (111) \Rightarrow \text{ERROR}$$

$$\left.\begin{aligned} 1 &= e_0 + e_3 + e_5 + e_6 \\ 1 &= e_1 + e_3 + e_4 + e_5 \\ 1 &= e_2 + e_4 + e_5 + e_6 \end{aligned}\right\} \text{ 3ec. 7incóg.} \Rightarrow \exists\, 2^4 = 16 \text{ soluciones}$$

por ejemplo:

$\vec{e}_1 = (0000010)$

$\vec{e}_2 = (1101010)$

$\vec{e}_3 = (0110110)$

Si quiero corregir el error (para lo cual necesito $\vec{e}$) deberé decantarme por un $\vec{e}$ de las posibles soluciones. Teniendo en cuenta que es más fácil cambiar (meter error) en 1 único bit antes que en muchos bits, la probabilidad de sucederse una de las soluciones del error con menor número de bits es mayor. Luego, si quiero decantarme por un vector de error, escogeré el que tenga menor número de "1", pues será el más probable de sucederse.

Distancia mínima:

sea $\vec{v} = (v_0\ v_1 \dots v_{n-1})$

Peso de Hamming de $\vec{v} \Rightarrow w(\vec{v}) \Rightarrow$ Nº de "1" de $\vec{v}$

p.ej. $w(1010110) = 4$

Distancia de Hamming entre $\vec{u}$ y $\vec{v} \Rightarrow d(\vec{u}, \vec{v}) \Rightarrow$ Nº de componentes diferentes

p.ej $d((1011011), (1010101)) = 3$

se cumple la desigualdad triangular:

$$d(\vec{u}, \vec{v}) + d(\vec{v}, \vec{w}) \geq d(\vec{u}, \vec{w})$$

sabiendo que: $a + b = \begin{cases} 0 \Leftrightarrow a = b \\ 1 \Leftrightarrow a \neq b \end{cases}$

$$d(\vec{u}, \vec{v}) = w(\vec{u} + \vec{v})$$

Dado un código $C(n,k)$, se define la distancia mínima:

$$d_{min} = \min \{ d(\vec{v},\vec{w}) ; \vec{v},\vec{w} \in C, \vec{v} \neq \vec{w} \}$$

$$d_{min} = \min \{ w(\vec{v}+\vec{w}) ; \vec{v},\vec{w} \in C, \vec{v} \neq \vec{w} \}$$

como $\vec{v},\vec{w} \in C \Rightarrow \vec{v}+\vec{w} \in C$

$$d_{min} = \min \{ w(\vec{x}) ; \vec{x} \in C ; \vec{x} \neq \vec{0} \}$$

Cálculo de d_{min}:

$$\forall \vec{v} \in C \Rightarrow \vec{v} \cdot H^t = 0$$

- Dado $C(n,k)$ con matriz de paridad H, para cada palabra código con peso l $\exists$ l columnas de H que suman 0
  $\exists$ l filas de H^t que suman 0
- Si $\exists$ l columnas de H que suman 0 $\Rightarrow \exists$ palabra código con peso l
- Si C es código lineal con H como matriz de paridad entonces si $\nexists (d-1)$ o menor nº de columnas de H que suman 0 $\Rightarrow d_{min} \geq d$
- Si tenemos $C(n,k)$ con H como matriz de paridad:
  entonces: d_{min} = menor nº de columnas de H que suman 0.

Ej:

$d_{min} = 1 \Rightarrow$ hay una columna nula ($\vec{0}$)

$d_{min} = 2 \Rightarrow$ hay dos palabras iguales

$d_{min} = 3 \Rightarrow \exists\ h_i + h_j + h_k = 0,\ i \neq j \neq k$

Capacidad de Detección:

Peso máximo de errores que son siempre detectados.

$s = d_{min} - 1$ = capacidad de detección

$\vec{V}$ → canal → $\vec{r}$

$\vec{e}$ ↑ ⟷ si $\begin{cases} w(\vec{e}) < d_{min} \Rightarrow \text{siempre detecto} \\ w(\vec{e}) \geq d_{min} \Rightarrow \text{a veces detecto} \end{cases}$

↳ $2^K - 1$ errores indetectables

Probabilidad de error en detección:

Probabilidad de No Detección: $P_{ND} = P(\vec{e} \in C)$, $\vec{e} \neq \vec{0}$

$$P_{ND} = p(\vec{e} = \vec{v}_1) + p(\vec{e} = \vec{v}_2) + \dots + p(\vec{e} = \vec{v}_{2^K-1})$$

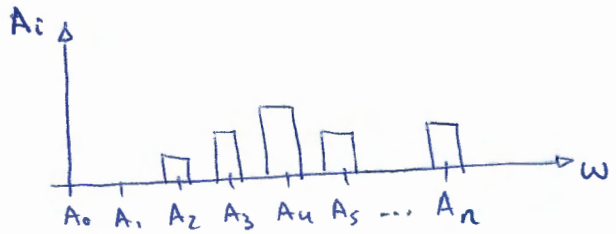
Ej: si $\vec{V} = (0110011)$ canal con probabilidad de error de bit = p

$$p(\vec{e} = (0110011)) = (1-p)^3 \cdot p^4$$

p^4 ↳ 4×"1" que han de cambiar

$(1-p)^3$ ↳ 3×"0" no cambian

Distribución de pesos de las palabras código:



Ej: $C(7,4)$:

$A_0 = 1$	$A_4 = 7$
$A_1 = 0$	$A_5 = 0$
$A_2 = 0$	$A_6 = 0$
$A_3 = 7$	$A_7 = 1$

$$P_{ND} = \sum_{i=0}^{n} A_i \cdot p^i (1-p)^{n-i}$$

realmente $\sum_{d_{min}}^{n}$ pues $i < d_{min}$ se detecta

$$P_{ND} = A_3 \cdot p^3 (1-p)^4 + A_4 p^4 (1-p)^3 + A_7 p^7 = 7 p^3 (1-p)^4 + 7 p^4 (1-p)^3 + p^7$$

Ej: $G(15,11)$ con $d_{min} = 3$

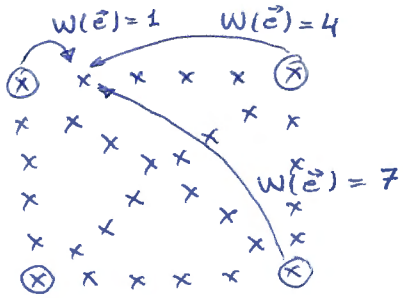
$A_5 \leq \binom{15}{5}$

↳ Nº de palabras de 15 bits con 5 "1"

$$\left[P_{ND} = \sum_{d_{min}}^{n} A_i \, p^i (1-p)^{n-i} \leq \sum_{i=d_{min}}^{n} \binom{n}{i} p^i (1-p)^{n-i} \right]$$

Capacidad de Corrección:

Ej: $d_{min} = 5$



Corregir es decidirse por una palabra código cuando recibimos una palabra que no pertenece al código.

El criterio de decisión será escoger la palabra código más cercana (menor peso del $\bar{e}$)

Capacidad de Corrección = peso máximo de los errores que son siempre corregidos correctamente. $= t$

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$

si corregimos con un peso mayor que t estaremos corrigiendo mal

MLD: Decodificación de Máxima similitud

$\vec{v} \longrightarrow$ canal $\longrightarrow \vec{r} \longrightarrow$ decod $\longrightarrow \hat{\vec{u}}$

Escoger $\hat{\vec{v}} = \vec{v}_i$ que minimice $p(\text{error} / \vec{r}) \Leftrightarrow$ minimizar $p\left(\hat{\vec{v}} \neq \vec{v} / \vec{r}\right)$

Escoger $\hat{\vec{v}} = \vec{v}_i$ { que maximice $p(\vec{e}_i)$ · que minimice $w(\vec{e}_i)$ que minimice $d(\vec{v}_i, \vec{r})$

- Sea $C(n,k)$ con d_{min}

  Sea $t \Rightarrow 2t+1 \leq d_{min} \leq 2t+2$

  Entonces: El código $C(n,k)$ es capaz de corregir todos los patrones de error con t o menos errores

- El código no es capaz de corregir adecuadamente los errores con $w(\vec{e}) > t$

$$P_{\substack{\text{corregir} \\ \text{MAL}}} = p(\vec{e} / w(\vec{e}) > t) \leq \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$$P_{NC} = \text{"}$$

Métodos mixtos:

$$S_{max} = d_{min} - 1$$

$$t_{max} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$

mixto: $d_{min} = s + t + 1$

Ej: $d_{min} = 5$

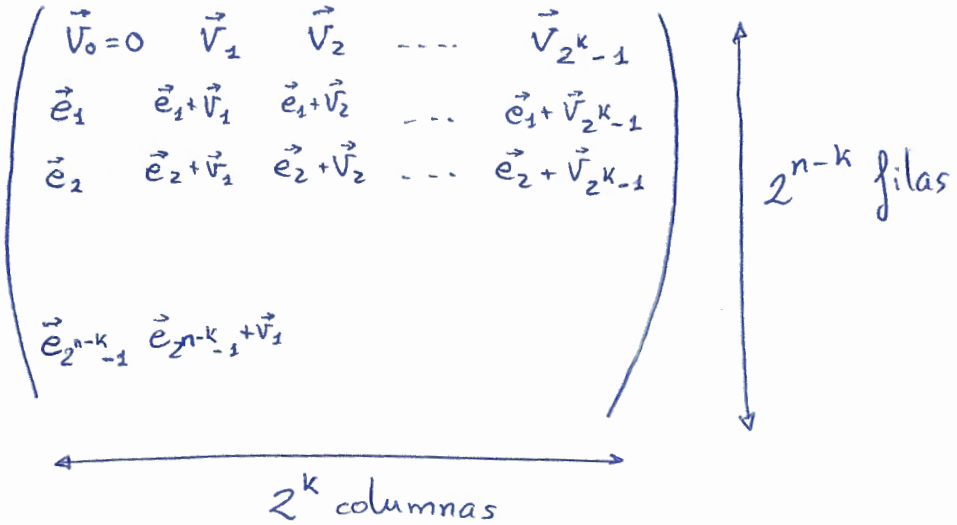
→ detección pura: $s = 4$, $t = 0$

→ mixto: $s = 3$, $t = 1$

→ corrección pura: $s = 2$, $t = 2$

Tabla Estándar: (Array estándar o tabla canónica)

Es una forma de particionar V_n en 2^k particiones



siendo $\vec{e}_1, \vec{e}_2 \dots \vec{e}_{2^{n-k}-1}$ vectores que no hayan sido escogidos anteriormente en toda la tabla.

- En cada fila, todos sus componentes son diferentes.
- Cada componente aparece únicamente en una fila.
- Entonces: todo componente es distinto

  Al ser una tabla $2^{n-k} \times 2^k = 2^n$ elementos únicos

  Luego: la tabla estándar contiene todos los elementos del subespacio V_n

Filas de la tabla = cogrupos (cosets)

1er elemento de cada fila = líder de cogrupo (coset leader)

Particiones = columnas de la tabla estándar

$D_i = \{ \vec{V}_i, \vec{e}_1 + \vec{V}_i, \vec{e}_2 + \vec{V}_i, \dots, \vec{e}_{2^{n-k}-1} + \vec{V}_i \}$

corregiremos identificando la partición y escogiendo la palabra código de la partición

¿Cuándo corregiré bien?

corrijo bien si $\vec{e}$ del canal es líder de cogrupo

Deberemos escoger como líderes de cogrupo los $\vec{e}$ con mayor probabilidad de aparición, es decir, los de menor peso.

- Sea $C(n,k)$ con d_{min}. Todas las n-tuplas de peso $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ o menor pueden ser usadas como líderes de cogrupo.
- Si en la tabla estándar sólo caben como líderes de cogrupo los errores; $w(\vec{e}) \leq t \Rightarrow$ código perfecto

Probabilidad de error de corrección:

Probabilidad de que $\vec{e}$ no sea líder de cogrupo.

Definimos α_i = distribución de pesos de líderes de cogrupo

$$P(\vec{e} \text{ sea líder de cogrupo}) = \sum_{i=0}^{n} \alpha_i \, p^i \, (1-p)^{n-i}$$

Probabilidad de error residual = probabilidad de que el peso del error exceda mis capacidades

Circuito de Corrección:

$\vec{v}$ → canal → $\vec{r}$

↑ $\vec{e}$

- Todas las 2^k n-tuplas de un cogrupo tienen el mismo síndrom

→ Calculo $\vec{s} = \vec{r} \cdot H^t$

→ Tengo tablas con "líder cogrupo" ↔ "síndrome"

→ Saco el $\vec{e}_i$ asociado a $\vec{r}$

→ obtengo $\hat{\vec{v}} = \vec{r} + \vec{e}_i$

Ej: $C(7,4)$ $d_{min} = 3$, $t = 1$

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

tabla estándar ( ) ↕ 8 cogrupos

líder cogrupo $\vec{e}_i$	$\vec{S}_i = \vec{e}_i \cdot H^t$
(0000000)	(000)
(0000001)	(101)
(0000010)	(111)
(0000100)	(011)
(0001000)	(110)
(0010000)	(001)
(0100000)	(010)
(1000000)	(100)

transmito:

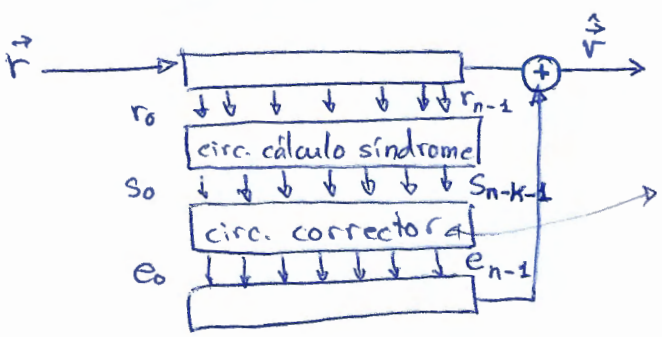
$\vec{v} = (1001011)$

$\vec{r} = (1001111)$

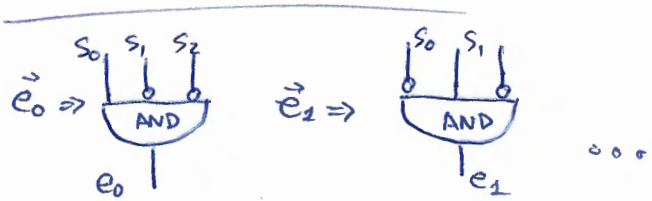
$\vec{s} = \vec{r} \cdot H^t = (011)$

$\vec{e}_i = (0000100)$

$\hat{\vec{v}} = \vec{r} + \vec{e}_i = (1001011)$ 😊



circuito corrector:



Códigos de Hamming:

$\forall m \geq 3$ $\exists$ código de Hamming $\Rightarrow$ $n = 2^m - 1$, $k = 2^m - m - 1$, $n - k = m$ $\Big\}$ $d_{min} = 3$ $\Big\}$ $s_{max} = 2$, $t_{max} = 1$

Ej: $m = 3 \Rightarrow n = 7$, $k = 4 \Rightarrow G(7,4)$
$m = 4 \Rightarrow n = 15$, $k = 11 \Rightarrow G(15,11)$
$m = 5 \Rightarrow n = 31$, $k = 26 \Rightarrow G(31,26)$

Su matriz H será: (todas las posibles m-tuplas como columnas)

(Ej: $n = 3$): $G(7,4)$

$$H = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}}_{\text{Columnas} \Rightarrow 7 \text{ posibles palabras} \neq 0 \text{ de 3 bits}} = (I_{n-k} \,|\, Q) \Rightarrow G = (Q^t \,|\, I_k)$$

En su tabla estándar: líderes de cogrupo $2^m - 1$ errores de peso 1 y ninguno más (código perfecto).

Códigos Cíclicos

Los códigos cíclicos son un subconjunto de los códigos lineales todo código cíclico es lineal.

Rotación cíclica:

Dado $\vec{v} = (v_0, v_1, \dots, v_{n-1})$

se define la operación rotación cíclica sobre $\vec{v}$ obteniendo:

$$\vec{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \dots, v_{n-1}, v_0, v_1, \dots, v_{n-i-1})$$

Ej: $\vec{v} = (1011001)$

$\vec{v}^{(1)} = (1101100)$ $\qquad \vec{v}^{(7)} = \vec{v}$

$\vec{v}^{(2)} = (0110110)$

Un código lineal es cíclico si $\forall \vec{v} \in C(n,k) \Rightarrow \vec{v}^{(i)} \in C(n,k)$

Notación polinomial:

Sea $\vec{v} = (v_0, v_1, v_2 \dots, v_{n-1})$

lo puedo representar como un polinomio con coeficientes v_i:

$$V(x) = v_0 + v_1 \cdot x + v_2 \cdot x^2 + \dots + v_{n-1} \cdot x^{n-1} = \text{polinomio código}$$

Ej: $\vec{v} = (1011001) \Rightarrow V(x) = 1 + x^2 + x^3 + x^6$

Luego: $V^{(i)}(x) = v_{n-i} + v_{n-i+1} x + \dots + v_{n-1} x^{i-1} + v_0 x^i + \dots + v_{n-i-1} x^{n-1}$

si multiplicamos $x^i \cdot V(x)$

$$x^i \cdot V(x) = q(x)(x^n + 1) + V^{(i)}(x) \Rightarrow V^{(i)}(x) = \text{resto}\left(\frac{x^i \cdot V(x)}{x^n + i}\right)$$

Ej: $\vec{v} = (10101) \Rightarrow \vec{v}^{(2)} = (01101)$

$V(x) = 1 + x^2 + x^4$

$V^{(2)}(x) = \text{resto}\left(\frac{x^2 \cdot V(x)}{x^5 + 1}\right)$

$x^2 + x^4 + x^6 \quad \big| \; 1 + x^5$

$+x \qquad\quad +x^6 \qquad\quad x$

$+x + x^2 + x^4 \quad 0$ ← Resto $= x^4 + x^2 + x = V^{(2)}(x)$

¡¡suma en binario!!

$\vec{v}^{(2)} = (01101)$

Ej: grado del polinomio:

$\vec{v} = (1101000) \Rightarrow V(x) = 1 + x + x^3 \Rightarrow$ grado $= 3$

- El polinomio código $\neq 0$ de grado mínimo en un código cíclico es único.

Demonstration:

sea $g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{r-1} x^{r-1} + x^r$ de grado mín $= r$

supongo $\exists\, g'(x) = g'_0 + g'_1 x + \dots + g'_{r-1} x^{r-1} + x^r \in C(n,k)$

entonces $g''(x) = g(x) + g'(x)$ tendrá grado menor que r

luego $g(x)$ no era de grado mínimo $\Rightarrow \nexists\, g'(x) \Rightarrow$

necesariamente el polinomio de grado mínimo es único

- Sea $g(x) = g_0 + g_1 \cdot x + g_2 x^2 + \dots + g_{r-1} x^{r-1} + x^r$ de grado mín.

entonces $g_0 = 1$

(ya que si $g_0 = 0$ podría rotar $g(x)$ y obtener otro con grado menor.

Un polinomio de grado mínimo tendrá la forma:

$$g(x) = 1 + g_1 x + \dots + g_{r-1} x^{r-1} + x^r$$

Dado $g(x)$ (polinomio de grado mínimo):

$$\left.\begin{array}{l} x \cdot g(x) \\ x^2 \cdot g(x) \\ \vdots \\ x^{n-r-1} \cdot g(x) \end{array}\right\} \text{ son palabras código}$$

se cumple que:

$$V(x) = u_0 \cdot g(x) + u_1 x \cdot g(x) + u_2 \cdot x^2 g(x) + \dots + u_{n-r-1} \cdot x^{n-r-1} g(x) \in G$$

$$V(x) = (u_0 + u_1 x + u_2 \cdot x^2 + \dots + u_{n-r-1} x^{n-r-1}) \cdot g(x)$$

$$V(x) = u(x) \cdot g(x)$$

Entonces:

- Todos los múltiplos de $g(x)$ son polinomios código (con grado $\leq n-1$)
- Si $g(x) = 1 + g_1 x + \dots + g_{r-1} x^{r-1} + x^r$ es el polinomio de grado mínimo de $G(n,k)$ cíclico, entonces:
  un polinomio de grado $\leq n-1$ pertenece al código si y sólo si i es múltiplo de $g(x)$

$$\forall v(x) \in G \Rightarrow V(x) = \dot{g}(x) \Leftrightarrow (\text{múltiplo de } g(x))$$
$$= a(x) \cdot g(x)$$

Dado $G(n,k) \Rightarrow 2^k$ palabras código ($\dot{g}(x)$ todas ellas)

$\exists\ 2^{n-r}$ posibles $u(x)$; $V(x) = u(x) \cdot g(x)$ luego:

$$\boxed{r = n - k = \text{grado mínimo de un polinomio de } G(n,k)}$$

Entonces, sabiendo que $r = n-k$,
el polinomio de grado mínimo tendrá la forma:

$$g(x) = 1 + g_1 x + g_2 x^2 + \dots + g_{n-k-1} x^{n-k-1} + x^{n-k}$$

$\Rightarrow \forall \vec{v} \in C \Rightarrow V(x) = a(x) \cdot g(x)$ ($V(x)$ es múltiplo de $g(x)$)

siendo $g(x)$ el <u>polinomio generador</u>

Ej: $C(7,4) \Rightarrow g(x) = 1 + x + x^3$

$g(x) = 1 + x + x^{n-k}$; $n-k = 7-4 = 3$

$\vec{0}$: (0000000)
$g(x)$: (1101000)

todas las demás de las $2^4 = 16$ palabras las obtendremos rotando y manipulando (combinación lineal) con $g(x)$.

- El polinomio generador $g(x)$ de un código cíclico es factor de (x^n+1)

Ej: $C(15,11) \Rightarrow g(x)$ { grado 4, factor de $(x^{15}+1)$

$$C(7,\dots) \Rightarrow (x^7+1) = \underbrace{(1+x)}_{g_1(x)} \underbrace{(1+x+x^3)}_{g_2(x)} \underbrace{(1+x^2+x^3)}_{g_3(x)}$$

$g_2(x) \rightarrow C_2(7,4)$
$g_1(x) \rightarrow C_1(7,6)$
$g_3 \rightarrow C_3$
$g_1 \cdot g_2 \rightarrow C_4$
$g_1 \cdot g_3 \rightarrow C_5$
$g_2 \cdot g_3 \rightarrow C_6$

podremos crear 6 códigos $= 2^{\text{número de factores}} - 2 = 2^{\text{num fact}} - 1$

Codificación Sistemática

Dado un $\vec{u} = (u_0\ u_1\ \dots\ u_{K-1})$

$$u(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{K-1} \cdot x^{K-1}$$

multiplico por x^{n-K}:

$$x^{n-K} \cdot u(x) = u_0 x^{n-K} + u_1 \cdot x^{n-K+1} + \dots + u_{K-1} \cdot x^{n-1}$$

$$\underbrace{x^{n-K} \cdot u(x)}_{\text{grado} = n-1} = a(x) \cdot g(x) + b(x)$$

$a(x) \cdot g(x)$: $gr = n-K$; $b(x)$: $gr < n-K$

$$a(x) \cdot g(x) = b(x) + x^{n-K} \cdot u(x)$$

$a(x) \cdot g(x) \in G$

Ej: $G(7,4)$ $\quad g(x) = 1 + x + x^3$

$\vec{u} = (1001) \Rightarrow \vec{v} = (\dots 1001)$

$$v(x) = b(x) + x^{n-K} u(x) =$$
$$= b(x) + x^3 (1 + x^3) =$$
$$= b(x) + (x^3 + x^6)$$

$$b(x) = \text{resto}\left(\frac{x^{n-K} \cdot u(x)}{g(x)}\right) = \text{resto}\left(\frac{x^3 + x^6}{1 + x + x^3}\right)$$

$x^3 + x^6 \quad | \; 1 + x + x^3$

$x^3 + x^4 + x^6$ $\quad x^3 + x$

x^4

$x + x^2 + x^4$

$x + x^2 \Rightarrow b(x)$

$$v(x) = b(x) + (x^3 + x^6) =$$
$$= x + x^2 + x^3 + x^6$$

$$\vec{v} = (0\ 1\ 1\ 1\ 0\ 0\ 1)$$

Matriz Generadora:

Sea $C(n,k)$ cíclico con $g(x)$ como polinomio generador:

$g(x) \rightarrow$ menor grado $= (n-k)$

$$g(x) = 1 + g_1 x + g_2 x^2 + \dots + g_{n-k-1} \cdot x^{n-k-1} + x^{n-k}$$

$$G_{k \times n} = \begin{pmatrix} 1 & g_1 & g_2 & \cdots & \cdots & 0 \\ 0 & 1 & g_1 & \cdots & & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & g_{n-k-1} & 1 \end{pmatrix} \begin{matrix} g(x) \\ x g(x) \\ \vdots \\ x^{k-1} g(x) \end{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} \text{lin. dep.} \in C$$

Ej: $C(7,4)$, $g(x) = 1 + x + x^3$

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

Another way:

$u_0(x) = 1 : (1\,0\,0 \dots 0) \rightarrow b_0(x) = \text{resto}\left(\frac{x^{n-k} \cdot u_0(x)}{g(x)} \right)$

$u_1(x) = x : (0\,1\,0 \dots 0) \rightarrow b_1(x) = \text{resto}\left(\frac{x^{n-k} \cdot u_1(x)}{g(x)} \right)$

$u_2(x) = x^2 : (0\,0\,1 \dots 0\,1 \dots$

$\vdots$

$u_{k-1}(x) = x^{k-1} : (0\,0 \dots 0\,1) \rightarrow b_{k-1}(x) = \text{resto}\left(\frac{x^{n-k}\, u_{k-1}(x)}{g(x)} \right)$

$$G_{sist} = \begin{pmatrix} b_{00} & b_{01} & \cdots & 1 & 0 \cdots 0 & 0 \\ b_{10} & b_{11} & \cdots & 0 & 1 \cdots 0 & 0 \\ \vdots & \vdots & \ddots & & & \vdots \\ b_{k-1,0} & b_{k-1,1} & \cdots & 0 & 0 \cdots 0 & 1 \end{pmatrix}$$

Matriz H:

Sabemos que $g(x)$ es factor de (x^n+1)

$$(x^n+1) = g(x)\cdot h(x)$$

$$h(x) = h_0 + h_1 x + \dots + h_{K-1} x^{K-1} + h_K x^K$$

$h(x)$ ha de tener grado $K \Rightarrow h_0 = h_K = 1$

La matriz H se puede calcular a partir de $h(x)$

H tiene filas ortogonales a G

tendremos $n-k$ ecuaciones:

$$\sum_{i=0}^{K} h_i v_{n-i-j} = 0 \qquad 1 \le j \le n-k$$

$$j = n-k \Rightarrow h_K \cdot v_0 + h_{K-1} v_1 + \dots + h_0 v_K = 0$$

tendremos entonces el polinomio recíproco de $h(x) \Rightarrow x^K h(x^{-1})$

$$x^K \cdot h(x^{-1}) = h_K + h_{K-1}\cdot x + \dots + h_1 x^{K-1} + h_0 x^K$$

↳ factor de x^n+1 → polinomio generador de cierto código

$$H = \begin{pmatrix} h_K & h_{K-1} & \dots & h_1 & h_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & h_K & h_{K-1} & \dots & h_1 & h_0 & 0 & 0 & \dots & 0 \\ 0 & 0 & h_K & h_{K-1} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & & & \ddots & & & & & & \vdots \\ 0 & 0 & \dots & & h_K & \dots & & h_1 & h_0 & \end{pmatrix}$$

$$\forall \vec{v} \in C \Rightarrow \vec{v} \cdot \text{filas de } H = 0$$

Ej: $C(7,4)$ $\quad g(x) = 1 + x + x^3$

$$(x^n + 1) = g(x) \cdot h(x)$$

$$(x^7 + 1) = (1 + x + x^3) \cdot h(x) \Rightarrow h(x) = \frac{x^7 + 1}{1 + x + x^3} = x^4 + x^2 + x + 1$$

$h(x)$ = polinomio de paridad

polinomio recíproco:

$$x^K h(x^{-1}) \Rightarrow x^4 (1 + x^{-1} + x^{-2} + x^{-4}) = \underbrace{1 + x^2 + x^3 + x^4}$$

↳ polinomio generador del código dual: $C_d(7,3)$

$$H = \begin{pmatrix} 1\,0\,1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix} \begin{matrix} \\ \\ \updownarrow 3 \end{matrix}$$

$\leftrightarrow 7$

H de $C(7,4)$
G de $C_d(7,3)$

del código $C(7,4)$:

- $d_{min} = 1 \Rightarrow$ NO, pues no hay col. nula
- $d_{min} = 2 \Rightarrow$ No, no hay dos cols. iguales
- $d_{min} = 3$

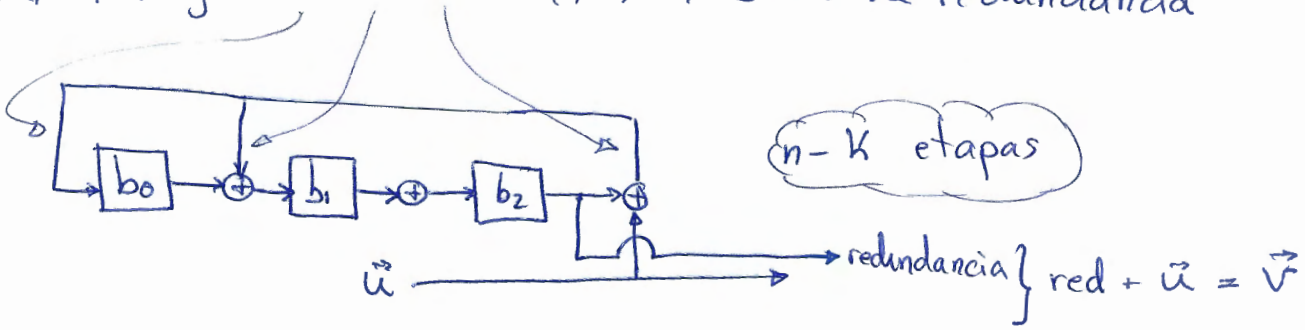
$d_{min} = 4$ en el código $C_d(7,3)$

Codificación de Códigos Cíclicos:

$$\left.\begin{aligned} \vec{v} &= \vec{u} \cdot G \\ v(x) &= u(x) \cdot g(x) \end{aligned}\right\} \text{NO es sistemático}$$

$$\left.\begin{aligned} v(x) &= b(x) + x^{n-k} u(x) \\ b(x) &= \text{resto}\left(\frac{x^{n-k} \cdot u(x)}{g(x)}\right) \end{aligned}\right\} \text{Sí sistemático}$$

Ej: $C(7,4)$ $g(x) = 1 + x + x^3$ $\quad C(7,4) \Rightarrow$ 3 bits de redundancia



Codificador basado en $h(x)$:

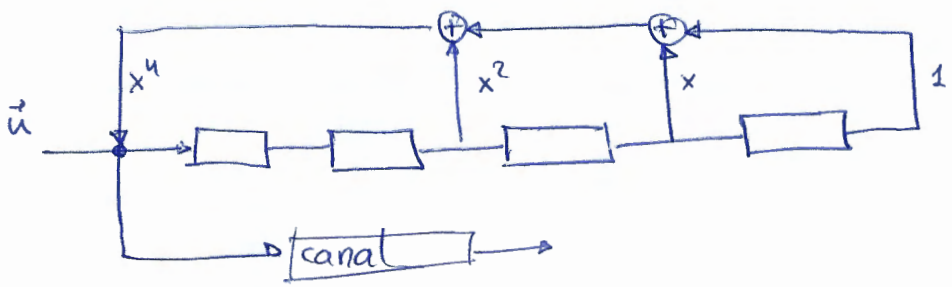
$$\sum_{i=0}^{K} h_i v_{n-i-j} = 0 \; ; \; 1 \le j \le n-K$$

$$h(x) = h_0 + h_1 x + \dots + h_{K-1} x^{K-1} + h_K x^K \; ; \; h_K = 1$$

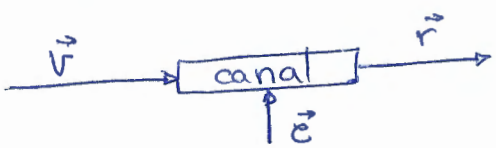
$$v_{n-K-j} = \sum_{i=0}^{K-1} h_i v_{n-i-j} \; ; \; 1 \le j \le n-K$$

Ej: $G(7,4) \Rightarrow g(x) = 1+x+x^3$

$$h(x) = \frac{x^7+1}{1+x+x^3} = 1 + x + x^2 + x^4$$



Síndrome:



$$\vec{S} = \vec{r} \cdot H^t = \begin{cases} = 0 \Rightarrow \vec{r} \in G & \begin{cases} \vec{r} = \vec{v} \text{ (NO error)} \\ \vec{r} \neq \vec{v} \text{ ($e \in G \Rightarrow$ error indetectable)} \end{cases} \\ \neq 0 \Rightarrow \vec{r} \notin G \quad \text{Error} \end{cases}$$

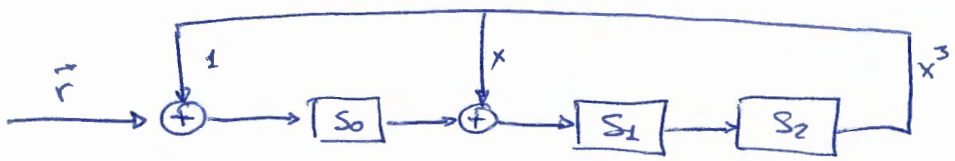
si $\vec{r} \in G \Rightarrow r(x) = \dot{g}(x)$

si $\vec{r} \notin G \Rightarrow r(x) = a(x) \cdot g(x) + s(x)$

$$r(x) = a(x)\, g(x) + s(x) \Rightarrow s(x) = \text{resto}\left(\frac{r(x)}{g(x)}\right)$$

$$s(x) = \begin{cases} =0 \Rightarrow r(x) = \dot{g}(x) \Rightarrow \vec{r} \in G \\ \neq 0 \Rightarrow r(x) \neq \dot{g}(x) \Rightarrow \vec{r} \notin G \end{cases}$$

Ej: $C(7,4) \Rightarrow g(x) = 1 + x + x^3$



si: $\begin{cases} S_0 \; S_1 \; S_2 \\ 0 \; 0 \; 0 \Rightarrow \text{no error ó error indetectable} \\ \text{otros casos} \Rightarrow \text{error} \end{cases}$

- Sea $s(x)$ el síndrome de $r(x)$. Si divido $\frac{x \cdot s(x)}{g(x)}$, queda un resto $s^{(1)}(x)$ que es el síndrome de $r^{(1)}(x)$

⚠ $s^{(1)}(x)$ NO es la rotación cíclica de $s(x)$, es el síndrome de la rotación cíclica de $r(x)$.

Capacidad de Detección

código cíclico ⇒ código lineal

↳ $S_{max} = d_{min} - 1$: se detectan todos los errores de peso $\leq S_{max}$

$\vec{v} \longrightarrow$ canal $\longrightarrow \vec{r} = a(x) \cdot g(x) + s(x)$

$\uparrow \vec{e}$ $\quad \vec{r} = \vec{v} + \vec{e}$

$r(x) = c(x) \cdot g(x) + e(x)$

$e(x) = (a(x) + c(x)) g(x) + s(x)$

$s(x) = \text{síndrome} = \text{resto}\left(\frac{e(x)}{g(x)}\right)$

$S(x) = 0 \Rightarrow e(x) = \dot{g}(x) \Rightarrow e(x) = \begin{cases} 0 \Rightarrow \text{No error} \\ \in C \Rightarrow \text{indetectable} \end{cases}$

$S(x) \neq 0 \Rightarrow e(x) \neq \dot{g}(x) \Rightarrow e(x) \notin C$

- Detecto todos los errores con grado menor que $g(x)$

Errores de tipo ráfaga:

$\vec{e} \rightarrow$ 0 0 0 0 ... 0 0 **1** x x ... x x **1** 0 0 .... 0 0 0

ráfaga de longitud ℓ

longitud de la ráfaga: nº máximo de bits de la ráfaga

sea un error ráfaga de longitud ℓ:

$$e(x) = x^j B(x)$$

$$e(x) = x^j \cdot (1 + e_1 x + e_2 x^2 + \dots + e_{\ell-2} x^{\ell-2} + x^{\ell-1})$$

- Un código cíclico $\mathcal{C}(n,k)$ detecta todas las ráfagas de longitud menor o igual a $n-k$, incluyendo las ráfagas finales

Sólo existe una palabra código con $\ell = n-k+1$ ($g(x)$)

Fracción de ráfagas indetectables de longitud ℓ:

$$\frac{\text{nº ráfagas indetectables}}{\text{nº ráfagas totales}} = \frac{¿?}{2^{\ell-2}}$$

↳ caso $\ell = n-k+1$: $\dfrac{1}{2^{n-k-1}}$

↳ caso $\ell > n-k+1$:

nº ráf. indet. $\Rightarrow \in \mathcal{C} \Rightarrow g(x)$

$$e(x) = x^j \cdot B(x)$$

$$e^{(-j)}(x) = \underbrace{B(x)}_{gr=\ell-1} \Rightarrow \overset{\text{supongo}}{\in \mathcal{C}} \Rightarrow \underbrace{B(x)}_{gr=\ell-1} = \underbrace{a(x)}_{gr=n-k} \cdot \underbrace{g(x)}$$

$\hookrightarrow 2^{\ell-(n-k)-2}$ ráfagas

$$\frac{2^{\ell-(n-k)-2}}{2^{\ell-2}} = \frac{1}{2^{n-k}}$$

Propiedades Adicionales de Detección

- Si $g(x) \neq 1$ se detectan todos los errores simples (peso 1)
  Ej: $e(x) = x^j$
- Si $g(x) = (1+x)$ se detectan todos los errores de peso impar
- Si $g(x)$ tiene como factor a un polinomio primitivo detecta todos los errores dobles (peso 2) si $n \leq 2^r - 1$

Polinomios primitivos: indivisible y desarrollar GF(2)

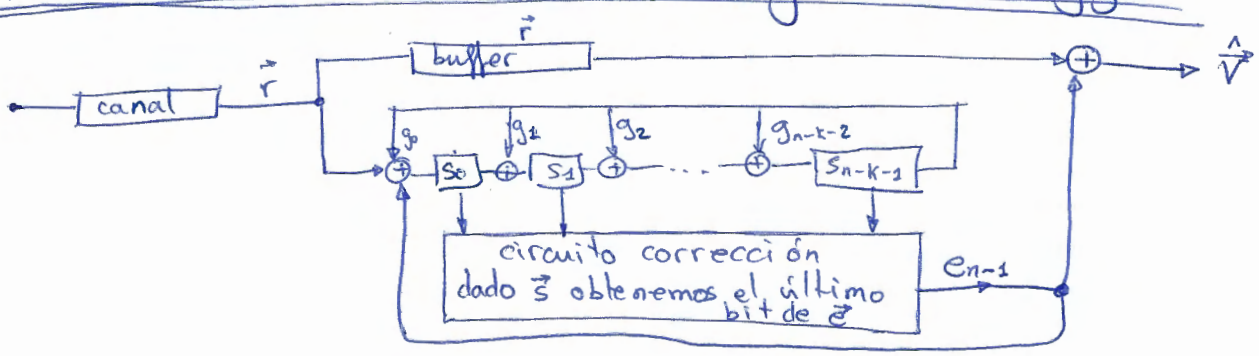
↳ factor de $(x^{2^r-1} + 1)$

↳ No es factor de $(x^m + 1)$ $m < 2^r - 1$

Ej: $g(x) = 1 + x + x^3$

a) indivisible
b) factor de (x^7+1)
c) No es factor de (x^6+1), (x^5+1), (x^4+1)...

Circuito Corrector: Decodif. de Meggit



habiendo obtenido e_{n-1}, si $e_{n-1} = 1 \Rightarrow r_{n-1}$ es erróneo $\Rightarrow$ corregir ese bit

se va rotando $\vec{r}$ hasta que se corrijan (si fuese necesario) toda la palabra

circuito corrección: puerta lógica AND con ciertas entradas negadas

Códigos de Hamming Cíclicos

→ Matriz H tiene como columnas todas las posibles k-tuplas

- Un código de Hamming Cíclico de longitud $n = 2^m - 1$ con $m \geq 3$ es generado por un polinomio primitivo $p(x)$ de grado m

$p(x)$ es primitiva si
- → indivisible
- → factor de $(x^{2^m-1} + 1)$
- → no es factor de $x^t + 1$, $t < 2^m - 1$

Ej: $p(x) = x^9 + x^4 + 1$ es primitivo

↳ $n = 2^9 - 1 = 511$
$n - k = 9 \Rightarrow k = 502$
$\Big\}$ $C(511, 502)$ → detecta peso 2
↳ $d_{min} = 3$

si $g(x) = (1+x) \cdot p(x) \Rightarrow d_{min} = 4$

Códigos recortados

Ej: $C(15, 11)$ ⟶ quiero un $C(12, 8)$

$\vec{u}$ 11 bits ⟶ $\vec{v}$ 15 bits (redundancia)

$(000\ldots001) \longrightarrow (000\ldots001\,1011)$
$(000\ldots010) \longrightarrow (000\ldots010\,1101)$

si a este código le recortamos todo $\vec{u}$ y $\vec{v}$ con 3 bits iniciales a '0' obtenemos:

$\vec{u}$ (8 bits) ⟶ $\vec{v}$ (12 bits) $\Rightarrow C(12, 8)$
$C^*(15-3, 11-3)$

Hemos obtenido un $C(12, 8)$ a partir de un $C(15, 11)$

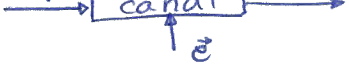
De un $C(n, k)$ obtenemos $C_R(n-\ell, k-\ell)$

Quitamos los vectores con los ℓ bits más signif. a '0' obteniendo $2^{k-\ell}$ vectores

Resulta en un código lineal (NO cíclico) pero mantiene las propiedades del código original (cíclico)

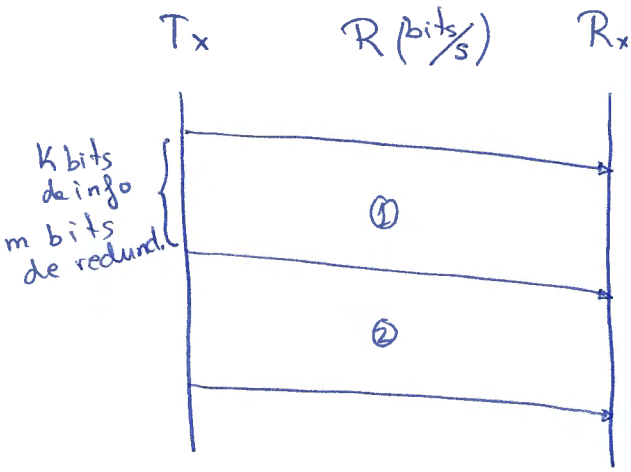
Técnicas ARQ (sólo aplicable a canales dúplex)

ARQ = Automatic Retransmition reQuest



$$\left.\begin{array}{l}\vec{s} = \vec{r}\cdot H^t \\ s(x) = \text{resto}\left(\frac{r(x)}{g(x)}\right)\end{array}\right\} = \begin{cases} = \vec{0} \Rightarrow \text{ok} \\ \neq \vec{0} \Rightarrow \text{error} \end{cases}$$

- error → solicitud de retransmis. (ARQ)
- error → intento de corrección (FEC)



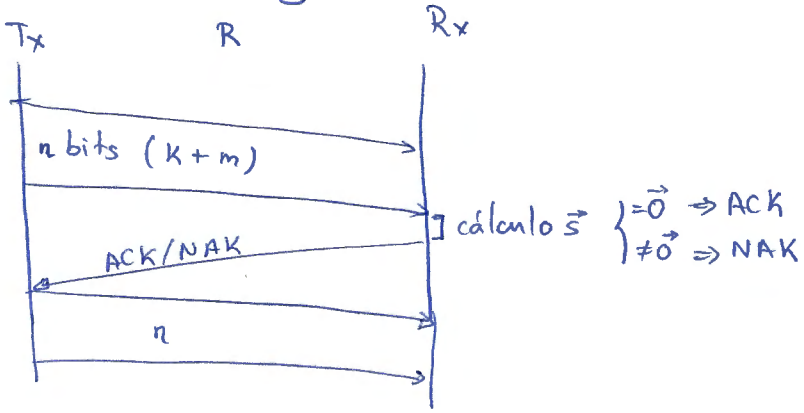
$$\text{Cadencia eficaz} = \frac{K}{T_{oc}} = \frac{n}{R}$$

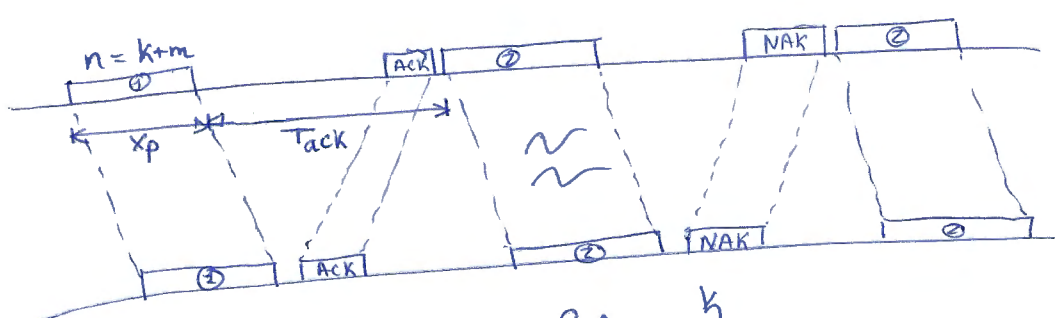
$$C_{ef} = \frac{K}{(K+m)/R} = \frac{K}{K+m}\cdot R$$

$K+m$: K información, m redundancia ($m = n - K$)

T_{oc} = tiempo de ocupación

ARQ parada y espera





$$X_p = \frac{K+m}{R}$$

$$T_{ack} = (D_{prop} + D_{proc} + \dots)$$

$$C_{ef} = \frac{k}{T_{oc}}$$

N° transm.	T_{oc}	$P(N^\circ \text{transm})$
1	$x_p + T_{ack}$	$1 - P_{RTX}$
2	$2 \cdot (x_p + T_{ack})$	$P_{RTX} \cdot (1 - P_{RTX})$
3	$3 \cdot (x_p + T_{ack})$	$P_{RTX}^2 \cdot (1 - P_{RTX})$
⋮	⋮	⋮
i	$i\,(x_p + T_{ack})$	$P_{RTX}^{i-1} \cdot (1 - P_{RTX})$

Estando a tope de detección:

si $w(\vec{e}) = 0 \Rightarrow$ no error

$w(\vec{e}) = 1$ … $w(\vec{e}) = s_{max}$ } error detectado $= P_{RTX}$

$w(\vec{e}) = d_{min}$ … $w(\vec{e}) = n$ } error no detectado $= P_{ER}$

$$\overline{T_{oc}} = \sum_{i=1}^{\infty} T_{oc_i} \cdot P(T_{oc_i}) = \sum_{i=1}^{\infty} i\,(x_p + T_{ack}) \cdot P_{RTX}^{\,i-1} (1 - P_{RTX}) =$$

$$= (1 - P_{RTX})(x_p + T_{ACK}) \frac{1}{(1 - P_{RTX})^2} = \frac{x_p + T_{ACK}}{1 - P_{RTX}}$$

$$C_{ef} = \frac{k}{\overline{T_{oc}}} = \frac{k}{\left(\frac{k+m}{R} + T_{ACK}\right)/(1 - P_{RTX})} = (1 - P_{RTX}) \frac{k}{k + m + T_{ACK} \cdot R} \cdot R \quad (\text{bps})$$

$$\rho = \frac{C_{ef}}{R} = (1 - P_{RTX}) \frac{k}{k + m + T_{ACK} \cdot R} \quad (\%)$$

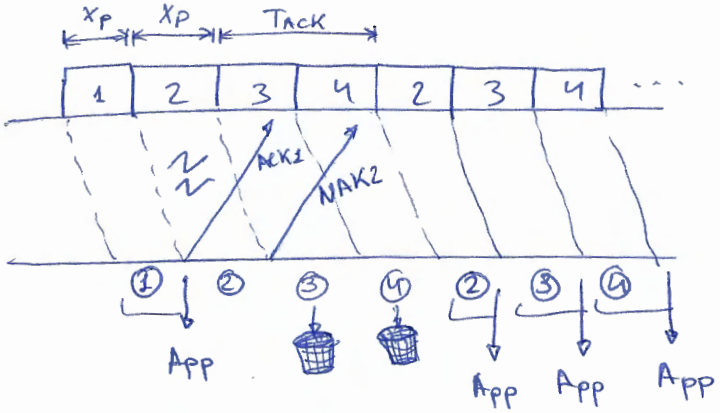
Si aproximamos diciendo que se detectan todos los errores ($P_{ER} = 0$) entonces: $P_{RTX} = 1 - P(\vec{e} = \vec{0}) = 1 - (1 - p)^n$

↳ P_{error} de bloque

Longitud óptima de bloque:

$$\frac{dC_{ef}}{dk} = 0 \Rightarrow k_{opt} \simeq \sqrt{\frac{m + R \cdot T_{ACK}}{p}}$$

ARQ envío continuo y rechazo simple:

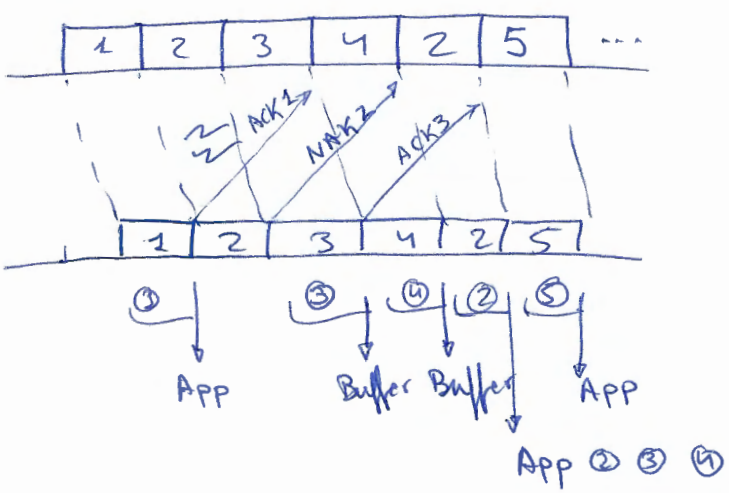


N_T	T_{oc}	$P(N_T)$
1	x_p	$1-P_{RTX}$
2	$(x_p+T_{ACK})+x_p$	$P_{RTX}(1-P_{RTX})$
3	$2(x_p+T_{ACK})+x_p$	$P_{RTX}^2(1-P_{RTX})$
⋮		
i	$(i-1)(x_p+T_{ACK})+x_p$	$P_{RTX}^{i-1}(1-P_{RTX})$

$$\overline{T_{oc}} = \sum_{i=1}^{\infty} (1-P_{RTX})\,P_{RTX}^{\,i}\,[(i-1)(x_p+T_{ACK})+x_p] = x_p + (x_p+T_{ACK})\left(\frac{1}{1-P_{RTX}}-1\right)$$

$$C_{ef} = \frac{K}{\frac{k+m}{R} + \left(\frac{k+m}{R}+T_{ACK}\right)\left(\frac{1}{1-P_{RTX}}-1\right)} = (1-P_{RTX})\,\frac{k}{k+m+R\,T_{ACK}\cdot P_{RTX}}\cdot R$$

ARQ envío continuo y rechazo selectivo:



N_T	T_{oc}	$P(N_T)$
1	x_p	$1-P_{RTX}$
2	$2x_p$	$P_{RTX}(1-P_{RTX})$
3	$3x_p$	
⋮		
i	ix_p	$P_{RTX}^{i-1}(1-P_{RTX})$

$$\overline{T_{oc}} = \sum_{i=1}^{\infty} i\,x_p\,P_{RTX}^{\,i-1}\,(1-P_{RTX}) = \frac{x_p}{1-P_{RTX}}$$

$$C_{ef} = \frac{k}{T_{oc}} = \frac{k}{\frac{k+m/R}{1-P_{RTX}}} = (1-P_{RTX})\,\frac{k}{k+m}\cdot R$$

PRIMER GRUPO DE EJERCICIOS - Curso 2013/2014

ENTREGA: 24 de Septiembre

Versión: 1.0.

ENUNCIADOS

1.-Dada la distribución conjunta de probabilidades de las cadenas de tres símbolos NCV (número, consonante, vocal) consecutivos, donde N ϵ {1, 2, 3}, C ϵ {b, d, f, l, m} y V ϵ {a, e, i} y cuya distribución conjunta de probabilidades P(N , C, V) viene dada por

P(N,C,V=a)	1	2	3
b	1/16	0	0
d	1/32	1/16	0
f	1/32	1/8	1/32
l	0	0	0
m	0	0	0

P(N,C,V=e)	1	2	3
b	1/16	0	0
d	1/32	1/16	0
f	0	0	0
l	0	1/16	1/32
m	0	0	1/16

P(N,C,V=i)	1	2	3
b	0	0	0
d	0	0	0
f	1/32	1/8	1/32
l	0	1/16	1/32
m	0	0	1/16

Se pide

a) Calcular la incertidumbre conjunta H(N ,C, V)
b) Determinar las distribuciones de probabilidades de p(n, c), p(n, v), p(c, v)
c) Calcular las incertidumbres H(N,C), H(N,V), H(C,V)
d) Determinar las distribuciones de probabilidades marginales p(n), p(c), p(v)
e) Calcular la incertidumbre de cada variable aleatoria H(N), H(C), H(V)
f) Determinar las probabilidades condicionales p(n, v | c).
g) Calcular a partir de la distribución anterior la incertidumbre condicional H(N, V | C).
h) Determinar las probabilidades condicionales p(c, v | n).
i) Calcular a partir de la distribución anterior la incertidumbre condicional H(C, V | N).

j) Calcular la incertidumbre condicional H(C, V | N) sin calcular la distribución p(c, v | n)
k) Calcular las incertidumbres condicionales H(N | C, V), H(C | N, V) y H(V | N, C)
l) Calcular la información mutua entre cada pareja de variables
m) Calcular la información mutua entre cada pareja de variables condicionada a la tercera.
n) ¿Existe alguna dependencia markoviana entre las variables? En caso afirmativo, diga cuál y justifíquela.

2.-La mitad de las llamadas de un operador son de líneas móviles y el resto de líneas fijas. De un segundo operador, una cuarta parte son de líneas móviles. El primer operador tiene una cuota de mercado del 75% y el segundo el 25%. En estas condiciones, donde O es el operador y T el tipo de llamada, justificar razonadamente y SIN CALCULAR ENTROPÍAS cuál de las dos siguientes sentencias es verdadera:

a) $H(T/O) > H(O/T)$
b) $H(O/T) > H(T/O)$

Calcular:

c) Si una llamada es de teléfono fijo, ¿cuánta incertidumbre tenemos sobre el operador?
d) Ídem si la llamada es de móvil
e) ¿Cuál es la reducción en la cantidad de información del operador si sabemos el tipo de llamada?

3.- Acotar cuales son los límites de la incertidumbre de una variable con nueve alternativas de las que la más frecuente sucede la mitad de las veces.

4.- Calcular la incertidumbre de B, y la información mutua entre dos variables A y B, tales que la incertidumbre de la primera es un tercio de la incertidumbre de la segunda; también es a su vez el doble de la entropía condicionada de la primera dada la segunda, y a su vez la incertidumbre de la primera es de 4 bit.

5.- Sea X una v.a. e $Y = f(X)$

a) ¿Qué condiciones debe cumplir f() para que la $H(X) = H(Y)$?
b) ¿Qué ocurre en caso contrario?

6.- Determinar la certeza o falsedad de las siguientes proposiciones

a) Siempre se cumple que $I(X ; Y , Z) = H(Y) + H(Z / Y) - I(X ; Z)$
b) Si $X \rightarrow Y \rightarrow Z$, entonces SIEMPRE se cumple que $I(X ; Y) \leq I(X ; Z)$
c) Si $X \rightarrow Y \rightarrow Z$, entonces SIEMPRE se cumple que $I(X ; Y) \leq I(Y ; Z)$
d) La condicionalidad reduce la entropía porque la entropía relativa entre dos variables aleatorias es no-negativa
e) Si la variable aleatoria $A \in \{1, 2, 3, 4, 5\}$ y la variable aleatoria $B \in \{par, impar\}$, con $H(B) = 1$, $H(A / B= impar)= 3/2$ y $H(A / B=par) =1$, entonces $H(A) = 2$ bits
f) La media del log de una variable es menor o igual que el log de la media
g) $H(A, B, C) \leq H(A, B), + H(B, C) - H(B)$
h) $H(A, B / C) \geq H(A /C) + H(B / C)$
i) $D(p||q) = D(q||p) + \log (p(x) / q(x))$
j) $D(p||q) - D(q||p) = H(p) - H(q)$

1

a) $H(N, C, V)$

Para calcular la incertidumbre conjunta de N, C y V, extenderemos la definición de incertidumbre para tres variables como:

$$H(N,C,V) = \sum_{\forall v} \sum_{\forall c} \sum_{\forall n} p(N,C,V) \cdot \log_2\left(\frac{1}{p(n,c,v)}\right)$$

los cálculos de $p(N,C,V)$ y $\log_2\left(\frac{1}{p(n,c,v)}\right)$ han sido calculados con una hoja de procesado de datos [ver siguiente página]

resumiendo:

$$H(N,C,V=a) = 1,34375$$
$$H(N,C,V=e) = 1,3125$$
$$H(N,C,V=i) = 1,34375$$

$$H(N,C,V) = \sum_{\forall v} H(N,C,V=v) = H(N,C,V=a) + H(N,C,V=e) + H(N,C,V=i) = 4 \text{ bits}$$

b) $p(n,c)$, $p(n,v)$, $p(c,v)$

En el cálculo de $p(x,y)$, sumaremos todos los valores de z para esas variables; así:

Y \ X	x_1
y_1	$p(x,y,z=1) + p(x,y,z=2)$
y_2	$p(x,y,z=1) + p(x,y,z=2)$
y_3	$p(x,y,z=1) + p(x,y,z=2)$

podemos ver las tablas con los resultados en la página titulada "Ejercicio 1b y 1c" dispuesta a continuación

c) $H(N,C)$, $H(N,V)$, $H(C,V)$

El cálculo de $H(X,Y)$ lo realizaremos haciendo uso de su definición:

$$H(X,Y) = \sum_{\forall x} \sum_{\forall y} p(x,y) \cdot \log_2 \left(\frac{1}{p(x,y)} \right)$$

como ya tenemos $p(n,c)$, $p(n,v)$ y $p(c,v)$ por el apartado anterior, será sencillo hacer el cálculo, los cuales se pueden observar en la página titulada "Ejercicio 1b y 1c".

Sólo falta hacer el sumatorio, resultando:

$H(N,C) = 3$ bits
$H(N,V) = 2,9836$ bits
$H(C,V) = 3,1864$ bits

d) $p(n)$, $p(c)$, $p(v)$

Para hallar $p(x)$ sabiendo $p(x,y)$, sumaremos todos los valores de la variable y; es decir: $p(x) = \sum_{\forall y} p(x, y_i)$

$$\begin{cases} p(n=1) = 1/4 \\ p(n=2) = 1/2 \\ p(n=3) = 1/4 \end{cases} \qquad \begin{cases} p(v=a) = 11/32 \\ p(v=e) = 5/16 \\ p(v=i) = 11/32 \end{cases}$$

$$\begin{cases} p(c=b) = 1/8 \\ p(c=d) = 3/16 \\ p(c=f) = 3/8 \\ p(c=l) = 3/16 \\ p(c=m) = 1/8 \end{cases}$$

como se puede observar,

$\sum_{\forall x} p(x) = 1$

Ejercicio 1a

p(n,c,v=a)	1	2	3		
b	1/16	0	0	p(n,c=b,v=a)	1/16
d	1/32	1/16	0	p(n,c=d,v=a)	3/32
f	1/32	1/8	1/32	p(n,c=f,v=a)	3/16
l	0	0	0	p(n,c=l,v=a)	0
m	0	0	0	p(n,c=m,v=a)	0
	p(n=1,c,v=a)	p(n=2,c,v=a)	p(n=3,c,v=a)		
	1/8	3/16	1/32	p(n,c,v=a)	11/32

1/p(n,c,v=a)	1	2	3
b	16		
d	32	16	
f	32	8	32
l			
m			

log2(1/p(n,c,v=a))	1	2	3
b	4		
d	5	4	
f	5	3	5
l			
m			

H(n,c,v=a)	1	2	3
b	1/4		
d	5/32	1/4	
f	5/32	3/8	5/32
l			
m			

$H(n,c,v=a) = 1'34375$

p(n,c,v=e)	1	2	3		
b	1/16	0	0	p(n,c=b,v=a)	1/16
d	1/32	1/16	0	p(n,c=d,v=a)	3/32
f	0	0	0	p(n,c=f,v=a)	0
l	0	1/16	1/32	p(n,c=l,v=a)	3/32
m	0	0	1/16	p(n,c=m,v=a)	1/16
	p(n=1,c,v=a)	p(n=2,c,v=a)	p(n=3,c,v=a)		
	3/32	1/8	3/32	p(n,c,v=a)	5/16

1/p(n,c,v=e)	1	2	3
b	16		
d	32	16	
f			
l		16	32
m			16

log2(1/p(n,c,v=e))	1	2	3
b	4		
d	5	4	
f			
l		4	5
m			4

H(n,c,v=e)	1	2	3
b	1/4		
d	5/32	1/4	
f			
l		1/4	5/32
m			1/4

$H(n,c,v=e) = 1,3125$

p(n,c,v=i)	1	2	3		
b	0	0	0	p(n,c=b,v=a)	0
d	0	0	0	p(n,c=d,v=a)	0
f	1/32	1/8	1/32	p(n,c=f,v=a)	3/16
l	0	1/16	1/32	p(n,c=l,v=a)	3/32
m	0	0	1/16	p(n,c=m,v=a)	1/16
	p(n=1,c,v=a)	p(n=2,c,v=a)	p(n=3,c,v=a)		
	1/32	3/16	1/8	p(n,c,v=a)	11/32

1/p(n,c,v=i)	1	2	3
b			
d			
f	32	8	32
l		16	32
m			16

log2(1/p(n,c,v=i))	1	2	3
b			
d			
f	5	3	5
l		4	5
m			4

H(n,c,v=i)	1	2	3
b			
d			
f	5/32	3/8	5/32
l		1/4	5/32
m			1/4

$H(n,c,v=i) = 1,34375$

Ejercicio 1b y 1c

p(n,c,v=a)	1	2	3
b	1/16	0	0
d	1/32	1/16	0
f	1/32	1/8	1/32
l	0	0	0
m	0	0	0

p(n,c,v=e)	1	2	3
b	1/16	0	0
d	1/32	1/16	0
f	0	0	0
l	0	1/16	1/32
m	0	0	1/16

p(n,c,v=i)	1	2	3
b	0	0	0
d	0	0	0
f	1/32	1/8	1/32
l	0	1/16	1/32
m	0	0	1/16

p(n,c)	1	2	3
b	1/8	0	0
d	1/16	1/8	0
f	1/16	1/4	1/16
l	0	1/8	1/16
m	0	0	1/8

p(n,v)	1	2	3
a	1/8	3/16	1/32
e	3/32	1/8	3/32
i	1/32	3/16	1/8

p(c,v)	b	d	f	l	m
a	1/16	3/32	3/16	0	0
e	1/16	3/32	0	3/32	1/16
i	0	0	3/16	3/32	1/16

log2(1/p(n,c))	1	2	3
b	3		
d	4	3	
f	4	2	4
l		3	4
m			3

log2(1/p(n,v))	1	2	3
a	3,0000	2,4150	5,0000
e	3,4150	3,0000	3,4150
i	5,0000	2,4150	3,0000

log2(1/p(c,v))	b	d	f	l	m
a	4,0000	3,4150	2,4150		
e	4,0000	3,4150		3,4150	4,0000
i			2,4150	3,4150	4,0000

H(N,C)	1	2	3
b	3/8		
d	1/4	3/8	
f	1/4	1/2	1/4
l		3/8	1/4
m			3/8

H(N,V)	1	2	3
a	0,3750	0,4528	0,1563
e	0,3202	0,3750	0,3202
i	0,1563	0,4528	0,3750

H(C,V)	b	d	f	l	m
a	0,2500	0,3202	0,4528		
e	0,2500	0,3202		0,3202	0,2500
i			0,4528	0,3202	0,2500

$H(N,V) = 2,9836$ bits

$H(C,V) = 3,1864$ bits

$H(N,C) = 3$ bits

e) $H(N)$, $H(C)$, $H(V)$

Sabiendo que: $H(X) = \sum_{\forall x} p(x) \cdot \log_2\left(\frac{1}{p(x)}\right)$

$$H(N) = \frac{1}{4}\cdot 2 + \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 = \frac{3}{2} = 1{,}5 \text{ bits}$$

$$H(C) = \frac{1}{8}\cdot 3 + \frac{3}{16}\cdot 2'415 + \frac{3}{8}\cdot 1'415 + \frac{3}{16}\cdot 2'415 + \frac{1}{8}\cdot 3 = 2{,}1863 \text{ bits}$$

$$H(V) = \frac{11}{32}\cdot 1'54 + \frac{5}{16}\cdot 1'678 + \frac{11}{32}\cdot 1'54 = 1{,}5831 \text{ bits}$$

f) $p(n, v/c)$

sabemos que: $p(x, y/z) = \dfrac{p(x, y, z_i)}{p(z_i)}$ luego:

v \ n	1	2	3
a	1/2	0	0
e	1/2	0	0
i	0	0	0

$p(c=b) = 1/8$

v \ n	1	2	3
a	1/6	1/3	0
e	1/6	1/3	0
i	0	0	0

$p(c=d) = 3/16$

v \ n	1	2	3
a	1/12	1/3	1/12
e	0	0	0
i	1/12	1/3	1/12

$p(c=f) = 3/8$

v \ n	1	2	3
a	0	0	0
e	0	1/3	1/6
i	0	1/3	1/6

$p(c=l) = 3/16$

v \ n	1	2	3
a	0	0	0
e	0	0	1/2
i	0	0	1/2

$p(c=m) = 1/8$

Se observa que todas las tablas suman 1.

g) $H(N, V/C)$

Podemos expresar la entropía condicionada como la diferencia entre la entropía conjunta y la entropía marginal de la variable que condiciona.

$$H(N, V/C) = H(N, V, C) - H(C)$$

Ambos elementos han sido calculados en los apartados a) y e) de este mismo ejercicio, luego:

$$H(N, V/C) = 4 - 2,1863 = 1,8137 \text{ bits}$$

h) $p(c, v/n)$

Análogamente al apartado f:

$$p(c, v/n) = \frac{p(c, v, n_i)}{p(n_i)}$$

n \ c	b	d	f	l	m
a	1/4	1/8	1/8	0	0
e	1/4	1/8	0	0	0
i	0	0	1/8	0	0

$p(n=1) = 1/4$

v \ c	b	d	f	l	m
a	0	1/8	1/4	0	0
e	0	1/8	0	1/8	0
i	0	0	1/4	1/8	0

$p(n=2) = 1/2$

v \ c	b	d	f	l	m
a	0	0	1/8	0	0
e	0	0	0	1/8	1/4
i	0	0	1/8	1/8	1/4

$p(n=3) = 1/4$

Cada tabla suma 1 como se puede comprobar.

i) $H(C, V/N)$

j) Idem apartado g:

$$H(C, V/N) = H(C, V, N) - H(N) = 4 - 1'5 = 2'5 \text{ bits}$$

k) $H(N/C,V)$, $H(C/N,V)$, $H(V/N,C)$

Podemos desarrollar $H(X/Y,Z)$ como:

$H(X,Y,Z) - H(Y) - H(Z/Y) = H(X,Y,Z) - H(Y) - (H(Z,Y) - H(Y)) =$

$= H(X,Y,Z) - H(Z,Y)$, luego:

$H(N/C,V) = H(N,C,V) - H(V,C) = 4 - 3,1864 = 0'8136$

$H(C/N,V) = H(C,N,V) - H(V,N) = 4 - 2,9836 = 1'0164$

$H(V/N,C) = H(V,N,C) - H(C,N) = 4 - 3 = 1$ bit

l) $I(N;C)$, $I(N;V)$, $I(C;V)$

Sabemos que: $I(X;Y) = H(Y) - H(Y/X) =$

$= H(Y) - (H(Y,X) - H(X))$

Luego:

$I(N;C) = H(C) - (H(C,N) - H(N)) =$

$= 2'1863 - (3 - 1'5) = 0'6863$ bits

$I(N;V) = H(V) - (H(V,N) - H(N)) =$

$= 1,5831 - (2,9836 - 1'5) = 0'0995$ bits

$I(C;V) = H(V) - (H(V,C) - H(C)) =$

$= 1'5831 - (3,1864 - 2,1863) = 0'583$ bits

m) $I(N;C/V)$, $I(N;V/C)$, $I(C;V/N)$

siendo $I(X;Y/Z) = H(X/Z) - H(X/Y,Z) =$

$= H(X,Z) - H(Z) - H(X/Y,Z)$

podemos formar las informaciones mutuas condicionadas pedidas:

$$I(N;C/V) = H(N,V) - H(V) - H/N/C,V) =$$
$$= 2,9836 - 1,5831 - 0'8136 = 0'5869 \text{ bits}$$

$$I(N;V/C) = H(N,C) - H(C) - H(N/V,C) =$$
$$= 3 - 2'1863 - 0'8136 = 0'0001 \text{ bits} \approx 0$$

$$I(C;V/N) = H(C,N) - H(N) - H(C/V,N) =$$
$$= 3 - 1's - 1'0164 = 0'4836 \text{ bits}$$

h) relación markoviana:

Observamos que $I(N;V/C) = 0$

lo que significa que N y V condicionados por C son independientes (pues no tienen información mutua entre ellas), luego la relación markoviana es la siguiente:

$$N \longrightarrow C \longrightarrow V$$

ó

$$V \longrightarrow C \longrightarrow N$$

Sabemos que: si $N \to C \to V \overset{\text{ENTONCES}}{\Longrightarrow} I(N;V/C) = 0$

la implicación sólo se cumple en el otro sentido si las informaciones mutuas de las otras variables NO es nula

(2) La opción correcta es a) $H(T/O) > H(O/T)$

ya que en el caso del operador A la entropía es máxima, pues sus llamadas se distribuyen al 50% entre la línea fija y móvil.

Así, tendremos mayor entropía sabiendo el operador.

En caso de conocer el tipo de llamada, gracias a las grandes diferencias del operador B (en cuanto a tipo de llamada se refiere), sabremos con mayor acierto el operador.

$$H(O,T) = \begin{cases} H(T) + H(O/T) \\ H(O) + H(T/O) \end{cases}$$

	OpA	OpB
T movil	3/8	1/16
T fija	3/8	3/16

c) si T = fija, ¿incertidumbre sobre el operador?

$$H(O/T=\text{fija}) = \frac{3}{8}\log_2\left(\frac{8}{3}\right) + \frac{3}{16}\log_2\left(\frac{16}{3}\right) = 0'9835 \text{ bits}$$

$= 0'9183$ bits

$\hookrightarrow = H\left(\frac{2}{3}, \frac{1}{3}\right)$

d) ídem si T = móvil

$$H(O/T=\text{móvil}) = \frac{3}{8}\cdot\log_2\left(\frac{8}{3}\right) + \frac{1}{16}\log_2(16) = 0'7806 \text{ bits}$$

$0'5917$ bits

e) $H(O) - H(O/T) = I(O;T)$

$$H(O) = \frac{3}{4}\cdot\log_2\left(\frac{4}{3}\right) + \frac{1}{4}\log_2(4) = 0'8113 \text{ bits}$$

$$H(O/T) = H(O,T) - H(T) = 1,7641 - 0,9887 = 0,7754 \text{ bits}$$

$$H(O) - H(O/T) = 0,0359 \text{ bits} = I(O;T)$$

(3) si $|X| = 9 \Rightarrow H(X) \leq \log_2(|X|) = \log_2(9) = 3{,}1699$ bits

por otro lado, una repartición equiprobable de las alternativas hará la entropía máxima, luego:

$$H_{max}(X) = \frac{1}{2}\log_2(2) + 8\cdot\left(\frac{1}{16}\log_2(16)\right) = \frac{1}{2} + 2 = 2'5 \text{ bits}$$

así mismo, la entropía de una fuente será mínima cuanto más dispares sean las probabilidades de los diferentes sucesos, con lo que:

$$H_{min}(X) = 2\cdot\left(\frac{1}{2}\log_2(2)\right) + 7\cdot\underbrace{\left(0\cdot\log_2(\infty)\right)}_{0} = 1 \text{ bit}$$

$$1 \text{ bit} \leq H(X) \leq 2'5 \text{ bits}$$

(4) $H(A) = 4$ bits

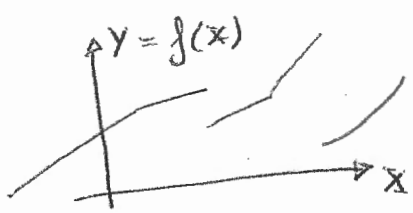
$$H(A) = \frac{1}{3}H(B) \Rightarrow H(B) = 3\cdot H(A) = 12 \text{ bits}$$

$$H(A) = 2\,H(A/B) \Rightarrow H(A/B) = H(A)\cdot\frac{1}{2} = 2 \text{ bits}$$

$$I(A;B) = H(A) - H(A/B) = 4 - 2 = 2 \text{ bits}$$

(5) $X \rightarrow Y = f(X)$

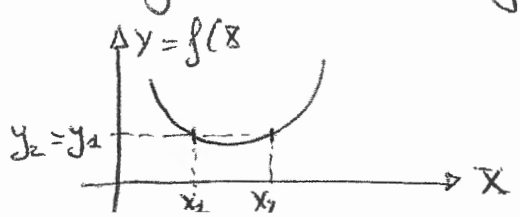
a) Para que $H(X) = H(Y)$ f debe ser inyectiva



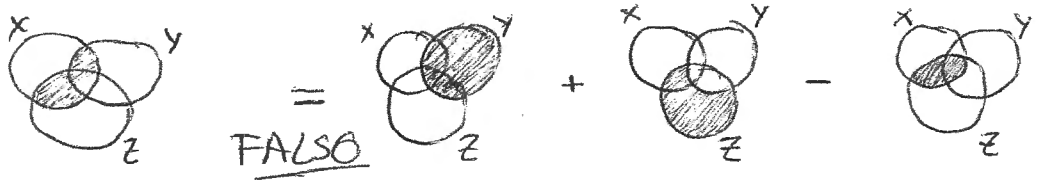
$\forall (x_i, x_j) \in X;\ i \neq j$

$f(x_i) \neq f(x_j)$

b) Si f no es inyectiva tendremos una función continua



(6) a) $I(X;Y,Z) = H(Y) + H(Z/Y) - I(X;Z)$



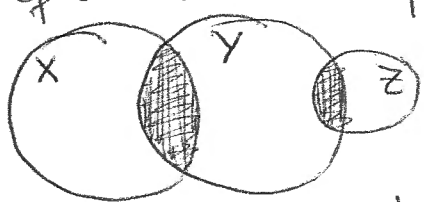
b) $X \rightarrow Y \rightarrow Z \underset{\text{siempre}}{\Rightarrow} I(X;Y) \leq I(X;Z)$

FALSO: El teorema del proceso de información dice lo contrario. "Nunca una manipulación más inteligente de los datos va a mejorar la información mutua entre las variables aleatorias."

c) $X \rightarrow Y \rightarrow Z \underset{\text{siempre}}{\Rightarrow} I(X;Y) \leq I(Y;Z)$

FALSO: No tiene por qué ocurrir siempre.

Podría suceder que:



donde
$I(X;Y) > I(Y;Z)$

d) Verdadero: Condicionar reduce la entropía.

En el "peor" de los casos, donde las V.A. sean independientes, condicionar no reducirá la entropía, aunque tampoco la aumentará.

e) $A \in \{1,2,3,4,5\}$, $B \in \{\text{par, impar}\}$

$H(B) = 1 \Rightarrow$ equiprobabilidad $\{\frac{1}{2}, \frac{1}{2}\}$

$H(A/B=\text{impar}) = 3/2$ bits

$H(A/B=\text{par}) = 1$ bit

$\Rightarrow H(A) \overset{¿?}{=} 2$

$H(A/B) = \frac{1}{2} \cdot \frac{3}{2} + \frac{1}{2} \cdot 1 = \frac{5}{4}$ bits

$H(A,B) = H(A/B) + H(B) = \frac{5}{4} + 1 = \frac{9}{4}$ bits

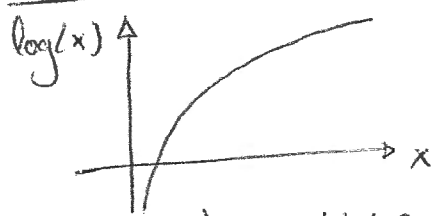
$H(A/B=\text{impar}) \neq H(A/B=\text{par}) \Rightarrow$ A y B dependientes $\Rightarrow$

$H(B/A) = 0 \Rightarrow H(A) = H(A,B) - H(B/A) = \frac{9}{4} - 0 = \frac{9}{4} \neq 2$

FALSO

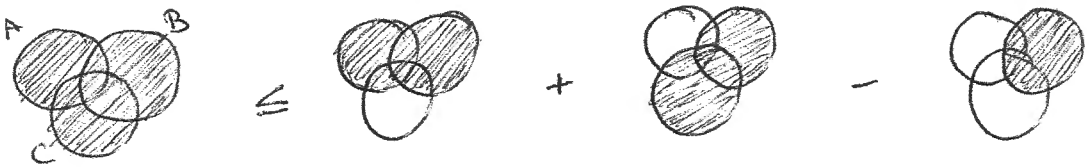
f) $E[\log(X)] \overset{¿?}{\leq} \log(E[X])$

Verdadero: por ser log una función convexa:



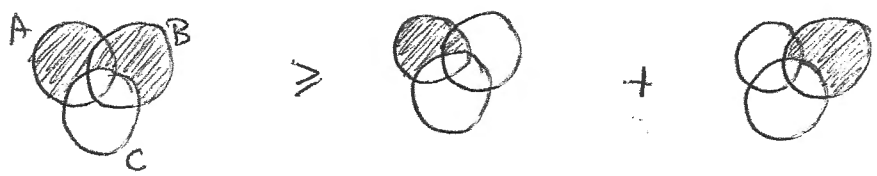
$E[\log(x)] \leq \log(E[x])$

g) $H(A,B,C) \leq H(A,B) + H(B,C) - H(B)$



Verdadero: será = cuando sean independientes

h) $H(A,B/C) \geq H(A/C) + H(B/C)$



Falso: es $\leq$

i) $D(p\|q) = D(q\|p) + \log\left(\frac{p}{q}\right)$

$\sum p \cdot \log_2\left(\frac{p}{q}\right) = \sum q \cdot \log_2\left(\frac{q}{p}\right) + \log\left(\frac{p}{q}\right)$

el último término no tiene sentido

Falso

j) $D(p\|q) - D(q\|p) = H(p) - H(q)$

↳ $\sum p \log_2\left(\frac{p}{q}\right) - \sum q \log_2\left(\frac{q}{p}\right)$

↳ $\sum p \log_2(p) - p \cdot \log_2(q) - \left(\sum q \log_2(q) - q \log_2(p)\right)$

$H(p) - \sum p \cdot \log_2(q) - \left(H(q) - \sum q \log_2(p)\right)$

FALSO: "sobran" dos términos

SEGUNDO GRUPO DE EJERCICIOS - Curso 2013/2014

ENTREGA: 10 de Octubre

Versión: 1.0.

ENUNCIADOS

1.- Fuente Pseudo-Morse: Un código tradicional muy extendido generaba secuencias de dos símbolos: el punto y la raya. Supongamos tener una fuente que genera sucesivos símbolos independientes e idénticamente distribuidos de puntos y rayas con probabilidades p y q (=1-p) respectivamente, que se codifican en binario del siguiente modo: el punto se codifica para ser transmitido como una subsecuencia binaria -10-, y la raya como -110-.

El resultado es un generador de símbolos binarios con una estructura de memoria específica. Se pide:

a) Modélese dicho generador como una fuente markoviana de primer orden un generador binario de este comportamiento (con tantos estados como fases de generación de los bits de las subsecuencias sean necesarias). Calcular la matriz de probabilidades de transición respectiva y su autovector de probabilidades.
b) ¿Cuál es la probabilidad de que tomando un bit al azar en una secuencia larga este sea el último de los 1´s correspondiente a una raya? ¿de que sea el primer 1 de una subsecuencia?
c) ¿Cuál es la probabilidad de tener un 0 en cada uno de los cinco primeros bits de una secuencia codificada?
d) Con estas consideraciones analizar el significado de la distribución de probabilidades del autovector. ¿En qué condiciones sería una distribución estacionaria?
e) Calcular cual es la tasa de entropía de esta fuente.
f) Calcular que valor de p maximiza la tasa de entropía. ¿Cuál sería su valor? ¿Y si p=q?
g) Si la codificación de la raya fuese 1110. Repetir los apartados a, b, c, d, e para este caso.

2.- Una secuencia X^L de símbolos, donde X ε {l,m,x,j,v,s,d} y de longitud l, representa la sucesión de días de la semana en que suceden una serie de eventos. Por ejemplo:

l l m m m j j j v v s d l x x x v v d d

significaría que los dos primeros sucesos fueron un lunes, los tres siguientes un martes, etc.

Al estudiar una secuencia larga se observa que el 50% de las veces el símbolo siguiente se repite al anterior, que del resto la mitad de las veces es el símbolo correspondiente al día siguiente, y que el resto suelen ser los de dos y tres días después con igual frecuencia.

Con esta consideración modélese la secuencia como un proceso markoviano, y

a) Represente diagrama de estados y matriz de transición.
b) Si procede, justifique y analice la distribución asintótica.
c) Analizar si existe algún requisito de la distribución del primer símbolo para que fuese estacionaria.
d) Analizar en una situación asintótica cual es la información mutua entre un símbolo y el siguiente.

e) Ídem entre un símbolo y el situado dos posiciones después.
f) Analizar en una situación asintótica cual es la incertidumbre de un solo símbolo, de dos sucesivos y de tres sucesivos.
g) Estudiar cuantos bits como mínimo harían falta en teoría para codificar una secuencia de un millón de símbolos ($L = 10^6$)

3.- Determinar la CERTEZA o FALSEDAD de las siguientes afirmaciones:

a) La tasa de entropía de una fuente markoviana de primer orden, que genera 3 símbolos según la siguiente matriz de transición

$$\Pi = \begin{pmatrix} 1/4 & 1/4 & 1/2 \\ 1/2 & 0 & 1/2 \\ 1/2 & 1/4 & 1/4 \end{pmatrix}$$

es de 7/5 bits/mensaje

b) En una cadena de Markov de primer orden, homogénea, irreducible y aperiódica la entropía relativa entre las distribuciones de probabilidad de la variable en dos estados consecutivos es monótamente decreciente.

4.- Si se sacan los naipes de uno en uno de una baraja española de 40 cartas y entre extracciones se vuelve a integrar en el mazo y a barajar, indicar cuál de las situaciones siguientes tiene mayor incertidumbre:

a) Que un naipe sea (o no) una copa.
b) Que un naipe sea (o no) una sota.
c) Que en dos naipes sucesivos haya alguna (o ninguna) copa.
d) Que en dos naipes sucesivos haya alguna (o ninguna) sota.

5.-En todo proceso markoviano homogéneo definido por una matriz de transición, dada una distribución de probabilidades del símbolo inicial que puede variar, si el proceso es:

a) aperiódico y reducible la solución asintótica es única.
b) periódico e irreducible puede que no exista distribución asintótica.
c) periódico y reducible puede que no exista distribución asintótica pero si existe es única.
d) aperiódico e irreducible puede que exista distribución asintótica pero que no sea única.

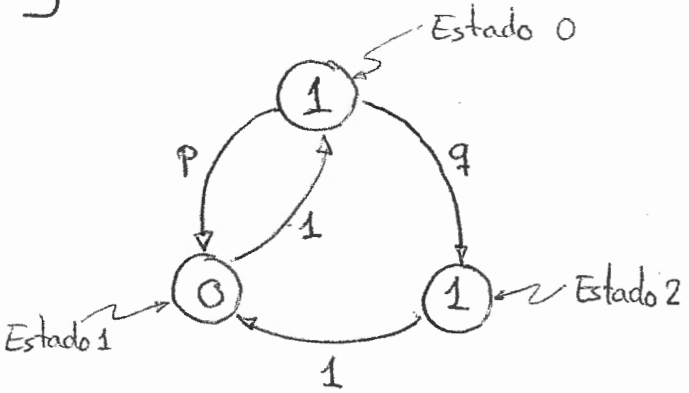
6.- En una cadena markoviana de primer orden, irreducible y aperiódica, la incertidumbre del símbolo n-ésimo condicionado al anterior

a) es monótonamente decreciente al crecer n
b) Es constante al crecer n

(1) $P\{\text{"}\cdot\text{"}\} = p$
$P\{\text{"}-\text{"}\} = q = 1-p$
} independientes

$\cdot \not\equiv$ '10'
$- \not\equiv$ '110'

a)



$$\Pi = \begin{pmatrix} 0 & p & q \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\vec{\mu}^A = \vec{\mu}^A \cdot \Pi \; ; \; \vec{\mu}^A = (\mu_0, \mu_1, \mu_2)$$

$$\left.\begin{aligned} \mu_0 &= \mu_1 \\ \mu_1 &= p\cdot\mu_0 + \mu_2 \\ \mu_2 &= q\cdot\mu_0 \\ \mu_0 + \mu_1 + \mu_2 &= 1 \end{aligned}\right\} \quad \vec{\mu}^A = \left(\frac{1}{2+q}, \frac{1}{2+q}, \frac{q}{2+q}\right) = \left(\frac{1}{3-p}, \frac{1}{3-p}, \frac{1-p}{3-p}\right)$$

b)

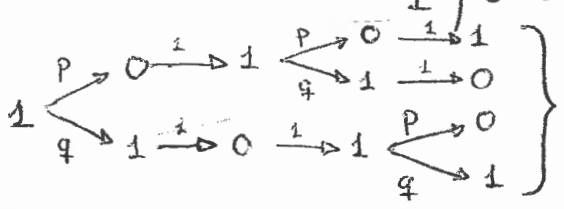
$P\{\text{"1 bit al azar sea el último '1' de una raya"}\} = \mu_2 = \frac{1-p}{3-p}$

$P\{\text{"1 bit al azar sea el primer '1' de una secuencia"}\} = \mu_0 = \frac{1}{3-p}$

c) En los primeros 5 bits de una secuencia se pueden dar:

10101
10110
11010
11011

$P\{\text{"0 en 1}^{er}\text{ bit"}\} = 0$ = suceso imposible
$P\{\text{"0 en 2}^{o}\text{ bit"}\} = p$
$P\{\text{"0 en 3}^{er}\text{ bit"}\} = 1-p$
$P\{\text{"0 en 4}^{o}\text{ bit"}\} = p^2$
$P\{\text{"0 en 5}^{o}\text{ bit"}\} = p\cdot(1-p) + (1-p)\cdot p = 2pq$



d) Significado de $\vec{\mu}^A$:

pasado un tiempo, la probabilidad de encontrarnos en el "Estado 0" (1er '1' de una subsecuencia) o en el "Estado 1" (bit '0') es la misma: $\frac{1}{3-p}$

Sin embargo, la de encontrarnos en el "Estado 2" (2° '1' del carácter raya) es $\frac{1-p}{3-p}$

homogéneo, irreducible, aperiódico $\Rightarrow \exists \vec{\mu}^A$ y es única

¿Será estacionaria?

H es constante $\Leftrightarrow$ homogén.

cadena irreducible $\Rightarrow$ si $\exists \vec{\mu}^A$ será ~~estacionaria~~ única

como es aperiódica $\Rightarrow \exists \vec{\mu}^A \Rightarrow \vec{\mu}^A$ NO es estacionaria

pues $\vec{\mu}^1 \neq \vec{\mu}^2 \neq \mu \ldots \neq \vec{\mu}^A$

e)

$$H(\mathcal{X}) = \sum_{i,j} \mu_i H(\text{fila}_i; H) =$$

$$= \frac{1}{2+q} H(0,p,q) + \frac{1}{2+q} \underbrace{H(1,0,0)}_{0} + \frac{q}{2+q} \underbrace{H(0,1,0)}_{0} =$$

$$= \frac{1}{2+q} \left[p \cdot \log_2\left(\frac{1}{p}\right) + q \cdot \log_2\left(\frac{1}{q}\right) \right]$$

f) si $H(\mathcal{X})|_{máx}$, ¿p?

Derivaremos la expresión de la entropía:

$$\frac{dH(\mathcal{X})}{dp} = \frac{3\log_2\left(\frac{1}{p}\right) - 2\log_2\left(\frac{1}{1-p}\right)}{(p-3)^2} = 0 \Leftrightarrow p = 0{,}56984$$

(usando Wolfram Alpha para resolverlo)

$H(\mathcal{X}) = 0'40553$

si $p = q = 1/2$

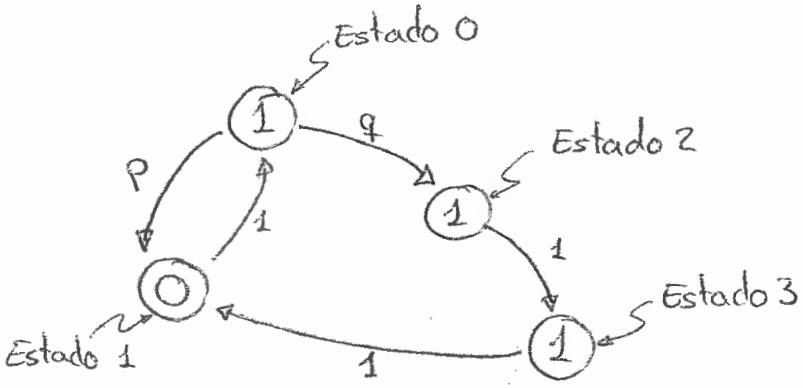
$$H(\mathcal{X}) = \frac{2}{5} H\left(0, \tfrac{1}{2}, \tfrac{1}{2}\right) + \frac{2}{5} \underbrace{H(1,0,0)}_{0} + \frac{1}{5} \underbrace{H(0,1,0)}_{0}$$

Con símbolos equiprobables (binario): $H(a,a) = 1$

Luego: $H(\mathcal{X})\Big|_{p=q=\frac{1}{2}} = \frac{2}{5} = 0'4$

g) Sea ahora: — ≠ '1110'

ga)



$$\Pi = \begin{pmatrix} 0 & p & q & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Es periódica! $\Rightarrow \nexists \vec{\mu}^A$ pues NO converge

$$\begin{cases} \mu_0 = \mu_1 \\ \mu_1 = p \cdot \mu_0 + \mu_3 \\ \mu_2 = q \cdot \mu_0 \\ \mu_3 = \mu_2 \\ \mu_0 + \mu_1 + \mu_2 + \mu_3 = 1 \end{cases}$$

No representa vector asintótico

$$\vec{\mu}^A = \left(\frac{1}{2(2-p)}, \frac{1}{2(2-p)}, \frac{1-p}{2(2-p)}, \frac{1-p}{2(2-p)} \right)$$

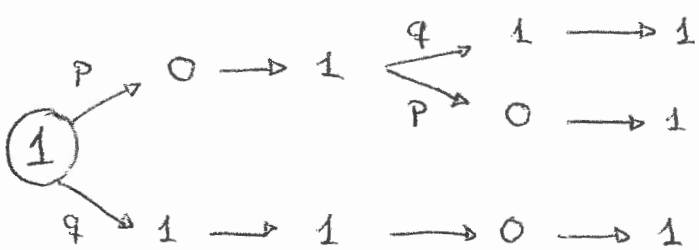
Si $\vec{\mu}^1 = \vec{\mu}^A$ sería estacionario

como $\vec{\mu}^1 \neq \vec{\mu}^A \Rightarrow$ No estacionario

gb) $P\{\text{"1 bit al azar sea último '1' de una raya"}\} = \mu_3 = \frac{1-p}{2(2-p)}$

$P\{\text{"1er bit sea el 1er bit de una secuencia"}\} = \mu_0 = \frac{1}{2(2-p)}$

gc)



$P\{\text{"1er bit} = 0\text{"}\} = 0$

$P\{\text{"2° bit} = 0\text{"}\} = p$

$P\{\text{"3er bit} = 0\text{"}\} = 0$

$P\{\text{"4° bit} = 0\text{"}\} = \frac{p^2 + 1 - p}{2}$

$P\{\text{"5° bit} = 0\text{"}\} = 0$

gd) idem apartado d) Es periódica a partir de 4 (4, 6, 8, 10, 12 ...)

ge) $H(\mathcal{X}) = \sum_{i,j} \mu_i H(f_{ij}) =$ | Como el sistema No converge, no se puede calcular $H(\mathcal{X})$

$$= \frac{1}{2(2-p)} \cdot H(0,p,q,0) + \frac{1}{2(2-p)} H(1,0,0,0) + \frac{1-p}{2(2-p)} H(0,0,0,1) +$$

$$+ \frac{1-p}{2(2-p)} H(0,1,0,0) =$$

$$= \frac{1}{2(2-p)} \cdot \left[p \cdot \log_2\left(\frac{1}{p}\right) + q \cdot \log_2\left(\frac{1}{q}\right) \right]$$

gf) si $H(\mathcal{X})|_{máx}$, ¿p?

Derivamos la expresión de la tasa de entropía:

$$\frac{d\,H(\mathcal{X})}{dp} = - \frac{\log_2\left(\frac{1}{1-p}\right) - 2\log_2\left(\frac{1}{p}\right)}{2(p-2)^2} = 0 \Leftrightarrow p = \frac{1}{2}(\sqrt{5}-1) = 0{,}61803$$

↳ por Wolfram Alpha

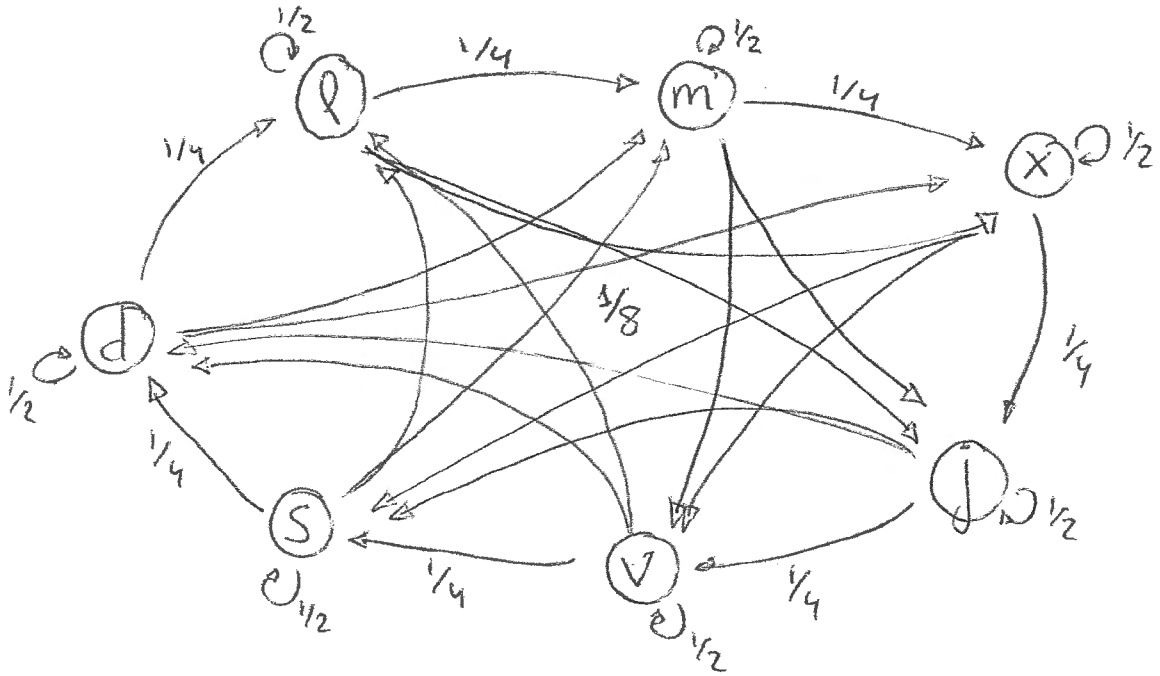
si $p = q = \frac{1}{2}$

$$H(\mathcal{X})|_{p=q=\frac{1}{2}} = \frac{1}{3} H\left(\frac{1}{2}, \frac{1}{2}, 1\right) = \frac{1}{3}$$

② $X \in \{l, m, x, j, v, s, d\}$

secuencia de longitud l

a)



$$H = \begin{pmatrix} 1/2 & 1/4 & 1/8 & 1/8 & 0 & 0 & 0 \\ 0 & 1/2 & 1/4 & 1/8 & 1/8 & 0 & 0 \\ 0 & 0 & 1/2 & 1/4 & 1/8 & 1/8 & 0 \\ 0 & 0 & 0 & 1/2 & 1/4 & 1/8 & 1/8 \\ 1/8 & 0 & 0 & 0 & 1/2 & 1/4 & 1/8 \\ 1/8 & 1/8 & 0 & 0 & 0 & 1/2 & 1/4 \\ 1/4 & 1/8 & 1/8 & 0 & 0 & 0 & 1/2 \end{pmatrix}$$

b) distribución asintótica: $\vec{\mu}^A = \vec{\mu}^A \cdot H = (\mu_0, \mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu$

$$\mu_0 + \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 + \mu_6 = 1$$

$$\left.\begin{aligned} \mu_0 &= \tfrac{1}{2}\mu_0 + \tfrac{1}{2}\mu_1 + \tfrac{1}{8}\mu_2 + \tfrac{1}{8}\mu_3 \\ \mu_1 &= \tfrac{1}{2}\mu_1 + \tfrac{1}{4}\mu_2 + \tfrac{1}{8}\mu_3 + \tfrac{1}{8}\mu_4 \\ \mu_2 &= \tfrac{1}{2}\mu_2 + \tfrac{1}{4}\mu_3 + \tfrac{1}{8}\mu_4 + \tfrac{1}{8}\mu_5 \\ \mu_3 &= \tfrac{1}{2}\mu_3 + \tfrac{1}{4}\mu_4 + \tfrac{1}{8}\mu_5 + \tfrac{1}{8}\mu_6 \\ \mu_4 &= \tfrac{1}{2}\mu_4 + \tfrac{1}{4}\mu_5 + \tfrac{1}{8}\mu_6 + \tfrac{1}{8}\mu_0 \\ \mu_5 &= \tfrac{1}{2}\mu_5 + \tfrac{1}{4}\mu_6 + \tfrac{1}{8}\mu_0 + \tfrac{1}{8}\mu_1 \end{aligned}\right\} \quad \mu_i = 1/7 \;\; \forall i = 0, 1, 2, \dots 6$$

$$\vec{\mu}^A = \left(\tfrac{1}{7}, \tfrac{1}{7}, \tfrac{1}{7}, \tfrac{1}{7}, \tfrac{1}{7}, \tfrac{1}{7}, \tfrac{1}{7}\right)$$

Nos encontramos ante un proceso aperiódico, pues no tiene ningún estado que se repita sobre sí mismo.

Es irreducible, pues todos los estados están "conectados" con todos (directa o indirectamente)

Es un proceso homogéneo, pues Π no varía con el tiempo

c) Si $\vec{\mu}^1 = \vec{\mu}^A \Rightarrow \vec{\mu}^n = \vec{\mu}^A \Rightarrow$ estacionaria

d) $I(X_{n-1}; X_n) = H(X_n) - H(X_n / X_{n-1})$

siendo una situación asintótica:

$$H(X_n) = 7 \cdot \left(\frac{1}{7} \cdot \log_2(7) \right) = 2,8074$$

$$H(X_n / X_{n-1}) = H(X) = \sum_i \mu_i \cdot H(\text{fila i de } \Pi) =$$

$$= 7 \cdot \left[\frac{1}{7} \cdot H\left(\tfrac{1}{2}, \tfrac{1}{4}, \tfrac{1}{8}, \tfrac{1}{8}, 0, 0, 0\right) \right] =$$

$$= \frac{1}{2} \cdot \log_2(2) + \frac{1}{4} \log_2(4) + 2 \cdot \frac{1}{8} \log_2(8) = 1,75$$

Luego: $I(X_{n-1}; X_n) = 2,8074 - 1,75 = \underline{1,0574 \text{ bits}}$

e) $I(X_{n-2}; X_n) = \underbrace{H(X_n)}_{2'8074} - H(X_n / X_{n-2})$

$$H(X_n / X_{n-2}) = \sum_i \mu_i \cdot H(\text{fila i de } \Pi^2)$$

Las propabilidades de cambios de estado a simbolos separados por otro símbolo vienen detalladas por Π^2

siendo $\Pi^2 = \Pi \cdot \Pi$ (producto matricial)

$$H^2 = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{3}{16} & \frac{3}{16} & \frac{5}{64} & \frac{1}{32} & \frac{1}{64} \\ \frac{1}{64} & \frac{1}{4} & \frac{1}{4} & \frac{3}{16} & \frac{3}{16} & \frac{5}{64} & \frac{1}{32} \\ \frac{1}{32} & \frac{1}{64} & \frac{1}{4} & \frac{1}{4} & \frac{3}{16} & \frac{3}{16} & \frac{5}{64} \\ \frac{5}{64} & \frac{1}{32} & \frac{1}{64} & \frac{1}{4} & \frac{1}{4} & \frac{3}{16} & \frac{3}{16} \\ \frac{3}{16} & \frac{5}{64} & \frac{1}{32} & \frac{1}{64} & \frac{1}{4} & \frac{1}{4} & \frac{3}{16} \\ \frac{3}{16} & \frac{3}{16} & \frac{5}{64} & \frac{1}{32} & \frac{1}{64} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{16} & \frac{3}{16} & \frac{5}{64} & \frac{1}{32} & \frac{1}{64} & \frac{1}{4} \end{pmatrix}$$

$$H(X_n / X_{n-2}) = 7 \cdot \frac{1}{7} \cdot \underbrace{H\left(\frac{1}{4}, \frac{1}{4}, \frac{3}{16}, \frac{3}{16}, \frac{5}{64}, \frac{1}{32}, \frac{1}{64}\right)} =$$

$$= 7 \cdot \frac{1}{7} \cdot \left(2 \times \frac{1}{2} + 2 \times 0'4528 + 0'2873 + 0'15625 + 0'09375\right) =$$

$$= 2'4429 \text{ bits}$$

$$I(X_n ; X_{n-2}) = 2,8074 - 2,4429 = 0,3644 \text{ bits}$$

f) $H(X_n) = 2,8074$ bits

$$H(X_n, X_{n+1}) = H(X_n) + H(X_{n+1} / X_n) = 2,8074 + 1,75 = 4,557 \text{ bits}$$

$$H(X_n, X_{n+1}, X_{n+2}) = H(X_n) + H(X_{n+1} / X_n) + H(X_{n+2} / X_{n+1}) =$$

$$= 2,8074 + 1,75 + 1,75 = 6,3074 \text{ bits}$$

g) una secuencia de 10^6 símbolos requerirá:

$$H(X) \cdot 10^6 = 1,75 \cdot 10^6 = 1,75 \text{ Mbits}$$

(3)

a) $H(\mathcal{X})$ de una fuente markoviana 1er orden, 3 simb $= \frac{7}{5}$

siendo $\Pi = \begin{pmatrix} 1/4 & 1/4 & 1/2 \\ 1/2 & 0 & 1/2 \\ 1/2 & 1/4 & 1/4 \end{pmatrix}$

$$H(\mathcal{X}) = \sum \mu_i \cdot H(\text{fila}_i)$$

$\vec{\mu}^A$:

$$\left.\begin{aligned} \mu_0 &= \mu_0 \tfrac{1}{4} + \mu_1 \tfrac{1}{2} + \mu_2 \tfrac{1}{2} \\ \mu_1 &= \mu_0 \tfrac{1}{4} + 0 + \tfrac{1}{4}\mu_2 \\ \mu_2 &= \mu_0 \tfrac{1}{2} + \mu_1 \tfrac{1}{2} + \mu_2 \tfrac{1}{4} \\ \mu_0 + \mu_1 + \mu_2 &= 1 \end{aligned}\right\} \quad \vec{\mu}^A = \left(\tfrac{2}{5}, \tfrac{1}{5}, \tfrac{2}{5}\right)$$

Luego: $H(\mathcal{X}) = \frac{2}{5} \cdot H\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{2}\right) + \frac{1}{5} H\left(\frac{1}{2}, 0, \frac{1}{2}\right) + \frac{2}{5} H\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\right) =$

$$= \frac{2}{5} \cdot \left[\frac{1}{2}\log_2(2) + 2\frac{1}{4}\log_2(4)\right] + \frac{1}{5} \cdot 1 + \frac{2}{5}\left[\frac{1}{2}\log_2(2) + 2 \cdot \frac{1}{4}\log_2(4)\right] =$$

$$= \frac{2}{5} \cdot \left(\frac{1}{2} + 1\right) + \frac{1}{5} + \frac{2}{5}\left(\frac{1}{2} + 1\right) = \frac{7}{5} \Rightarrow \underline{\text{Verdad}}$$

b) Si es homogénea, las probabilidades de cambio de estado permanecen constantes, luego la entropía no fluctúa: permanece constante.

si cte $\neq$ monótona decreciente $\Rightarrow$ <u>Falso</u>

(4) 40 cartas: extracciones con reintegración

a) ser o no copa:

ser copa: $\frac{1}{4}$

No ser copa: $\frac{3}{4}$

b) ser o no sota:

ser sota: $\frac{1}{10}$

no ser sota: $\frac{9}{10}$

c) sacar $\begin{cases} \text{alguna} \\ \text{ninguna} \end{cases}$ copa en 2 intentos

alguna: $\frac{1}{4} \cdot \frac{1}{4} + 2 \times \left(\frac{1}{4} \cdot \frac{3}{4}\right) = \frac{7}{16}$

ninguna: $\frac{3}{4} \cdot \frac{3}{4} = \frac{9}{16}$

d) sacar $\begin{cases} \text{alguna} \\ \text{ninguna} \end{cases}$ sota en 2 intentos

alguna: $\frac{1}{10} \cdot \frac{1}{10} + 2 \times \left(\frac{1}{10} \cdot \frac{9}{10}\right) = \frac{19}{100}$

ninguna: $\frac{9}{10} \cdot \frac{9}{10} = \frac{81}{100}$

Sabiendo que la entropía es mayor cuanto más igualadas sean las probabilidades de los sucesos, podemos decantarnos por que la opción b) tiene mayor incertidumbre, pues es la opción con mayor disparidad entre sucesos.

(5) proceso markoviano homogéneo con $\vec{\mu}^1$ variable:

a) si aperiódico y reducible $\Rightarrow \vec{\mu}^A$ única

FALSO: si es aperiódico, diferentes $\vec{\mu}^1$ producirán diferentes $\vec{\mu}^A$

b) si periódico e irreducible $\Rightarrow$ puede que no exista $\vec{\mu}^A$

VERDADERO: si es periódico no converge $\Rightarrow \nexists \vec{\mu}^A$

c) periódico y reducible $\Rightarrow$ puede que $\nexists \vec{\mu}^A$ pero si $\exists$ es única

FALSO:

d) aperiódico e irreducible $\Rightarrow$ puede que $\exists \vec{\mu}^A$ pero no sea única

FALSO:

(6) cadena markoviana de 1er orden irreducible y aperiódica

$H(X_n / X_{n-1})$ es:

a) decreciente al crecer n

b) constante al crecer n ← por ser estacionario $\vec{\mu}^n = \vec{\mu}^{n-1}$

TERCER GRUPO DE EJERCICIOS - Curso 2013/2014 ENTREGA:

24 de Octubre.

1.- Una fuente genera mensajes según una distribución proporcional a {5,1,4,8,3,7,2,y 6}. Se pide diseñar los correspondientes códigos prefijo, analizar su desigualdad de Kraft, calcular su longitud media y comparar con la incertidumbre para:

a) Código binario con el método de Shannon
b) Código binario óptimo
c) Código ternario óptimo
d) Código binario alfabético con método (Shannon)-Elias-Fano
e) Código alfabético de Fano
f) Recortar los códigos en los casos d) y e) si es posible

2.- Una fuente de información X emite símbolos independientes X={A, B, C} con distribución de probabilidades Pr(x)={0'7, 0'15, 0'15}.

a) Determinar la entropía de la fuente.
Se pretende codificar dicha fuente con un código binario cuya longitud media difiera en menos de 2% de la entropía de la fuente.
b) Proponga un esquema de codificación óptimo de símbolos individuales para dicha fuente. Calcule la longitud media del código. Justifique que dicha codificación es óptima.

En caso de que la eficiencia no sea la deseada, se propone como alternativa realizar una extensión de fuente de orden n= 2, 3, ... En la extensión de fuente, se codifican secuencias de n símbolos de la fuente (x_1, x_2, ..., x_n), considerando que los x_i símbolos son independientes. Empezando con n= 2, se pide:

c) Determine la distribución conjunta de n símbolos de la fuente.
d) Proponga un esquema de codificación de bloque de n símbolos.
e) Calcule la longitud media del código resultante.
f) Si el código resultante difiere en más de un 5% de la entropía de la fuente, repita los apartados c), d) y e) incrementando el valor de n (3, 4, ...) hasta que consiga el objetivo.
[NOTA: utilice suficiente precisión para analizar los resultados pedidos].

3.- Supongamos una fuente como la del ejercicio 2) de la segunda entrega, donde la probabilidad de repetición, de pasar al día siguiente o al posterior son de 1/2, 1/4 y 1/4 respectivamente

a) diseñar un esquema de codificación eficiente de las secuencias.
b) aplicar el esquema de codificación al ejemplo inicial (se repite aquí por comodidad) suponiendo una situación asintótica y que el símbolo anterior a la secuencia dada YA está codificado.
(Nota: la secuencia del enunciado es: l l m m m j j j v v s d l x x x v v d d)
c) repetir el análisis si las probabilidades fuesen (0,8, 0,1 y 0,1)
d) codificar de nuevo esta secuencia.

4.- Sea una cadena de Markov de primer orden homogénea con la matriz de probabilidades de transición siguiente:

$$\Pi = \begin{matrix} 0'89 & 0'055 & 0'055 \\ 1/2 & 1/4 & 1/4 \\ 0 & 1/2 & 1/2 \end{matrix}$$

Se pide:

a) Calcular la tasa de entropía
b) Diseñar una codificación eficiente de la fuente
c) Calcular la longitud media del código anterior y comparar con la tasa de entropía

5.- Clasificar los siguientes códigos:
a) { 110, 010, 101, 0111, 0110}
b) {011, 101, 1100, 010}
c) {AA, AB, BA, AAB, BAA, AB}
d) {AA, AAB, ABB, BABBA, BBAA}

6.- Para que un código fuente binario sea óptimo siempre es imprescindible que:

a) No haya palabras-código con símbolos prescindibles (recortables).
b) El número de mensajes ha de ser n(D-1) + 1.
c) Las palabras-código de los mensajes más probables sean más cortas que las de los menos probables.
d) Las palabras-código de los dos mensajes menos probables han de coincidir en todos los bits salvo el último.

7.- Razonar la veracidad de la siguiente sentencia:
a) Con las siguientes longitudes de las palabras código {1,1,2,2,2,3,3,3} se puede construir un código ternario unívocamente descodificable

(1) distribución proporcional a $\{5, 1, 4, 8, 3, 7, 2, 6\}$ (A B C D E F G H)

normalizando: $\{\frac{5}{36}, \frac{1}{36}, \frac{1}{9}, \frac{2}{9}, \frac{1}{12}, \frac{7}{36}, \frac{1}{18}, \frac{1}{6}\}$

diseño de código, desigualdad de Kraft y longitud media

a) <u>código binario con método de Shannon:</u>

El código subóptimo de Shannon establece las longitudes de los códigos como: $l_i = \lceil \log_2(\frac{1}{p_i}) \rceil$

$l_1 = 3 \longrightarrow 000$

$l_2 = 6 \longrightarrow 101010$

$l_3 = 4 \longrightarrow 1000$

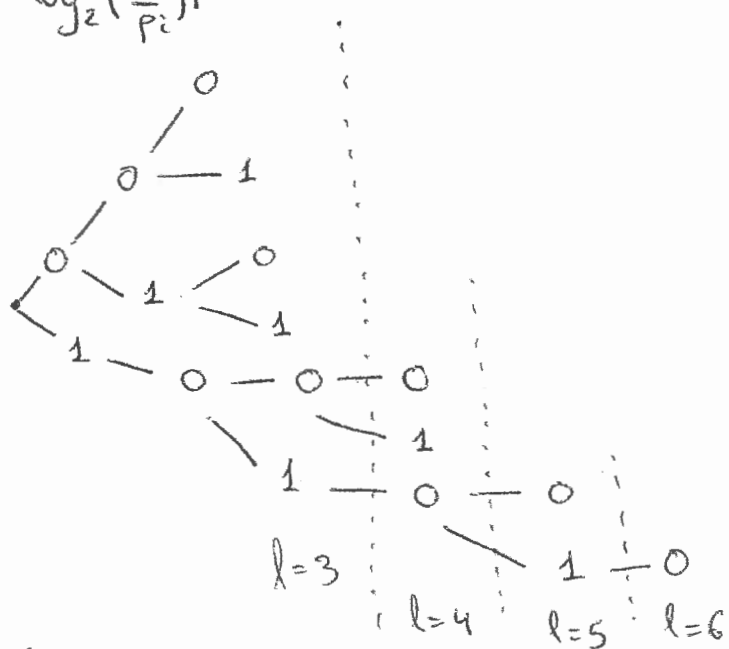
$l_4 = 3 \longrightarrow 010$

$l_5 = 4 \longrightarrow 1001$

$l_6 = 3 \longrightarrow 001$

$l_7 = 5 \longrightarrow 10100$

$l_8 = 3 \longrightarrow 011$



Desigualdad de Kraft: $\sum D^{-l_i} \leq 1$

$$2^{-3} + 2^{-6} + 2^{-4} + 2^{-3} + 2^{-4} + 2^{-3} + 2^{-5} + 2^{-3} = 0,6718 \leq 1 \quad \underline{ok.}$$

$$L = \sum_i p_i l_i = 3,388 \text{ bits}$$

$$H(X) = \frac{5}{36}\log_2\left(\frac{36}{5}\right) + \frac{1}{36}\log_2(36) + \frac{1}{9}\log_2(9) + \frac{2}{9}\log_2\left(\frac{9}{2}\right) + \frac{1}{12}\log_2(12) + \frac{7}{36}\log_2\left(\frac{36}{7}\right) + \frac{1}{18}\log_2(18) + \frac{1}{6}\log_2(6) = 2,7942 \text{ bits}$$

$$\begin{cases} H(X) \leq L \leq H(X)+1 \\ 2,7942 \leq 3,388 \leq 3,7942 \quad \underline{o.k.} \end{cases}$$

b) código binario óptimo: Huffman

X	p(x)	p'(x)	p''(x)	p'''(x)	p^IV(x)	p^V(x)	p^VI(x)	c(x)
D	2/9 →	2/9 →	2/9 →	9/36 →	1/3 →	15/36 →	21/36 [0]	10
F	7/36 →	7/36 →	7/36 →	2/9 →	9/36 →	1/3 [0]	15/36 [1]	11
H	1/6 →	1/6 →	1/6 →	7/36 →	2/9 [0]	9/36 [1]		000
A	5/36 →	5/36 →	1/6 →	1/6 [0]	7/36 [1]			010
C	1/9 →	1/9 →	5/36 [0]	1/6 [1]				011
E	1/12 →	1/12 [0]	1/9 [1]					0010
G	1/18 [0]	1/12 [1]						00110
B	1/36 [1]							00111

$$L = \sum_i p_i \cdot l_i = 2,8\overline{33} \text{ bits} > H(X) = 2,79 \text{ bits}$$

$$L_{\text{Huffman bin}} = 2,8\overline{33} < L_{\text{Shannon}} = 3,3\overline{88}$$

Kraft: $\sum D^{-l_i} \leq 1 \Leftrightarrow 2\cdot 2^{-2} + 3\cdot 2^{-3} + 2^{-4} + 2\cdot 2^{-5} = 1 \leq 1$ o.k.

c) código ternario óptimo: Huffman

X	p(x)	p'(x)	p''(x)	p'''(x)	c(x)
D	2/9 →	2/9 →	15/36 →	17/36 [0]	00
F	7/36 →	7/36 →	2/9 [0]	15/36 [1]	01
H	1/6 →	1/6 →	7/36 [1]	* [2]	02
A	5/36 →	1/6 [0]	1/6 [2]		11
C	1/9 →	5/36 [1]			12
E	1/12 [0]	1/9 [2]			110
G	1/18 [1]				111
B	1/36 [2]				112

↳ necesitamos inventarnos otro símbolo con p = 0

$$L = \sum_i p_i \cdot l_i = 2,1\overline{66} \text{ trits} \qquad L > H(X) \text{ o.k.}$$

$$H(X) = 2,7942 \text{ bits} = 2,7942 \cdot \frac{\log_{10}(2)}{\log_{10}(3)} \text{ trits} = 1,7629 \text{ trits}$$

Kraft: $\sum D^{-l_i} \leq 1 \Leftrightarrow 5\cdot 3^{-2} + 3\cdot 3^{-3} = 0,\overline{66} < 1$ o.k.

d) código binario alfabético: Shannon-Elías-Fano

x_i	$p(x_i)$	$F(x_i)$	$\tilde{F}(x_i)=F(x_{i-1})+\frac{1}{2}p(x_i)$	$l(x)=\lceil \log_2(\frac{1}{p})\rceil+1$	$c(x)$
A	$5/36$	$5/36$	$0'0694 \rightarrow 0'0001$	4	0001
B	$1/36$	$6/36$	$0'15277 \rightarrow 0'0010011$	7	0010011
C	$1/9$	$10/36$	$0'2\overline{22} \rightarrow 0'00111$	5	00111
D	$2/9$	$18/36$	$0'3\overline{88} \rightarrow 0'0110$	4	0110
E	$1/12$	$21/36$	$0'54\overline{166} \rightarrow 0'10001$	5	10001
F	$7/36$	$28/36$	$0'68\overline{055} \rightarrow 0'1010$	4	1010
G	$1/18$	$30/36$	$0'8\overline{0555} \rightarrow 0'110011$	6	110011
H	$1/6$	$36/36$	$0'9\overline{166} \rightarrow 0'1110$	4	1110

$L = \sum_i p_i \cdot l_i = 4,3\overline{88}$ bits $> H(x) = 2,79$ bits

Kraft: $\sum D^{-l_i} \leq 1 \Leftrightarrow 4\cdot 2^{-4} + 2^{-7} + 2\cdot 2^{-5} + 2^{-6} = 0'3359 < 1$ o.k.

e) código alfético de Fano:

x	p(x)	c(x)
D	$8/36$	00
F	$7/36$	010
H	$6/36$	011
A	$5/36$	100
C	$4/36$	101
E	$3/36$	110
G	$2/36$	1110
B	$1/36$	1111

$L = \sum p_i \cdot l_i = 3,36$ bits $> H(x) = 2,79$ bits

$L_{Fano} < L_{Sh\text{-}E\text{-}F}$

Kraft: $\sum D^{-l_i} \leq 1 \Leftrightarrow 6\cdot 2^{-3} + 2\cdot 2^{-4} = 0'875 < 1$ o.k.

f) recortar códigos de apartados d) y e)

d) Sh-E-F:

x	c(x)	$c_r(x)$
A	0001	000
B	00100 11	0010
C	00 111	0011
D	0110	01
E	10001	100
F	1010	101
G	1100 11	110
H	1110	111

$L_{código\ orig} = 4{,}388\ \overline{8}$ bits

$L_{código\ recortado} = 2{,}805\ \overline{5}$ bits $\approx H(X) = 2{,}79$ bits

El código del apartado e NO se puede recortar.

② $X = \{A, B, C\}$ independientes $P_r = \{0'7, 0'15, 0'15\}$

a) $H(X) = \sum_{\forall x} p(x) \cdot \log_2\left(\frac{1}{p(x)}\right) = 1,18129$ bits

b) código binario $|L - H(X)| < 0{,}02$

Huffman: es codificación óptima por definición

x	p(x)			
A	0'7	→ 0'7	0	A → 0
B	0'15 (0)	0'3	1	B → 10
C	0'15 (1)			C → 11

$L = 1'6$ bits

$|1,18 - 1,6| = 0'42 > 0{,}02$

NO podemos cumplirlo

↳ haremos extensión

c) extensión de fuente de orden $n = 2, 3, 4 \ldots$

n=2 $Y = \{AA, AB, AC, BA, BB, BC, CA, CB, CC\}$

como son indep. $\Rightarrow P(X_1 X_2) = P(X_1) \cdot P(X_2)$

$P(Y) = \{0'49, 0'105, 0'105, 0'105, 0'0225, 0'0225, 0'105, 0'0225, 0'0225\}$

d) Huffman: óptimo por definición

X	$p(x)$	$p'(x)$	$p''(x)$	$p'''(x)$	$p^{IV}(x)$	$p^{V}(x)$	$p^{VI}(x)$	$p^{VII}(x)$	$c(x)$
AA	0'49 →	0'49 →	0'49 →	0'49 →	0'49 →	0'49 →	0'49	0'51 | 0	1
AB	0'105 →	0'105 →	0'105 →	0'105	0'195	0'21	0'3 | 0	0'49 | 1	001
AC	0'105 →	0'105 →	0'105 →	0'105	0'105	0'195 | 0	0'21 | 1		010
BA	0'105 →	0'105 →	0'105 →	0'105	0'105 | 0	0'105 | 1			011
CA	0'105 →	0'105 →	0'105 →	0'05 | 0	0'105 | 1				0000
BB	0'0225	0'045 →	0'045 | 0	0'09 | 1					000110
BC	0'0225	0'0225 | 0	0'045 | 1						000111
CB	0'0225 | 0	0'0225 | 1							000100
CC	0'0225 | 1								000101

e) $L = \sum p_i \cdot l_i = 2{,}395$ bits

f) $H(Y) = 0'49 \cdot \log_2\left(\frac{1}{0'49}\right) + 4 \cdot 0'105 \cdot \log_2\left(\frac{1}{0'105}\right) + 4 \cdot 0'0225 \cdot \log_2\left(\frac{1}{0'0225}\right) = 2'3625$ bits

$|L - H(X)| = 0'0325 < 0'05$ ok.

③ sean los estados $\{+0, +1, +2\}$ los que produce la fuente

X	$p(x)$	$p'(x)$
+0	1/2 →	1/2 | 0
+1	1/4 | 0 →	1/2 | 1
+2	1/4 | 1	

$\Rightarrow$ +0 ⇒ 0, +1 ⇒ 10, +2 ⇒ 11 por Huffman

b) l l m m m j j j r r s d l x x x r r d d

X - 0 - 10 - 0 - 0 - 11 - 0 - 0 - 10 - 0 - 10 - 10 - 10 - 11 - 0 - 0 - 11 - 0 - 11 - 0

↑ conocido

c) sea ahora $P = \{0'8, 0'1, 0'1\}$

Se podría codificar con Huffman, quedando el mismo resultado que el apartado anterior.

No obstante, debido a la alta probabilidad de permanecer en el primer estado (0'8) frente a las bajas probabilidades de permanecer en los otros estados (0'2) parece lógico aplicar la codificación de recorrido (Run-Length)

④ cadena de Markov de 1er orden homogénea

$$\Pi = \begin{pmatrix} 0'89 & 0'055 & 0'055 \\ 1/2 & 1/4 & 1/4 \\ 0 & 1/2 & 1/2 \end{pmatrix}$$

a) $H(X) = \sum_i \mu_i \cdot H(\text{fila } i \text{ de } \Pi)$

$H(\text{fila } 1) = H(0'89, 0'055, 0'055) = 0'6099$ bits

$H(\text{fila } 2) = H(1/2, 1/4, 1/4) = 3/2$ bits

$H(\text{fila } 3) = H(1/2, 1/2) = 1$ bit

$\vec{\mu}^A = \vec{\mu}^A \cdot \Pi$; $\vec{\mu}^A = (\mu_1, \mu_2, \mu_3)$

$$\left.\begin{array}{l} \mu_1 = 0'89\mu_1 + 0'5\mu_2 \\ \mu_2 = 0'055\mu_1 + \frac{1}{4}\mu_2 + \frac{1}{4}\mu_3 \\ \mu_3 = 0'055\mu_1 + \frac{1}{4}\mu_2 + \frac{1}{2}\mu_3 \\ \mu_1 + \mu_2 + \mu_3 = 1 \end{array}\right\} \quad \begin{array}{l} \mu_1 = 0'6944 \\ \mu_2 = 0'15277\overline{7} \\ \mu_3 = 0'25277\overline{7} \end{array}$$

así pues: $H(X) = \mu_1 \cdot H(\text{fila } 1) + \mu_2 H(\text{fila } 2) + \mu_3 H(\text{fila } 3) = 0'8056$ b

b) Huffman:

x	p(x)		p'(x)	
A	$\mu_1 = 0'69$		$\rightarrow 0'69$	0
B	$\mu_2 = 0'15$	0	$\rightarrow 0'3$	1
C	$\mu_3 = 0'15$	1		

A ⇒ 0

B ⇒ 10

C ⇒ 11

c) $L = \sum_i p_i l_i = 1,3055$ bits $>$ $H(X) = 0'8054$ bits

No demasiado eficiente

Sería mejor codificación con transiciones en vez de con estados

(5)

a) {110, 010, 101, 0111, 0110}

código prefijo

b) {011, 101, 1100, 010}

código prefijo

c) {AA, AB, BA, AAB, BAA, AB}

código singular (dos palabras con código AB)

d) {AA, AAB, ABB, BABBA, BBAA}

código NO unívocamente descodificable

pues {AA + BABBA + ...} (AAB ABB ...)

la extensión del código es No singular

(6) para que un código binario sea óptimo; siempre es imprescindible que:

a) No haya símbolos prescindibles:

Verdad: un símbolo prescindible NO haría L mínima

b) número de mensajes = $n(D-1)+1$

Falso: sin sentido

c) si $p(x) \uparrow \Rightarrow l(x) \downarrow$

Verdad: a mayor p, "saldrá" más veces, por lo que engordará $L = \sum_i p_i \cdot l_i$

d) c(x) de los 2 mensajes menos probables han de coincidir en todos los bits salvo en el último

Falso: deberían tener la misma longitud, pero podría NO ser ni siquiera así

(7) con longitudes {1,1,2,2,2,3,3,3} se construye un c. univ. descod.

Falso: No cumple McMillan: $\sum_i 3^{-l_i} = 1{,}11 \not\leq 1$

CUARTO GRUPO DE EJERCICIOS - Curso 2013/2014

ENTREGA: 28 de Noviembre

Versión: 1.0.

ENUNCIADOS

1.- Calcular la capacidad de los siguientes canales:

a) $\Pi = \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 0 & 1 \end{bmatrix}$

b) $\Pi = \begin{bmatrix} 0{,}9 & 0{,}05 & 0 & 0{,}05 \\ 0{,}05 & 0{,}9 & 0{,}05 & 0 \\ 0 & 0{,}05 & 0{,}9 & 0{,}05 \\ 0{,}05 & 0 & 0{,}05 & 0{,}9 \end{bmatrix}$

c) Considérense las simetrías para buscar la solución derivando o por cálculo numérico:

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

2.- Las siguientes palabras pertenecen a un CÓDIGO LINEAL:

1 0 1 0 1 0 0 1 0 1 1 0 0
0 0 1 1 1 0 1 1 0 0 1 0 1
0 1 0 0 1 1 0 1 0 1 1 1 1
1 0 0 1 1 0 1 0 1 1 1 0 1
0 1 1 0 0 1 1 1 0 0 1 0 0
0 1 0 1 1 1 0 0 0 0 0 0 1

Se pide:

a) Obtener el conjunto de palabras código
b) ¿Cuáles son sus dimensiones?
c) Obtener la matriz generadora sistemática
d) Obtener la matriz de paridad H
e) Calcular cual es el mínimo número de columnas de la matriz H que son linealmente dependientes
f) Analizar las propiedades detectoras y correctoras.
g) Calcular la distribución de pesos de las palabras código (A_i)
h) Analizar cuáles serían los líderes de cogrupo de la agrupación canónica (tabla estándar). ¿Cuántos habrá de peso 3?
i) Si se transmiten las palabras código por un canal BSC con $p=10^{-4}$, ¿cuál sería la probabilidad de no detección?
j) Si se corrige, ¿Cuál es la probabilidad de no corrección?
k) Calcular ambas probabilidades en el caso híbrido.

3.- Si en un código lineal, se modifica el conjunto de palabras código por las palabras de otra fila de su tabla estándar, analice si el conjunto de palabras resultante forma o no un código lineal y calcule la distancia mínima entre los miembros de dicho conjunto en función de la del código original.

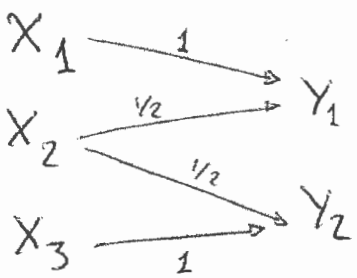
4.- Determine la certeza o falsedad de las siguientes sentencias:

a) En un código lineal, las filas de la matriz generadora son ortogonales a las columnas de la matriz de comprobación de paridad.
b) En un código lineal, si se conoce el síndrome de un error, es posible calcular el conjunto de errores del canal que han podido suceder.
c) Para generar un código lineal C(n,k), es válido cualquier subespacio vectorial S_k de dimensión k del espacio vectorial V_n de dimensión n.
d) En la distribución de pesos de un código lineal, A_i es igual a cero si i es mayor que cero y menor que la distancia mínima del código.
e) En un código perfecto utilizado en modo de corrección pura, es posible corregir algunos errores de peso mayor que la capacidad de corrección del código.
f) En un código lineal, a cada error del canal le corresponde un síndrome distinto.

5.- Un código que tenga una distancia Hamming de 8 y un n de 255, ¿cuál es el número mínimo de bits de redundancia que necesita?

(1)

a) $H = \begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 0 & 1 \end{pmatrix}$



$C = \max_{p(x)} I(X;Y) = \max \{ H(Y) - H(Y/X) \}$

será máximo si son equiprobables, pues aumentará la entropía

$H(Y)\Big|_{\substack{\text{máximo} \\ \text{(equiprob.)}}} = \log_2(2) = 1$

$H(Y/X) = \sum_{\forall x} H(Y/X=x) \cdot p(X=x)$

$H(Y/X=x_1) = 0$, pues $X_1 \to Y_1$

$H(Y/X=x_3) = 0$, pues $X_3 \to Y_2$

$H(Y/X=x_2) = \frac{1}{2}$, pues $X_2 \xrightarrow{1/2} Y_1$, $X_2 \xrightarrow{1/2} Y_2$

$H(Y/X) = \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$

$C = 1 - \frac{1}{6} = \frac{5}{6}$ bps

b) $H = \begin{pmatrix} 0,9 & 0'05 & 0 & 0'05 \\ 0'05 & 0'9 & 0'05 & 0 \\ 0 & 0'05 & 0'9 & 0'05 \\ 0'05 & 0 & 0'05 & 0'9 \end{pmatrix}$ Canal simétrico

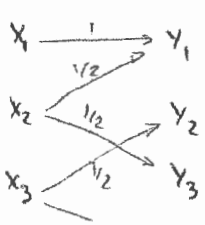
$C = \log_2(4) - H(\text{fila}) = 2 - \left[0'9 \cdot \log_2\left(\frac{1}{0'9}\right) + 0'1 \cdot \log_2\left(\frac{1}{0'05}\right) \right] = 2 - 0'57 = 1'43$

c) $H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$C = \max_{p(x)} I(X;Y) = \max \{ H(Y) - H(Y/X) \}$

$H(Y/X) = \sum_{\forall x} H(Y/X=x_i) \cdot p(x_i) =$

$= H\left(\frac{1}{2}, 0, \frac{1}{2}, 0\right) \cdot p + H\left(0, \frac{1}{2}, 0, \frac{1}{2}\right) q = p + q = 1$ bit



(2) Siendo:

$\vec{V}_1 = 10101\ 00101\ 100$ (peso 6)
$\vec{V}_2 = 00111\ 01100\ 101$ (peso 7)
$\vec{V}_3 = 01001\ 10101\ 111$ (peso 8)
$\vec{V}_4 = 10011\ 01011\ 101$ (peso 8)
$\vec{V}_5 = 01100\ 11100\ 100$ (peso 6)

} linealmente independientes

$\vec{V}_6 = 01011\ 10000\ 001 = \vec{V}_2 + \vec{V}_5$

obtenemos:

(peso)

$\vec{V}_1 + \vec{V}_2 = 10010\ 01001\ 001$ (5)
$\vec{V}_1 + \vec{V}_3 = 11100\ 10000\ 011$ (6)
$\vec{V}_1 + \vec{V}_4 = 00110\ 01110\ 001$ (6)
$\vec{V}_1 + \vec{V}_5 = 11001\ 11001\ 000$ (6)
$\vec{V}_2 + \vec{V}_3 = 01110\ 11001\ 010$ (7)
$\vec{V}_2 + \vec{V}_4 = 10100\ 00111\ 000$ (5)
$\vec{V}_2 + \vec{V}_5 = 01011\ 10000\ 001$ (5)
$\vec{V}_3 + \vec{V}_4 = 11010\ 11110\ 010$ (8)
$\vec{V}_3 + \vec{V}_5 = 00101\ 01001\ 011$ (6)
$\vec{V}_4 + \vec{V}_5 = 11111\ 10111\ 001$ (10)

deberemos añadir: 00000 00000 000 (0)

$\vec{V}_1 + \vec{V}_2 + \vec{V}_3 = 11011\ 11100\ 110$ (9)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_4 = 00001\ 00010\ 100$ (3)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_5 = 11110\ 10101\ 101$ (9)
$\vec{V}_1 + \vec{V}_3 + \vec{V}_5 = 10000\ 01100\ 111$ (6)
$\vec{V}_1 + \vec{V}_4 + \vec{V}_5 = 01010\ 10010\ 101$ (6)
$\vec{V}_2 + \vec{V}_3 + \vec{V}_4 = 11101\ 10010\ 111$ (9)
$\vec{V}_2 + \vec{V}_3 + \vec{V}_5 = 00010\ 00101\ 110$ (5)
$\vec{V}_2 + \vec{V}_4 + \vec{V}_5 = 01111\ 11011\ 110$ (10)

$\vec{V}_3 + \vec{V}_4 + \vec{V}_5 = 10110\ 00010\ 110$ (6)
$\vec{V}_2 + \vec{V}_4 + \vec{V}_5 = 11000\ 11011\ 100$ (7)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_3 + \vec{V}_4 = 01000\ 10111\ 011$ (7)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_3 + \vec{V}_5 = 10111\ 00000\ 010$ (5)
$\vec{V}_1 + \vec{V}_3 + \vec{V}_4 + \vec{V}_5 = 00011\ 00111\ 010$ (6)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_4 + \vec{V}_5 = 01101\ 11110\ 000$ (7)
$\vec{V}_2 + \vec{V}_3 + \vec{V}_4 + \vec{V}_5 = 10001\ 01110\ 011$ (7)
$\vec{V}_1 + \vec{V}_2 + \vec{V}_3 + \vec{V}_4 + \vec{V}_5 = 00100\ 01011\ 111$ (7)

tenemos $2^5 = 32$ vectores

b) Se trata de un Código $C(13,5)$

$n = 13$ = longitud de palabras código
$k = 5$ = longitud de palabras fuente

c) Gsistemática

$$G = \begin{matrix} \vec{v}_1 \\ \vec{v}_2 \\ \vec{v}_3 \\ \vec{v}_4 \\ \vec{v}_5 \end{matrix} \begin{pmatrix} 10101 & 00101 & 100 \\ 00111 & 01100 & 101 \\ 01001 & 10101 & 111 \\ 10011 & 01011 & 101 \\ 01100 & 11100 & 100 \end{pmatrix}$$

Intercambio filas 4ª por 1ª
sumo fila 5 a todas las demás
intercambio filas 2ª por 4ª y 3ª por 5ª
intercambio filas 4ª por 5ª

$$G_{sist} = \left(\begin{array}{ccc} 01101 & 11110 & 000 \\ 11001 & 11001 & 000 \\ 01100 & 11100 & 100 \\ 10111 & 00000 & 010 \\ 01011 & 10000 & 001 \end{array}\right) = (P \mid I_5)$$

d) $H = (I_8 \mid P^t)$; $G_{sist} = (P \mid I_5)$

$$H = \left(\begin{array}{cc} 10000000 & 01010 \\ 01000000 & 11101 \\ 00100000 & 10110 \\ 00010000 & 00011 \\ 00001000 & 11011 \\ 00000100 & 11101 \\ 00000010 & 11100 \\ 00000001 & 10100 \end{array}\right)$$

e) ya que tenemos 8 columnas independientes (las col. de la matriz identidad) tendremos 5 dependientes

f) $d_{min} = \min \{ w(\vec{x}) ; \vec{x} \in C ; \vec{x} \neq \vec{0} \} = 3$

$s_{max} = d_{min} - 1 = 2$

$t_{max} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = 1$

g) Distribución de pesos A_i:

$A_0 = 1$	$A_5 = 5$	$A_{10} = 2$
$A_1 = 0$	$A_6 = 10$	$A_{11} = 0$
$A_2 = 0$	$A_7 = 7$	$A_{12} = 0$
$A_3 = 1$	$A_8 = 3$	$A_{13} = 0$
$A_4 = 0$	$A_9 = 3$	

h) Líderes de cogrupo de la tabla estándar:

$\vec{e}_0 = \vec{0}$

tendremos después $\binom{13}{1}$ palabras código con $w = 1$ (13 palabras)

tendremos después $\binom{13}{2}$ palabras código con $w = 2$ (78 palabras)

tendremos además $\binom{13}{3}$ palabras código con $w = 3$ (286 palabras)

Como en la tabla estándar sólo podemos ubicar $2^8 = 256$ filas, tendremos:

1 x $\vec{0}$
13 x palabras de peso 1
78 x palabras de peso 2
164 x palabras de peso 3

256 (filas o palabras)

i) si $p = 10^{-4}$

$$P_{ND} = \sum_{i=d_{min}=3}^{n=13} A_i \cdot p^i \cdot (1-p)^{n-i} =$$

$$= 1 \cdot (10^{-4})^3 \cdot (1-10^{-4})^{10} + 5 \cdot (10^{-4})^5 \cdot (1-10^{-4})^8 +$$

$$+ 10 \cdot (10^{-4})^5 \cdot (1-10^{-4})^7 + 7 \cdot (10^{-4})^7 \cdot (1-10^{-4})^6 +$$

$$+ 3 \cdot (10^{-4})^8 \cdot (1-10^{-4})^5 + 3 \cdot (10^{-4})^9 \cdot (1-10^{4})^4 +$$

$$+ 2 \cdot (10^{-4})^{10} \cdot (1-10^{-4})^3 = 9,99 \cdot 10^{-13}$$

jj) $$P_{NC} = \sum_{i=t+1}^{13} \binom{13}{i} p^i (1-p)^{13-i} = 7,79 \cdot 10^{-7}$$

$t = 1$: cumple $2t+1 \leq d_{min} \leq 2t+2$

kj) Para el caso mixto ($d_{min} = 3 \Rightarrow \begin{cases} s = 1 \\ t = 1 \end{cases}$ pues $d_{min} = t+s+1$)

P_{ND} es igual pues no afecta s

P_{NC} es igual pues $t = 1$ igual que antes

③ La tabla estándar es:

$$\begin{pmatrix} \vec{v}_1 & \vec{v}_2 & \vec{v}_3 & \cdots & \vec{v}_{2^k} \\ \vec{e}_2 & \vec{v}_2+\vec{e}_2 & \vec{v}_3+\vec{e}_2 & \cdots & \vec{v}_{2^k}+\vec{e}_2 \\ \vec{e}_3 & \vec{v}_2+\vec{e}_3 & \vec{v}_3+\vec{e}_3 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vec{e}_{2^{n-k}} & \vec{e}_{2^{n-k}}+\vec{v}_2 & \cdots & \cdots & \vec{v}_{2^k}+\vec{e}_{2^{n-k}} \end{pmatrix}$$

Las filas de la tabla estándar son conjuntos de palabras código a las que se las suma un vector $\vec{e}_i$

$\vec{e}_i$ pertenecen al código lineal

Al alternar las filas, tendremos un código con palabras

$$\vec{e}_i,\ \vec{e}_i+\vec{v}_2,\ \vec{e}_i+\vec{v}_3,\ \ldots,\ \vec{e}_i+\vec{v}_{2^k}$$

este nuevo código será lineal si:

$$\begin{cases} \vec{0} \in C' \\ \forall \vec{u}, \vec{v} \in C' \Rightarrow \vec{u}+\vec{v} \in C' \\ \forall \vec{u} \in C' \Rightarrow \lambda \cdot \vec{u} \in C';\ \lambda \in \{0,1\} \end{cases}$$

$\vec{0} \notin C' \Rightarrow$ C' no es lineal

Sabemos que $d(\vec{u},\vec{v}) = w(\vec{u}+\vec{v})$

si $(\vec{e}_i+\vec{v}_j)+(\vec{e}_i+\vec{v}_k) = \cancel{(\vec{e}_i+\vec{e}_i)}^{\,0} + \vec{v}_j+\vec{v}_k \in C$ con $j \neq k$

$w\left((\vec{e}_i+\vec{v}_j)+(\vec{e}_i+\vec{v}_k)\right) = w(\vec{v}_j+\vec{v}_k)$

$d\left((\vec{e}_i+\vec{v}_i)+(\vec{e}_i+\vec{v}_k)\right) = d(\vec{v}_i,\vec{v}_k) \Rightarrow d_{min}(C) = d_{min}(C')$

(4)

a) FALSO

$G \cdot H^t = 0$ pero no $G \cdot H = 0$

b) CIERTO

$\vec{s} = \vec{r} \cdot H^t = (\vec{e} + \vec{v}) \cdot H^t = \vec{e} \cdot H^t + \cancel{\vec{v} \cdot H^t}^{\,0} \Rightarrow$ cada $\vec{e}_i$ tiene un síndrome asociado $\vec{s}_i$

c) FALSO

necesita ser base

d) CIERTO

$d_{min} = \min \{ w(\vec{x}) ;\ \vec{x} \neq \vec{0} \}$ luego $A_i = 0$ si $i < d_{min}$

pues d_{min} marca la palabra de menor peso.

e) FALSO

Sólo podremos corregir hasta peso t (todos, pero no más)

f) FALSO

a cada síndrome le corresponden 2^k errores.

(5)

distancia Hamming $= 8$, $n = 255$

Límite $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = 3$

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i} \Rightarrow n - k \geq \log_2 \left(\sum_{i=0}^{t} \binom{n}{i} \right) \Rightarrow n - k \geq \log_2 \left(1 + \binom{255}{1} + \binom{255}{2} + \binom{255}{3} \right)$$

$$\geq 21{,}3982$$

$m = n - k \geq 22$ bits

QUINTO GRUPO DE EJERCICIOS - Curso 2013/2014

ENTREGA: 19 de Diciembre

Versión: 1.0.

ENUNCIADOS

1.- Demostrar que todo polinomio binario con un número par de términos es divisible por (1+x).

2.- Demostrar que los factores de un polinomio divisible con un número impar de términos, tienen un número impar de términos.

3.- Dado el polinomio generador $g(x) = 1 + x^4 + x^6 + x^7 + x^8$

a) Si es reducible, descomponerlo en factores irreducibles.
b) Si este polinomio g(x) es el generador de un código cíclico, y considerando las propiedades de los polinomios irreducibles, encontrar el n mínimo.
c) A partir de este g(x) encontrar la matriz G en sus distintas formas sistemática y no sistemática, y de esta la H.
d) Calcular el polinomio complementario h(x) y sus factores.
e) A partir de h(x) encontrar la matriz H, y de esta G.
f) A partir de la matriz H demostrar que la distancia mínima es 5.
g) Demostrar que la palabra todo 1´s (111…1) pertenece al código.
h) Analizar el impacto que tiene este hecho sobre la distribución de pesos.
i) Acotar los valores de A_i.
j) Acotar los valores de la distribución α_i de pesos de los líderes de cogrupo.
k) Si se utiliza en un Canal BSC con $p=10^{-4}$, calcular probabilidades de error residual y de retransmisión cuando proceda, si se corrige.
l) Ídem si se detecta.
m) Ídem en los casos híbridos si procede

4.- En un sistema ARQ de Parada y Espera, el emisor debe enviar una gran cantidad de datos que puede segmentar en tramas de la longitud que necesite. El régimen binario del canal es de 1 Mbit/sg y la probabilidad de error de bit p=10-3 en ambos sentidos del canal. Para la codificación de las tramas de datos, puedo escoger entre los siguientes códigos, utilizados maximizando sus capacidades de detección:

1. Un código cíclico BCH con distancia mínima 7 y dimensiones (63, 43)
2. Un código cíclico generado por $g(x) = (1+x)(1+x+x^6)$.

Se pide:

a) Calcule la probabilidad de error residual de ambos códigos.
b) Calcule la cadencia eficaz en ambos casos despreciando las probabilidades de no detectar errores en las tramas de datos. El tiempo de asentimiento es el tiempo de transmisión de las tramas de control (ACK/NAK), las cuales como se verá posteriormente tienen una longitud de 15 bits.
c) Con los datos anteriores, argumente cuál de los dos elegiría y por qué lo haría.

En este sistema, se pretende proteger frente a errores también las tramas de control (ACK / NAK) que el receptor envía al emisor. Por ello, se dispone de otro código cíclico del que se saben los siguientes datos:

- Si el canal introduce los errores *(1 1 0 1 0 1 0 0 0 1 1 0 1 0 1)* o *(1 1 0 1 0 0 1 0 1 1 0 0 1 0 1),* el decodificador no es capaz de detectarlos, independientemente de su modo de utilización (detección o corrección).
- El decodificador es capaz de detectar todas las ráfagas de error de longitud menor o igual a 5, existiendo ráfagas de longitud 6 y superiores que no detecta.

Se pide:

d) Determine las dimensiones del código y su polinomio generador.
e) Determine las capacidades de detección del código y calcule su distancia mínima.
f) Calcule la probabilidad de error residual

La diferencia con ARQ en Parada y Espera teórico, es que ahora el emisor puede recibir una trama de control (ACK/NAK) errónea. En ese caso, el emisor decide siempre retransmitir la trama de datos anterior. Se pide:

g) Deduzca la formula genérica (utilizando los parámetros p_1 como probabilidad de error de bloque en tramas de datos y p_2 como probabilidad de error de bloque en tramas de control) de la cadencia eficaz para este caso.

LISTA DE POLINOMIOS PRIMITIVOS

x^2+x+1	x^5+x^2+1	$x^8+x^4+x^3+x+1$
x^3+x+1	x^6+x+1	x^9+x^4+1
x^4+x^3+1	x^7+x^3+1	$x^{10}+x^3+1$

FORMULAS DE UTILIDAD

$$\sum_{i=0}^{\infty} i \cdot m^i = \frac{m}{(1-m)^2}; \qquad \sum_{i=1}^{\infty} i \cdot m^{i-1} = \frac{1}{(1-m)^2};$$

① Sea un polinomio con 2 términos: $x^a + x^b$; $a > b$

$$x^a + x^b \quad \big| \; x+1$$

$$x^a + x^{a-1} \qquad x^{a-1} + x^{a-2} + \dots + x^{a-i}$$

$$x^{a-1} + x^{a-2}$$

$$x^{a-i+1} + x^{a-i}$$

$$0 \quad 0 \longleftarrow \text{si } x^{a-i} = x^b \Leftrightarrow a-i = b$$

tendrá resto nulo cuando se alcance $a-i=b$
por extensión, sucederá del mismo modo con un número par cualquiera de términos, pues los coeficientes se irán anulando entre sí dos a dos.

② sea el polinomio a factorizar $p(x)$ con número impar de términos. Entonces:

$$p(x) = a(x) \cdot b(x)$$

si $a(x)$ ó $b(x)$ tuviese alguno (o ambos) un número par de términos, $p(x)$ tendría un número par de térm.
por tanto, el único modo de obtener un número impar de términos en $p(x)$ es que sus factores tengan un número impar de términos también
Además, en binario, obteniendo la suma de dos términos del mismo grado quedarían anulados

impar − par = impar.

(3) $g(x) = 1 + x^4 + x^6 + x^7 + x^8 \Rightarrow \text{grado} = n - k = 8$

a) Descomposición:

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

[Realizado con Wolfram]

De modo que $(x^{15} + 1) = g(x) \cdot (x+1)(x^2 + x + 1)(x^4 + x^3 + 1)$

b) Hallar el n mínimo.

$$x^{15} + 1 \quad \Big| \; x^8 + x^7 + x^6 + x^4 + 1$$

$$x^{15} + x^{14} + x^{13} + x^{12} + x^7$$
$$x^{14} + x^{13} + x^{12} + x^{10} + x^6$$
$$x^{12} + x^{11} + x^{10} + x^8 + x^4$$
$$x^8 + x^7 + x^6 + x^4 + 1$$

$$x^7 + x^6 + x^4 + 1$$

$\Rightarrow n = 15$

$n - k = 8 \Rightarrow k = 7$

$C(15, 7)$

c) $g(x) = 1 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4 + 0 x^5 + 1 \cdot x^6 + 1 \cdot x^7 + 1 \cdot x^8$

$g_0 \; g_1 \; g_2 \; g_3 \; g_4 \; g_5 \; g_6 \; g_7 \; g_8$

$$G = \begin{pmatrix} 1&0&0&0&1&0&1&1&1&0&0&0&0&0&0 \\ 0&1&0&0&0&1&0&1&1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&1&0&1&1&1&0&0&0&0 \\ 0&0&0&1&0&0&0&1&0&1&1&1&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&1&1&1&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&1&1&1&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \end{pmatrix} \begin{matrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ x^3 \cdot g(x) \\ x^4 \cdot g(x) \\ x^5 \cdot g(x) \\ x^6 \cdot g(x) \end{matrix}$$

7 filas
15 columnas

$$G_{sist} = \left(\begin{array}{cccccccc|ccccccc} 1&0&0&0&1&0&1&1&1&0&0&0&0&0&0 \\ 1&1&0&0&1&1&1&0&0&1&0&0&0&0&0 \\ 0&1&1&0&0&1&1&1&0&0&1&0&0&0&0 \\ 1&0&1&1&1&0&0&0&0&0&0&1&0&0&0 \\ 0&1&0&1&1&1&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&1&1&1&0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&1&1&1&0&0&0&0&0&0&1 \end{array}\right)$$

teniendo $G_{sist} = (P \mid I_k)$ obtenemos $H = (I_{n-k} \mid P^t)$

$$H = \left(\begin{array}{cccccccc|cccccccc} 1&0&0&0&0&0&0&0&1&1&0&1&0&0&0&\\ 0&1&0&0&0&0&0&0&0&1&1&0&1&0&0&\\ 0&0&1&0&0&0&0&0&0&0&1&1&0&1&0&\\ 0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&\\ 0&0&0&0&1&0&0&0&1&1&0&1&1&1&0&\\ 0&0&0&0&0&1&0&0&0&1&1&0&1&1&1&\\ 0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&\\ 0&0&0&0&0&0&0&1&1&0&1&0&0&0&1& \end{array}\right)$$

d) $g(x) \cdot h(x) = (x^{15}+1) \Rightarrow h(x) = \dfrac{x^{15}+1}{g(x)} = \{ap.b\} = x^7+x^6+x^4+1$

$h(x) = x^7 + x^6 + x^4 + 1$

$x^7 + x^6 + x^4 + 1 \quad \big| \; 1+x$

$x^7 + x^6 \qquad x^6 + x^3 + x^2 + x + 1$

$x^4 + x^3$

$x^3 + x^2$

$x^2 + x$

$x + 1$

$h(x) = (x+1)(x^6 + x^3 + x^2 + x + 1)$

$x^6 + x^3 + x^2 + x + 1 \quad \big| \; x^2+x+1$

$x^6 + x^5 + x^4 \qquad x^4 + x^3 + 1$

$x^5 + x^4 + x^3$

$x^2 + x + 1$

$h(x) = (x+1)(x^2+x+1)(x^4+x^3+1)$

e) siendo $h(x) = x^7 + x^6 + x^4 + 1$ obtenemos:

$n-k = 8$ filas

15 columnas

$$H = \left(\begin{array}{cccccccccccccc} h_k & h_{k-1} & \cdots & \cdots & h_2 & h_0 & & & & & & & & \\ 1&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&1&0&0&0&0&0 \\ 0&0&1&1&0&1&0&0&0&1&0&0&0&0 \\ 0&0&0&1&1&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&1&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&1&1&0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&1&1&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&1&1&0&1&0&0&0 \end{array}\right) \begin{array}{l} h(x) \\ x \cdot h(x) \\ x^2 \cdot h(x) \\ x^3 \cdot h(x) \\ x^4 \cdot h(x) \\ x^5 \cdot h(x) \\ x^6 \cdot h(x) \\ x^7 \cdot h(x) \end{array}$$

Análogamente a como hicimos con G para obtener H, sabiendo que $H = (I_{n-k} \mid P^t) \Rightarrow G_{sist} = (P \mid I_k)$ tan sólo deberemos obtener la matriz identidad de dimensión n-k a la izquierda de H y a partir de ésta obtener G. Lógicamente, el resultado de G es el mismo.

ℓ)

→ Podemos garantizar $d_{min} \geq 1$, pues no existe ninguna columna de H nula.

→ Podemos garantizar $d_{min} \geq 2$, pues no existe ninguna combinación lineal (suma) de dos columnas de H que resulte nula.

→ Podemos garantizar también que $d_{min} \geq 3$, pues no existen 3 columnas de H que sumadas resulten cero.

Podríamos seguir garantizando la cota inferior de d_{min} de este modo, pero resulta complejo obtener todas las posibles combinaciones de 4 elementos columna de H.

j) $\vec{u} \in G \iff \vec{u} \cdot H^t = 0$

se demuestra que $(111 \ldots 111) \cdot H^t = (000 \ldots 000)$

o lo que es lo mismo: todas las filas de H (columnas de H^t) tienen un número par de '1' por lo que al multiplicar por $(1 \ldots 1)$ y sumar un número par de '1' obtendremos 0.

h) i) Al existir la palabra (111 ... 11) y pertenecer al código, cualquier palabra sumada con ésta resultará en su "palabra simétrica" (cambia '0' por '1' y '1' por '0')

Si $\vec{0} \in \mathcal{C} \Rightarrow A_0 = 1$

si $\vec{1} \in \mathcal{C} \Rightarrow A_{15} = 1$

si $d_{min} = 5 \Rightarrow \nexists$ ninguna palabra de peso 1, ?, 3 ni 4

por lo anteriormente dicho: $\nexists$ palabras de peso 14, 13, 12, 11

si $\nexists$ palabra con peso 5, 6 ..., 9, 10 podrían existir 15 palabras del mismo peso, pues las rotaciones de esa palabra también pertenecerán al código, luego:

teniendo $2^7 = 128$ palabras código:

$A_0 = 1$, $A_1 = A_2 = A_3 = A_4 = 0$

$$\left.\begin{matrix} A_5 \\ A_6 \\ A_7 \\ A_8 \\ A_9 \\ A_{10} \end{matrix}\right\} \in (15, 126) \cup \{0\}$$

$A_{11} = A_{12} = A_{13} = A_{14} = 0$, $A_{15} = 1$

j) $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{5-1}{2} \right\rfloor = 2 \Rightarrow$ cabrán en la tabla estándar todas las palabras con peso ≤ 2

$\alpha_0 = 1$

$\alpha_1 = 15$

$\alpha_2 = \binom{15}{2} = 105$

$\alpha_3 = 135$

tabla estándar tiene $2^{n-k} = 2^8 = 256$ filas

luego: $\alpha_3 = 256 - \alpha_0 - \alpha_1 - \alpha_2 = 135$

k) BSC, $p = 10^{-4}$ en corrección pura

$P_{retransmisión} = 0$ (pues no se detecta nunca, siempre se corrige)

$$P_{ER} \leq \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} = \sum_{i=3}^{15} \binom{15}{i} p^i (1-p)^{15-i} = 4,5459 \cdot 10^{-10}$$

l) BSC, $p = 10^{-4}$ en detección pura

$$P_{retransmisión} = P\{w(\vec{e}) \in (1,4)\} \leq \sum_{i=1}^{4} \binom{15}{i} p^i (1-p)^{15-i} = 0,001498$$

$$P_{ER} \leq \sum_{i=d_{min}=5}^{15} \binom{15}{i} p^i (1-p)^{n-i} = 3 \cdot 10^{-17}$$

m) BSC, $p = 10^{-4}$ en híbrido

$$d_{min} = 5 \Rightarrow \left\{ \begin{array}{l} s_{max} = d_{min} - 1 = 4 \\ t_{max} = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 2 \\ s+t+1 = d_{min} \end{array} \right\} \Rightarrow \begin{array}{l} s = 3 \\ t = 1 \end{array}$$

$$P_{retransmisión} = P\{w(\vec{e}) \in (2,3)\} \leq \sum_{i=2}^{3} \binom{n}{i} p^i (1-p)^{n-i} = 1,049 \cdot 10^{-6}$$

$$P_{ER} \leq \sum_{i=4}^{15} \binom{n}{i} p^i (1-p)^{n-i} = 1,36 \cdot 10^{-13}$$

↑ El error será a partir de peso $\max\{s,t\} + 1$

(4) ARQ parada y espera, $p = 10^{-3}$, $R = 1$ Mbps

a)

1) $d_{min} = 7 \Rightarrow S_{max} = 6$, $C(63,43)$

$$P_{ER} \leq \sum_{i=7}^{63} \binom{63}{i} p^i (1-p)^{n-i} = 5,2681 \cdot 10^{-13}$$

2) $g(x) = (1+x)(1+x+x^6) = x^7 + x^6 + x^2 + 1 \Rightarrow n-k = 7$

$1+x+x^6$ es primitivo de grado 6 luego:

$2^m - 1 = 63 \Leftrightarrow m = 6 = n-k \Rightarrow k = 57$ con $d_{min} = 3$

pero como $g(x) = (1+x)\cdot(1+x+x^6)$ tenemos:

$n-k = 7 \Rightarrow k = 56 \Rightarrow C(63,56) \rightarrow d_{min} = 4$

Luego:

$$P_{ER} \leq \sum_{i=4}^{63} \binom{63}{i} p^i (1-p)^{63-i} = 5,68218 \cdot 10^{-7}$$

b)

$$C_{ef} = \frac{k}{T_{oc}} = (1 - P_{RTX}) \frac{k}{k + m + T_{ACK} \cdot R} R$$

si aproximamos a $P_{ER} \simeq 0$ tendremos:

$$P_{RTX} = 1 - P(\vec{e} = \vec{0}) = 1 - (1-p)^n = 0,061086$$

1) $k = 43$, $m = 20$

$$T_{ACK} = \frac{15 \text{ bits}}{10^6 \text{ bps}} = 15 \mu s$$ (despreciamos tiempo de propagación) $RTT \simeq 0$

$$C_{ef} = (1 - 0'061086) \cdot \frac{43}{43 + 20 + 15} 10^6 = 517.606 \text{ bps}$$

2) $k = 56$, $m = 7$, $T_{ACK} = 15 \mu s$

$$C_{ef} = (1 - 0,061086) \frac{56}{56 + 7 + 15} 10^6 = 674.092 \text{ bps}$$

c) La diferencia en C_{ef} es un 30%, considerable pero el código $C(63,43)$ tiene $d_{min}=7$, mientras que el $C(63,56)$ tiene $d_{min}=4$

Si lo que quiero es fiabilidad, o tengo un canal muy malo, optaré por el código $C(63,43)$.

Si lo que me interesa es tener una transferencia maximizada, perdiendo las prestaciones de $d_{min}=7$ optaré por $C(63,56)$, ganando un 30% del C_{ef}

d) Detecta ráfagas de $l = 5 = n-k$

$\vec{e}_1 = (1\,1\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0\,1)$
$\vec{e}_2 = (1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1)$
} Errores indetectables

$l\{\vec{e}_1\} = 15 \Rightarrow n = 15 \; ; \; k = 10 \Rightarrow C(15,10)$

Errores indetectables $\Leftrightarrow \vec{e}_i \in C \Leftrightarrow \vec{e}_1 + \vec{e}_2 \in C$ Luego:

$\vec{e}_1 + \vec{e}_2 = (00000\,1\,1\,0\,1\,0\,1\,0\,0\,0\,0) \in C$

rotando: $(1\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0)$

siendo $g(x) = 1 + x + x^3 + x^5$; grado de $g(x) = 5$

e) $gr(g(x)) = 5$; $g(x) = (1+x)\underbrace{(1+x^3+x^4)}_{\text{primitivo}}$

$g(x) = (x+1) \Rightarrow$ detecta errores impares

por ser múltiplo de un primitivo detecta errores dobles

Luego: detecta hasta peso 3 $\Rightarrow d_{min} = 4$

h)

$$P_{ER} \leq \sum_{i=4}^{15} \binom{15}{i} p^i (1-p)^i = 1{,}353 \cdot 10^{-9}$$

g) Sabemos que: $C_{ef} = (1 - P) \frac{k}{k+m+T_{ACK} \cdot R} R$

siendo $P = P\{ \text{error}_{ACK} \text{ y/o } \text{error}_{datos} \}$

$$\left.\begin{array}{l} P\{\text{error}_{ACK}\} = p_1 \\ P\{\text{error}_{datos}\} = p_2 \end{array}\right\} P\{\text{error}_{ACK} \cup \text{error}_{datos}\} = p_1 + p_2 - p_1 \cdot p_2$$

Luego: $C_{ef} = (1 - (p_1 + p_2 - p_1 p_2)) \frac{k}{k+m+T_{ACK} \cdot R} R$