05/12/03

Problema 1

Probl. 1

a) La codificación Huffman aprovecha que no todos los símbolos de una secuencia transmitida ocurran con la misma frecuencia: unos símbolos ocurren más a menudo que otros. Nota: Tenga o no memoria la fuente, no se considera con Huffman.

En vez de usar un nº fijo de bits por símbolo, se usan menos bits para codificar los símbolos (o caracteres) más frecuentes y más bits en los caracteres menos frecuentes.

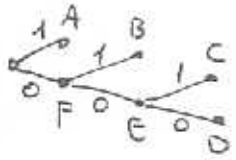
Así, la longitud media de las palabras código es menor, tendiendo a su cota inferior, que es la entropía de la fuente. $E = \frac{H}{\bar{L}}$

Nota: las probabilidades no deben ser muy dispersas, lo cual hace bajar la eficiencia.

b.1)

símbolo fuente	probabilidad
A	4/8 = 0'5
B	2/8 = 0'25
C	1/8 = 0'125
D	1/8 = 0'125

A 0'5
B 0'25
C 0'125 } E 0'25
D 0'125 } F 0'5



A	1
B	0 1
C	0 0 1
D	0 0 0

b.2) $L = \underset{\text{AAAA BBC D}}{4\cdot 1 + 2\cdot 2 + 1\cdot 3 + 1\cdot 3} = 14 \text{ bits}$

b.3) $\bar{L} = 1\cdot 0'5 + 2\cdot 0'25 + 3\cdot 0'125 + 3\cdot 0'125 = 1'75 \ \frac{\text{bits}}{\text{símbolo}}$

$\bar{L} = \sum_{i=1}^{F=4} L_i \cdot P(S_i)$, L_i = longitud del símbolo S_i.

b.4] $E = \frac{H}{\bar{L}}$ // $H = \sum_{i=1}^{F=4} P(S_i) \cdot \log_2 \frac{1}{P(S_i)} =$

$= \frac{1}{2} \cdot \log_2 2 + \frac{1}{4} \cdot \log_2 2^2 + 2 \cdot \frac{1}{8} \cdot \log_2 2^3 = \frac{1}{2} + \frac{1}{2} + \frac{6}{8} = 1'75 \frac{\text{bits}}{\text{símbolo}}$

$E = \frac{1'75}{1'75} = 1$

b.5] Código ASCII $\begin{cases} \rightarrow L = 8 \text{ caracteres} \times 7 \frac{\text{bits}}{\text{caracter}} = 56 \text{ bits para emitir la secuencia.} \\ \rightarrow \bar{L} = 7 \frac{\text{bits}}{\text{caracter}} \rightarrow E = \frac{H}{\bar{L}} = \frac{1'75}{7} = 0'25 \end{cases}$

Código Huffman binario diseñado $\begin{cases} \rightarrow L = 14 \text{ bits necesarios para transmitir la secuencia} \\ \rightarrow \bar{L} = 1'75 \frac{\text{bits}}{\text{caracter}} \rightarrow E = \frac{H}{\bar{L}} = 1 \end{cases}$

Con Huffman se utilizan 4 veces menos recursos que con ASCII.

c.1] Desigualdad de Kraft: $\sum_{i=1}^{S} D^{-L_i} \leq 1$ para que exista algún código instantáneo para esas longitudes L_i.
D = número de símbolos del alfabeto del código.
S = " de símbolos fuente

$S = 10$, $D = 4$
$L_1 = L_2 = L_3 = 1$
$L_4 = L_5 = L_6 = L_7 = 2$
$L_8 = L_9 = L_{10} = 3$

$3 \cdot 4^{-1} + 4 \cdot 4^{-2} + 3 \cdot 4^{-3} =$
$= \frac{3}{4} + \frac{1}{4} + \frac{3}{64} = 1'047 > 1 !!$

No existe ningún código instantáneo en este caso.

c.2] $S = 5$, $D = 3$
$L_1 = L_2 = 1$
$L_3 = L_4 = 2$
$L_5 = 3$

$2 \cdot 3^{-1} + 2 \cdot 3^{-2} + 1 \cdot 3^{-3} =$
$= \frac{2}{3} + \frac{2}{9} + \frac{1}{27} = 0'9259 \leq 1$

Sí que existe algún código instantáneo para este caso.

d) $E = \frac{H}{\bar{L}}$

$H = \sum_{i=1}^{F=10} P(S_i) \cdot \log_q \frac{1}{P(S_i)}$, q = nº de símbolos del alfabeto código. En este caso $q=4$.

$$H = 4 \cdot 0'05 \cdot \log_4 \frac{1}{0'05} + 4 \cdot 0'1 \cdot \log_4 \frac{1}{0'1} + 2 \cdot 0'2 \cdot \log_4 \frac{1}{0'2} =$$

$$= 0'43219 + 0'66438 + 0'46438 =$$

$$= 1'56095 \ \frac{\text{dígitos cuaternarios}}{\text{símbolo}}$$

$\bar{L}$ = long. media del código

$$\bar{L} = 1 \cdot 0'05 + 3 \cdot 2 \cdot 0'05 + 4 \cdot 3 \cdot 0'1 + 2 \cdot 3 \cdot 0'2 =$$

$$= 2'75 \ \frac{\text{dígitos cuaternarios}}{\text{símbolo}}$$

$E = \frac{1'56095}{2'75} = 0'567620 < 1$ → Sí que se puede hallar algún otro código más eficiente que el dado.

e) Observando las $p(S_i)$ y las L_i, vemos que sí se puede proponer un código más eficiente tipo Huffman, que otorga palabras código más largas a los símbolos fuente menos probables. No como en el código dado.

A	0'05
B	0'05
C	0'05
D	0'05
E	0'1
F	0'1
G	0'1
H	0'1
I	0'2
J	0'2

Reordeno →

I	0'2
J	0'2
E	0'1
F	0'1
G	0'1
H	0'1
A	0'05
B	0'05
C	0'05
D	0'05

(A, B, C, D) → K 0'2

Reordeno →

I	0'2
J	0'2
K	0'2
E	0'1
F	0'1
G	0'1
H	0'1

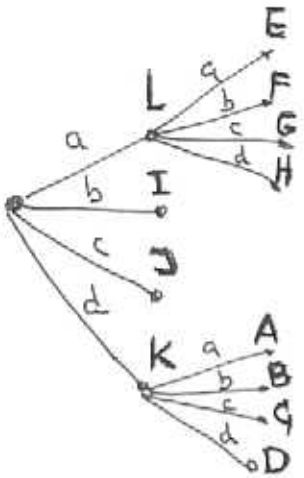
(E, F, G, H) → L 0'4

Reordeno ↓

L	0'4
I	0'2
J	0'2
K	0'2

//

Prob. 1



A	da
B	db
C	dc
D	dd
E	aa
F	ab
G	ac
H	ad
I	b
J	c

$H_{F_2} = 1'56095$ $\frac{\text{dígitos cuaternarios}}{\text{símbolo}}$, es intrínseca a la fuente y no depende del código utilizado.

$$\bar{L} = \underbrace{2}_{\text{long.}} \cdot (\underbrace{4 \cdot 0'05}_{p(s_i)} + 4 \cdot 0'1) + 2 \cdot 1 \cdot 0'2 = 1'6 \ \frac{\text{dígitos cuaternarios}}{\text{símbolo}}$$

$$E = \frac{H}{\bar{L}} = \frac{1'56095}{1'6} = 0'97559 \rightarrow \text{Ha mejorado mucho.}$$

b)

$$H(F_3, F_2) = H(F_2) + H(F_3 \setminus F_2)$$

$$H(F_2) = 1'56095 \ \frac{\text{dig. cuat.}}{\text{símbolo}}$$

$F_2 = \{A, B, C, D, E\} \Rightarrow F_3 = A$

$F_2 = \{F, G, H, I, J\} \Rightarrow F_3 \rightarrow A, \ p(A) = 0'2$
$\qquad\qquad\qquad\qquad\qquad\quad \rightarrow B, \ p(B) = 0'8$

$$H(F_3 \setminus F_2) = H(F_3 \setminus F_2 = A) \cdot P(F_2 = A) + H(F_3 \setminus F_2 = B) \cdot P(F_2 = B) +$$
$$+ H(F_3 \setminus F_2 = C) \cdot P(F_2 = C) + H(F_3 \setminus F_2 = D) \cdot P(F_2 = D) +$$
$$+ H(F_3 \setminus F_2 = E) \cdot P(F_2 = E) + H(F_3 \setminus F_2 = F) \cdot P(F_2 = F) +$$
$$+ H(F_3 \setminus F_2 = G) \cdot P(F_2 = G) + H(F_3 \setminus F_2 = H) \cdot P(F_2 = H) +$$
$$+ H(F_3 \setminus F_2 = I) \cdot P(F_2 = I) + H(F_3 \setminus F_2 = J) \cdot P(F_2 = J)$$

$P(F_3 = A \setminus F_2 = A,B,C,D,E) = 1$
$P(F_3 = B \setminus F_2 = A,B,C,D,E) = \phi$

$H(F_3 \setminus F = A,B,C,D,E) = \phi$

No hay información ....

$P(F_3 = A \setminus F_2 = F,G,H,I,J) = 0'2$
$P(F_3 = B \setminus F_2 = F,G,H,I,J) = 0'8$

$H(F_3 \setminus F_2 = F,G,H,I,J) =$

$= 0'2 \cdot \log_4 \frac{1}{0'2} + 0'8 \cdot \log_4 \frac{1}{0'8} =$

$= 0'23219 + 0'12877 =$

$= 0'36096$ $\frac{\text{dígitos cuaternarios}}{\text{símbolo}}$.

$H(F_3 \setminus F_2) = 0'36096 \cdot (0'1 \cdot 3 + 0'2 \cdot 2) = 0'25267$

$H(F_3 \setminus F_2) = 0'25267$ $\frac{\text{dígitos cuaternarios}}{\text{símbolo}}$

$H(F_3, F_2) = 1'56095 + 0'25267 = 1'82217$ $\frac{\text{dig. cuat.}}{\text{símb.}}$

05/12/03 Problema 2

a) $A \rightarrow N_A = p_A \cdot q_A = 3 \cdot 11 = 33$;; $\phi(N_A) = (p_A - 1) \cdot (q_A - 1) = 2 \cdot 10 = 20$

¿ $\text{mcd}(e_A, \phi(N_A)) = 1$? Sí $\Rightarrow \exists\ d_A = e_A^{-1} \bmod \phi(N_A)$

e_A: 3 ; $\phi(N_A)$: $30 = 5 \cdot 2^2$

$e_A \cdot d_A = 1 + K \cdot \phi(N_A) \rightarrow d_A = \dfrac{1 + K \cdot 20}{3} = \dfrac{1 + K \cdot (6 \cdot 3 + 2)}{3} = 6K + \dfrac{2K+1}{3}$

$20 \mid 3$
$2 \quad 6$

$d_A = 6 + 1 = 7$ (K = 1)

$K_{PA} = (e_A, N_A) = (3, 33)$
$K_{SA} = d_A = 7$

$B \rightarrow N_B = p_B \cdot q_B = 7 \cdot 17 = 119$;; $\phi(N_B) = (p_B - 1) \cdot (q_B - 1) = 6 \cdot 16 = 96$

¿ $\text{mcd}(d_B, \phi(N_B)) = 1$? Sí $\Rightarrow \exists\ e_B^{-1} = d_B \bmod \phi(N_B)$

d_B: 35 $= 7 \cdot 5$; $\phi(N_B)$: 96 $= 2^5 \cdot 3$

$e_B \cdot d_B = 1 + K \cdot \phi(N_B) \rightarrow e_B = \dfrac{1 + K \cdot 96}{35} = \dfrac{1 + K \cdot (35 \cdot 2 + 26)}{35} =$

$96 \mid 35$
$26 \quad 2$

$= 2K + \dfrac{26K + 1}{35} = 2 + 3 = 11$ (K = 4)

$K_{PB} = (e_B, N_B) = (11, 119)$
$K_{SB} = d_B = 35$

b) CA → A

$A \rightarrow CA \Rightarrow ID_A \| e_A \| N_A = 0001 \| 0011 \| 0010 \| 0001$ ($ID_A = 1$, $e_A = 3$, $N_A = 33$)

$N_A = 33_d = 100001 = 0010 \| 0001$

Certificado en claro$_A$ = 1321_H

M_A: 0001 0011 0010 0001 ; n = 4

m_0 m_1 m_2 m_3

$h_0 = 4$

$h_1 = E(h_0 \oplus m_0) = E(0100 \oplus 0001) = E(0101) = E(5) = (5 \cdot 5 + 2)_{16} = 27_{16} = 11 \equiv 1011$

$h_2 = E(h_1 \oplus m_1) = E(1011 \oplus 0011) = E(1000) = E(8) = (8 \cdot 5 + 8)_{16} = 42_{16} = 10 \equiv 1010$

$h_3 = E(h_2 \oplus m_2) = E(1010 \oplus 0010) = E(1000) = E(8) = \dots = 1010$

$h_4 = E(h_3 \oplus m_3) = E(1010 \oplus 0001) = E(1011) = E(11) = (5 \cdot 11 + 2)_{16} = 57_{16} = 9 \equiv 1001 = H(M_A)$

CA firma $H(M_A)$ con su clave secreta, $d_{CA} = 13$:

$FD_A = H(M_A)^{d_{CA}} \bmod N_{CA} = 9^{13} \bmod 77 = 58$

$9^{13} = \left((9^2 \cdot 9)^2\right)^2 \cdot 9$

$81_{77} = 4$

$36^2 = 1296_{77} = 64$

$64^2 = 4096_{77} = 15$

$15 \cdot 9 = 135_{77} = 58$

$FD_A = 58 \equiv 0011\,1010_b \equiv 3A_H$

Certificado firmado (A) = $0001 \| 0011 \| 0010 \| 0001 \| 0011 \| 1010 =$

($ID_A = 1$, $e_A = 3$, $N_A = 33$; $FD(M_A)$; M_A)

$= 13213A_{16}$

CA → B

$B \to CA \Rightarrow \quad ID_B \| e_B \| N_B = 0010 \| 1011 \| 0111 \| 0111$

(ID_B, e_B, $N_B = 119$)

Certificado en Claro$_B$ = $2B77_{16}$

$M_B = \underbrace{0010}_{m_0}\ \underbrace{1011}_{m_1}\ \underbrace{0111}_{m_2}\ \underbrace{0111}_{m_3} \qquad n = 4$

$h_0 = 4$

$h_1 = E(h_0 \oplus m_0) = E(0100 \oplus 0010) = E(0110) = E(6) = (5 \cdot 6 + 2)_{16} = 32_{16} = \emptyset \equiv 0000$

$h_2 = E(h_1 \oplus m_1) = E(0000 \oplus 1011) = E(1011) = E(11) = (5 \cdot 11 + 2)_{16} = 57_{16} = 9 \equiv 1001$

$h_3 = E(h_2 \oplus m_2) = E(1001 \oplus 0111) = E(1110) = E(14) = (5 \cdot 14 + 2)_{16} = 72_{16} = 8 \equiv 1000$

$h_4 = E(h_3 \oplus m_3) = E(1000 \oplus 0111) = E(1111) = E(15) = (5 \cdot 15 + 2)_{16} = 77_{16} = 13 \equiv 1101 = H(M_B)$

CA firma $H(M_B)$ con su clave secreta, $d_{CA} = 13$:

$FD_B = H(M_B)^{d_{CA}} \bmod N_{CA} = 13^{13} \bmod 77 = 41$

$13^{13} = \left(\left(13^2 \cdot 13\right)^2\right)^2 \cdot 13$

$169_{77} = 15$

$15 \cdot 13 = 195_{77} = 41$

$41^2 = 1681_{77} = 64$

$64^2 = 4096_{77} = 15$

$15 \cdot 13 = 195_{77} = 41$

$FD_B = 41_d \equiv 0010\,1001_b \equiv 29_H$

Certificado firmado (B) = $0010 \| 1011 \| 0111 \| 0111 \| 0010 \| 1001$ =

($ID_B = 2$, $e_B = 11$, $N_B = 119$, $FD(H_B)$; M_B)

$= \boxed{2B7729_H}$

c)
- A y B han obtenido sus certificados firmados de CA.
- A y B se los intercambian.
- A autentica la clave pública de B extrayendola del certificado de B, decodificando $FD(H_B)$ mediante (e_{CA}, N_{CA}), recalculando $H(H_B)$:
  - Extrae (e_B, N_B) del certificado de B.
  - Decodifica $FD(M_B)$ con $(e_{CA}, N_{CA}) = K_{PCA}$: $H(M_B$
  - Recalcula $H(H_B)$ y si coincide con el anterior, queda A autenticado.
- B autentica la K_{PA} haciendo los mismos pasos con el certificado de A.

d)
- Clave de sesion que A envia a B, codificada:

$$C_{A\to B} = (K_{A\to B})^{e_B} \bmod N_B = 10^{11} \bmod 119 = 54$$

Después, B la decodificará y recuperará $K_{A\to B}$:

$$K_{A\to B} = (C_{A\to B})^{d_B} \bmod N_B = 54^{35} \bmod 119 = 10$$

$35 \equiv 100011$ // $54^{35} = (((((54^2)^2)^2)\cdot 54)^2)\cdot 54$

$54^2 = 2916_{119} = 60$
$60^2 = 3600_{119} = 30$
$30^2 = 900_{119} = 67$
$67^2 = 4489_{119} = 86$
$86 \cdot 54 = 4644_{119} = 3$
$3^2 = 9_{119} = 9$
$9 \cdot 54 = 486_{119} = 10$ //

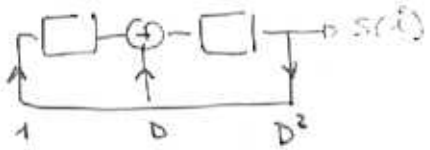
• Clave de sesión que B envía a A, codificada:

$$C_{B\to A} = (K_{B\to A})^{e_A} \bmod N_A = 5^3 \bmod 33 = 125_{33} = 26$$

Después, A la decodifica y recupera la $K_{B\to A}$:

$$K_{B\to A} = (C_{B\to A})^{d_A} \bmod N_A = 26^7 \bmod 33 = 5 \;//$$

e) $C(D) = D^2 + D + 1$, polinomio primitivo de grado 2: $L = 2^{\#} - 1 = 3$.



$$K_{A\to B} = 10 = 3\cdot L + 1$$

$$P^{(10)}(D) = P^{(1)}(D)$$

L es la longitud del periodo de la secuencia pseudoaleatoria s(i) generada por el LFSR:

10
01
11
10
01
11
⋮

s(i) = ...110|110→

←L=3→

$P^{(0)}(D)$ $P^{(0)}(D)$

$M_{\overline{AB}}$ = 00|10|01|10|11

↓ ↓ ↓ ↓ ↓

$C_{\overline{AB}}$ = 00 01 11 01 10

$P^{(1)}(D)$ $P^{(1)}(D)$

→ La codificación es avanzar un estado en el LFSR.

$$K_{B\to A} = 5 = 1\cdot L + 2 \Rightarrow P^{(5)}(D) = P^{(2)}(D)$$

La codificación que realiza B, es avanzar dos estados en el LFSR:

M_{BA} = 11 001 → $P^{(0)}(D)$

C_{BA} = 01 11 10 → $P^{(2)}(D)$