Solució de tots els Exercicis fets a classe (temari primer parcial)

Informació i Seguretat (Universitat Autònoma de Barcelona)

PROBLEMES

LLISTA TEMA 2 (FETS A CLASSE)

② Tenim 4 itineraris i una assignatura de lliure elecció que poden cursar els 4 itineraris
X

$A = I_1 \rightarrow 10\%$ alumnes $\rightarrow P(X|I_1) = 25\%$

$B = I_2 \rightarrow 25\%$ alumnes $\rightarrow P(X|I_2) = 6\%$

$C = I_3 \rightarrow 25\%$ alumnes $\rightarrow P(X|I_3) = 10\%$

$D = I_4 \rightarrow 40\%$ alumnes $\rightarrow P(X|I_4) = 15\%$

Si escollim una persona que faci l'assignatura, prob. de que cursi A.

$P(I_1|X)$?

BAYES

$$P(I_1|X) = \frac{P(I_1 \cap X)}{P(X)} = \frac{P(X|I_1)\cdot P(I_i)}{\sum P(X|I_i)\cdot P(I_i)} =$$

$$= \frac{0{,}25 \cdot 0{,}1}{0{,}25\cdot 0{,}1 + 0{,}06\cdot 0{,}25 + 0{,}1\cdot 0{,}25 + 0{,}15\cdot 0{,}4} = \boxed{0{,}2} \quad (20\%)$$

③ Una caixa conté 3 monedes:
(C = cara)

ⓜ₁ $P(C|m_1) = 1/2$

ⓜ₂ $P(C|m_2) = 1$

ⓜ₃ $P(C|m_3) = 1/3$

a) Prob. que surti cara al agafar 1 moneda.
$P(C)$?

TEOREMA DE LES PROBAB. TOTALS

$$P(C) = P(C|m_1)\cdot P(m_1) + P(C|m_2)\cdot P(m_2) + P(C|m_3)\cdot P(m$$

$$= \frac{1}{2}\cdot\frac{1}{3} + 1\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{3} = \boxed{\frac{11}{18}}$$

b) Quina és l'esperança de guany si guanyem un € si surt cara i perdem 2€ si surt creu?

$$X: \{\underset{1}{C}, \underset{-2}{X}\} \qquad \begin{matrix} C \rightarrow 1 \\ X \rightarrow -2 \end{matrix}$$

$$Ex = X_{(C)} \cdot P_{(C)} + X_{(X)} \cdot P_{(X)} = 1 \cdot P(C) + (-2)\cdot P(X) =$$

$$= 1 \cdot \underbrace{\frac{11}{18}}_{\text{Prob cara}} + (-2)\cdot \underbrace{\frac{7}{18}}_{\text{Probab. creu}} = \boxed{-\frac{1}{6}}$$

Com és negativa, hi ha esperança que perdrem.

⑤ Resultats de llançar un dau de 5 cares: $S=\{1,2,3,4,5\}$

a) Digues el valor de l'entropia pels següents casos:

i) L'entropia de S és la mínima possible.

Tindrem entropia mínima si la probab. d'una de les cares és 1 (100%). → La resta de prob. seran 0.

$$\left(H(S)=0 \longrightarrow P(j)=1 \Rightarrow P(i)=0 \quad \forall i \neq j\right)$$

ii) L'entropia de S és la màxima possible.

Serà màxima quan les probabilitats siguin equiprobables.

$$p(j)=\frac{1}{5} \ \ \forall j \longrightarrow I(j) = -\log\frac{1}{5} = \log 5 \text{ bits}$$

$$\boxed{H(S) = \log 5 \text{ bits/resultat}}$$

iii) $p(1)=p(2)=\frac{1}{5}$ || $p(3)=\frac{2}{5}$ || $p(4)=p(5)=\frac{1}{10}$

⬇ ⬇ ⬇

$I(1)=I(2)=-\log\frac{1}{5}= \boxed{\log 5 \text{ bits}}$

$I(3)=-\log\frac{5}{2}= \boxed{\log 5 - 1 \text{ bits}}$

$I(4)=I(5)=-\log\frac{1}{10}= \boxed{\log 5 + 1 \text{ bits}}$

$$H(S)= 2\cdot\frac{1}{5}\cdot\log 5 + \frac{2}{5}\cdot(\log 5-1) + 2\cdot\frac{1}{10}\cdot(\log 5+1) =$$

$$= \boxed{\log 5 - \frac{1}{5} \text{ bits/resultat}}$$

⑥ Ciutat A → sempre VERITAT
Ciutat B → sempre MENTIDA } → Un viatger arriba al poble i pregunta a algú (aquest no té perquè ser del poble o n'està).

a) Mín. preguntes per saber en quina ciutat està.

resposta $\in \{Sí, No\}$ → 4 situacions equiprobables.

Incertesa = 1 bit → cada resposta ens dóna 1 bit d'informació en el millor dels casos.

Per tant, amb una pregunta és suficient:

P.exemple: ETS D'AQUÍ? {
a A de A Sí
a A de B Sí → A
a B de A No
a B de B No → B

b) De quina ciutat és l'habitant?

Tindríem una incertesa de 2 bits i per tant, amb 1 pregunta impossib

⑦ a) Tenim 27 monedes, una de les quals pesa més. Quantes pesades són necessàries per trobar-la?

Com podem distribuir-les de forma equiprobable → mesura de Hartley.

Incertesa $= \log 27 = \log 3^3 = 3 \log 3$ bits

Cada pesada ens dóna en el millor dels casos $\log 3$ bits → $\boxed{3 \text{ pesades}}$

b) Si tenim 12 monedes i una pesa més/menys. → 24 casos

Incertesa inicial $= \log 24$ bits

Cada pesada ens dona en el millor dels casos $\log 3$ bits d'info.

$$K \text{ pesades} \rightarrow K \cdot \log 3 \geq \log 24$$

Per tant, $\boxed{K \geq 3}$

⑧ Quantes preguntes hem de fer per endevinar un número entre 1 i 10?

Incertesa = $\log 10 = \log 5\cdot 2 = \log 5 + 1$ bits $= 3{,}32$ bits

Resposta $\in \{Sí, No\} \rightarrow$ Cada pregunta ens proporciona 1bit en el millor cas.
(màxim en una entropia binària)

Per tant, mínim 4 preguntes

⑪ 1,2,3,4 → llancem una moneda un cop
5,6 → " " " dos cops

DAU $X \rightarrow \{1,2,3,4,5,6\} \rightarrow \{A_1(1,2,3,4), A_2(5,6)\}$

CARES $Y \rightarrow \{0,1,2\} \rightarrow \{B_1, B_2, B_3\}$

$P(B_j \mid A_i)$	B_1	B_2	B_3
A_1	1/2	1/2	0
A_2	1/4	1/2	1/4

$P(A_i \mid B_j)$	B_1	B_2	B_3
A_1	1/3	1/3	0
A_2	1/12	1/6	1/12

$P(B_1|A_1)\cdot P(A_1)$

$$P(A_1) = \frac{4}{6} = \frac{2}{3}$$

$$P(A_2) = \frac{2}{6} = \frac{1}{3}$$

a) Probabilitat d'obtenir menys de dues cares.

$$P(B_1)+P(B_2) = 1 - \underbrace{P(B_3)} = 1 - \frac{1}{12} = \boxed{\frac{11}{12}}$$

$$P(B_3) = P(A_1|B_3) + P(A_2|B_3) = \frac{1}{12}$$

b) Informació obtinguda sobre el valor que ha sortit al dau segons el nombre de cares obtingudes amb les monedes?

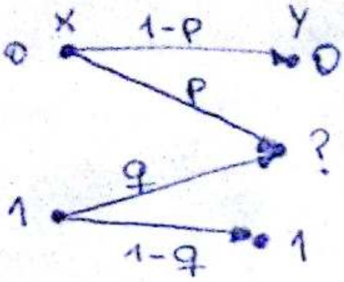
$I(X,Y) = H(Y) - H(Y|X) = 1{,}33 - \frac{7}{6} = \boxed{0{,}16 \text{ bits/resultat}}$

$H(Y) = H\left(\frac{5}{12}, \frac{1}{2}, \frac{1}{12}\right) \simeq 1{,}33$ bits/resultat

$H(Y|X) =$ LOCURA $= \frac{2}{3}\cdot H\left(\frac{1}{2}, \frac{1}{2}, 0\right) + \frac{1}{3}\cdot H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) =$

$= \frac{2}{3}\cdot 1 + \frac{1}{3}\cdot\frac{3}{2} = \frac{7}{6}$ bits/resultat

⑫ Canal BEC



WTF.

a) Matriu d'aquest canal.

$$\begin{array}{c|ccc} & 0 & ? & 1 \\ 0 & 1-p & p & 0 \\ 1 & 0 & q & 1-q \end{array}$$

b) Calcular $H(Y|X=0)$ i $H(Y|X=1)$.

$H(Y|X=0) = -P(X=0|X=0) \cdot \log P(Y=0|X=0) - P(Y=?|X=0) \cdot \log P(Y=?|X=0) = -P(Y=1|X=0) \cdot \log P(Y=1|X=0) = \boxed{H(p, 1-p)}$

$H(Y|X=1) = \boxed{H(q, 1-q)}$

c) $H(Y|X)$ si $P(X=0)=\alpha$ i $P(X=1) = 1-\alpha$

$H(Y|X) = P(X=0) \cdot H(Y|X=0) + P(X=1) \cdot H(Y|X=1) =$

$= \boxed{\alpha \cdot H(p, 1-p) + (1-\alpha) \cdot H(q, 1-q)}$

d) $P(X=0) = 2/3$ $P(X=1) = \frac{1}{3}$ $p = -\frac{1}{4}$ $q = 1/2$

$H(X) = H(1/3, 2/3) \simeq \boxed{0{,}92 \text{ bits/entrada}}$

$H(X|Y=0) = \boxed{0}$ Perque per $Y=0$ només tenim entrada (X) 0.

$H(X|Y=1) = \boxed{0}$ " el mateix però amb 1.

$H(X|Y=?) = -P(X=0|Y=?) \cdot \log P(X=0|Y=?) - P(X=1|Y=?) \cdot \log P(X=1|Y=?) =$

amb Bayes... $= (\ldots)$

e) Amb els valors anteriors, calcula $H(X|Y)$.

$H(X|Y) = \underbrace{P(Y=0) \cdot H(X|Y=0)}_{0} + \underbrace{P(Y=1) \cdot H(X|Y=1)}_{0} + P(Y=?) \cdot H(X|Y=?) = \boxed{\frac{1}{3}}$

f) Capacitat?

Dòna $C = 1 -$

LLISTA TEMA 3

②

Missatge	Codi 1	Codi 2	Codi 3
U_1	000	00	0
U_2	001	01	1
U_3	010	100	10
U_4	011	101	11
U_5	100	1100	100
U_6	101	1101	101
U_7	110	1110	1000
U_8	111	1111	1001

a) Són codis de descodificació única?

Codi 1 → Els codis de L fixa sempre ho són.

Codi 2 → És instantani, cap paraula és prefix d'una altre . per tant é de desc. única.

Codi 3 → No és instantani i tampoc de desc. única.

b) Suposant que els missatges són equiprobables quin dels codis de descod. única és millor?

$L_1 = 3$ $\quad \bar{L}_2 = \frac{1}{8} \cdot (2+2+3+3+4+4+4+4) = 3{,}25$

$\boxed{\text{El codi 1 és millor}}$

c) Assigna probab. per tal que el segon codi sigui millor que el primer.

Per millorar el segon codi assignariem probabilitats més altes a les paraules curtes.

③ Sigui S una font amb H(S)=2,7540

a) És possible construir un codi binari de $\overline{L}=2,6120$?

$D=2$. $\overline{L}=2,6120$

Apliquem el 1r Teorema de Shannon:

$$\overline{L} \geq \frac{H(S)}{\log D} = \frac{\overset{2,7540}{H(S)}}{\underset{>1}{\log 2}} = 2,7540 \rightarrow \text{Longitud mitjana mínima}$$

$\boxed{\text{Per tant no existeix un codi amb } \overline{L} = \underline{2,6120}}$

b) És possible construir un codi de $\overline{L}=3$? I de $\overline{L}=3,8$?

- És possible però no segur
- És factible però no ho sabem

c) En cas que es puguin construir, serien òptims?

$\overline{L}=3$ ➡ $\boxed{\text{No ho sabem}}$

$\overline{L}=3,8$ ➡

$$\underset{\text{OBLIGATORI}}{\frac{H(S)}{\log D}} \leq \overline{L} \leq \underset{\text{HO PODEM ACONSEGUIR}}{\frac{H(S)}{\log D}+1}$$

COM A MÀXIM
$2,7521+1=3,754$
per tant, no seria òptim

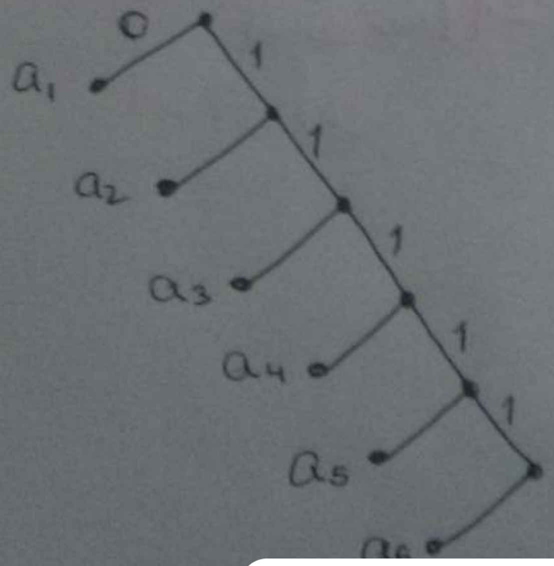
⑥ VERSIÓ REDUÏDA → font amb 6 missatges → $S=\{a_1, \dots, a_6\}$

a) És possible construir un codi binari instantani amb:

$L_1=1$ $L_2=2$ $L_3=3$ $L_4=4$ $L_5=5$ $L_6=6$

Apliquem Kraft → $\sum D^{-l_i} \leq 1$

$$2^{-1}+2^{-2}+2^{-3}+2^{-4}+2^{-5}+2^{-6} \leq 1$$ ➡ EXISTEIX UN CODI INSTANTANI



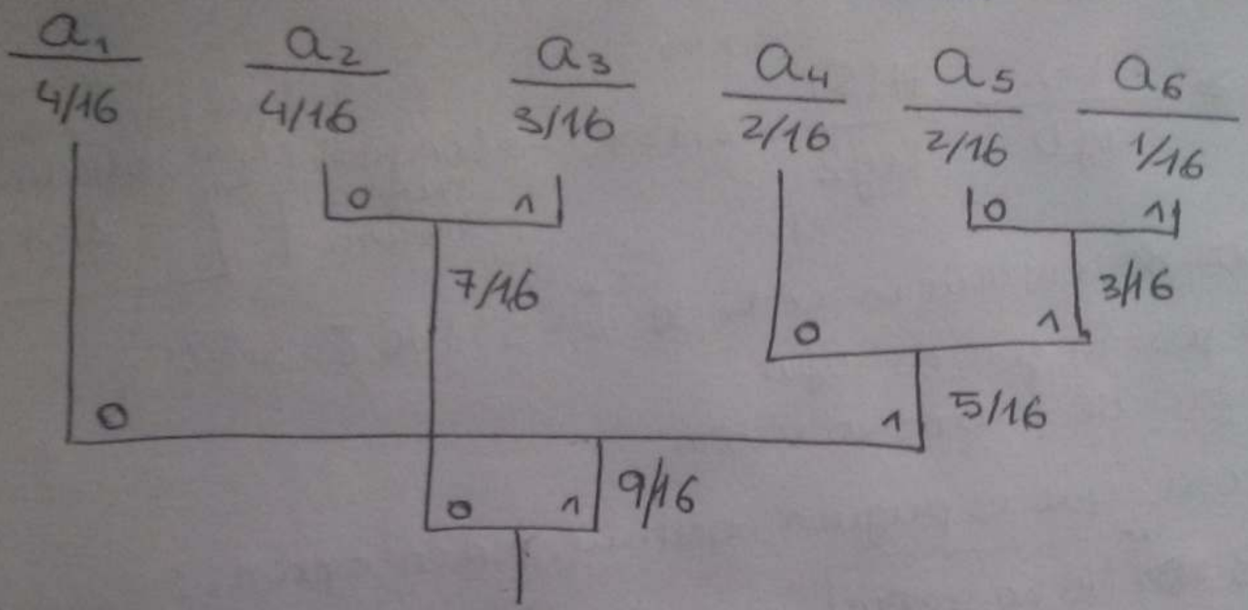
De l'arrel cap a les fulles:

$a_1=0$
$a_2=10$
$a_3=110$
$a_4=1110$
$a_5=11110$
$a_6=111110$

b) Si la distribució de probab. és:

$P_1 = P_2 = \frac{4}{16}$ $P_3 = \frac{3}{16}$ $P_4 = P_5 = \frac{2}{16}$ $P_6 = \frac{1}{16}$

Construir codi òptim per a S. → HUFFMAN



De l'arrel cap a les fulles:

$a_1 = 10$ $a_4 = 110$
$a_2 = 00$ $a_5 = 1110$
$a_3 = 01$ $a_6 = 1111$

c) Calcular l'eficiència i la redundància dels codis suposant la distribució de b).

$$\underset{\text{eficiència}}{\eta} = \frac{H(S)}{\bar{L}\cdot \log D} = \frac{H(S)}{\bar{L}}$$

$\bar{L}_A = 2{,}81 \longrightarrow \boxed{\eta_A = 0{,}87}$

$\bar{L}_B = 2{,}5 \longrightarrow \boxed{\eta_B = 0{,}98}$ $\simeq 1$ (màx. òptim)

⑦

S	P	C_1	C_2
a_1	0,2	01	10
a_2	0,4	1	00
a_3	0,2	000	11
a_4	0,1	0010	010
a_5	0,1	0011	011

a) Calcular $H(S)$, $\overline{L_1}$ i $\overline{L_2}$.

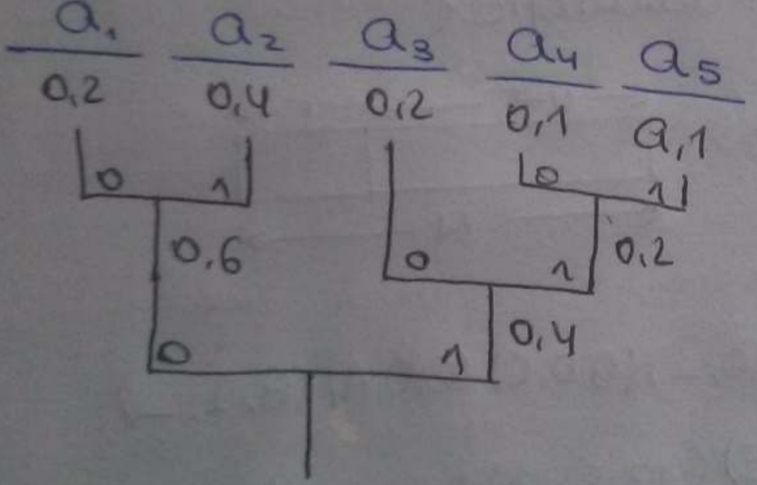
$$H(S) = -\left[0{,}2\cdot\log 0{,}2 + 0{,}4\cdot\log 0{,}4 + 0{,}2\cdot\log 0{,}2 + 0{,}1\cdot\log 0{,}1 + 0{,}1\cdot\log 0{,}1\right]$$
$$= \boxed{2{,}12 \text{ bits/missatge}}$$

$\overline{L_1} = \boxed{2{,}2}$

$\overline{L_2} = \boxed{2{,}2}$

} Els dos codis són candidats a òptims, per saber-ho fem un òptim i comparem $\overline{L}$.

b)



HUFFMAN

a_1 = 00
a_2 = 01
a_3 = 10
a_4 = 110
a_5 = 111

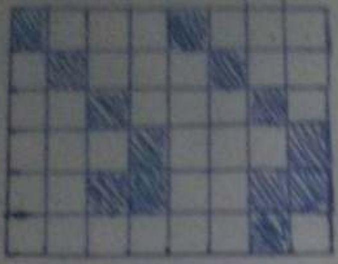
$\boxed{\overline{L} = 2{,}2}$

↳ Per tant, C_1 i C_2 són òptims.

LLISTA TEMA 4

② Codifiqueu utilitzant RLE i calculeu la taxa de compressió.

a)



8
0 1 3 1 3
1 1 3 1 2
2 1 3 1 1
3 1 3 1
2 2 2 2
6 1 1

BITMAP

$6 \cdot 8 + \underset{\substack{\downarrow \\ \text{longitud fila}}}{4} = \text{52 bits}$

RLE

$26 \cdot 4 + 4 = \text{108 bits}$

$R = \frac{108}{52} = \boxed{2,07 \text{ bpb}}$

b) Imatge

Img → $16 \cdot 31 + 5 = 501$ bits

RLE → $64 \cdot 5 + 5 = 325$ bits

$R = \frac{325}{501} = \boxed{0,65 \text{ bpb}}$

⑨ |T|H|E|_|C|A|T_|AT_ T|HE_ CAR|_ ATE|_ THE_ R|AT.

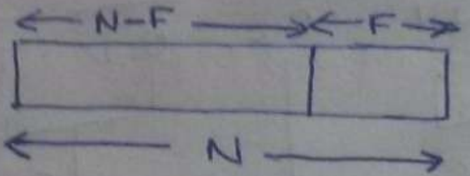
a) Codificar amb LZ77. Paràmetres?

(i , j , c)

i ↑ despl. esquerre

j ↑ long. cadena repetida

c ↑ següent caràcter



(0,0,T) (0,0,H) (0,0,E) (0,0,_) (0,0,C) (0,0,A) (6,1,_) ← només T

(3,3,T) (11,5,R) (11,3,E) (12,5,R) (9,2,.)

N-F = 12 (longitud màxima)

F = 6 (cadena més llarga +1)

N = 18

⑩ b) Descomprimir l'LZ78 següent:

$\underset{\hookrightarrow \text{num frase}}{(0,A)}$ (0,B) (2,C) (3,A) (2,A) (4,A) (6,B)

Entrada:	A	B	BC	BCA	BA	BCAA	BCAAB
Num. frase:	1	2	3	4	5	6	7

$\boxed{\text{Sortida: ABBCBCABABCAABCAAB}}$

c) Calcular R si cada caràcter ocupa 8 bits i cada index enter es representa en 4 bits

Original → 18 caràcters · 8 bits = 144 bits

LZ78 → Cada parella: 8+4 = 12 bits

12 bits · 7 parelles = 84 bits

$$R = \frac{84}{144} = \boxed{0{,}58 \text{ bpb}} \qquad (1-0{,}58)\cdot 100 = \boxed{42\% \text{ COMPRESSIÓ}}$$

LZ77 → Cada triple: 4+4+8 = 16 bits

7 triples: 7 · 16 = 112 bits $\Big\}$ → $\boxed{R = 0{,}78 \text{ bpb}}$ $\boxed{22\% \text{ COMPRESSIÓ}}$

LLISTA TEMA 5

①

$$\Pi = \begin{pmatrix} 0 & 0 & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{1}{3} & 0 & 0 \\ \frac{1}{3} & \frac{2}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

a) Tipus canal i capacitat.

És simètric perque files i columnes són iguals però en diferent ordre.

$$C = \log M - \underset{\hookrightarrow H(B|A)}{H} = \log 4 - 0{,}92 = \boxed{1{,}08 \text{ bits}/\text{entrada}}$$

$(H(B|A) = 0{,}92)$

b) Informació mútua si la dist. probabilitats és $(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$

c) Dist. prob. perque assoleixi la capacitat.

Inicial: la equiprobable.

Final: podriem