Transmissió de dades

Problemes resolts

Mónica Aguilar Igartua
Jordi Forné Muñoz
Jordi Mata Díaz
Francisco Rico Novella
Alfonso Rojas Espinosa
Miquel Soriano Ibáñez

UPCGRAU 79

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Transmissió de dades

Problemes resolts

Mónica Aguilar Igartua
Jordi Forné Muñoz
Jordi Mata Díaz
Francisco Rico Novella
Alfonso Rojas Espinosa
Miquel Soriano Ibáñez

UPCGRAU 79

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Amb el suport de

Generalitat de Catalunya
Departament de Recerca i Universitats

Traducció del llibre: *Transmisión de datos. Problemas resueltos*
Traductor: Gabriel Genescà Dueñas

Primera edició: juny de 2024

© Els autors, 2024
© Iniciativa Digital Politècnica, 2024
Oficina de Publicacions Acadèmiques Digitals de la UPC
Edificio K2M, Planta S1, Despacho S103-S104
Jordi Girona 1-3, 08034 Barcelona
Tel.: 934 015 885
www.upc.edu/idp
E-mail: info.idp@upc.edu

Producción: Service Point
Pau Casals, 161-163
08820 El Prat de Llobregat (Barcelona)

ISBN:978-84-10008-61-8
ISBN digital: 978-84-10008-62-5
DL: B 13392-2024
DOI: 10.5821/ebook-9788410008625

Qualsevol forma de reproducció, distribució, comunicació pública o transformació d'aquesta obra només es pot fer amb l'autorització dels seus titulars, excepte l'excepció prevista a la llei.

Índex

Índex de figures

1
Codificació de font

1.1. Introducció

La transmissió de dades és el conjunt de tècniques i conceptes que sorgeixen en estudiar el problema de la transmissió d'informació digital, independentment de quins siguin el seu origen i la seva naturalesa. La transmissió es farà a través d'un canal físic limitat en ample de banda i potència, com poden ser un parell de cables, un cable coaxial, una fibra òptica, un radioenllaç o una combinació de tots ells.

Una descripció global del que constitueix la transmissió de dades ha de començar fent una distinció conceptual dels diferents elements de què es compon. Aquesta divisió permetrà comprendre millor el problema i, en conseqüència, poder-lo analitzar millor.

El primer pas és la compressió de les fonts de dades (veu, imatges, dades digitals, etc.) a partir de la definició del concepte d'informació realitzada per Shannon [ABR63]. La formalització del concepte d'informació ens porta, a més, a estudiar el comportament d'un sistema considerant la transmissió de seqüències de dades aleatòries. D'aquesta manera, el problema inicial s'ha dividit en dos: la caracterització de la font i la caracterització del canal, tot això sense pèrdua de generalitat.

En aquest capítol, es tracta el problema partint d'una font discreta equivalent. En general, la transmissió de les dades tal com surten de la font comportaria un malbaratament de recursos. Per reduir-ne la redundància, hem de recórrer a la compressió [HAN03]. Shannon estableix un límit teòric per sota del qual ja no es pot comprimir més sense que hi hagi pèrdues. Aquest límit depèn de l'estadística d'emissió i s'anomena *entropia*. L'entropia és un paràmetre bàsic i propi de la font.

Alguns codificadors de font requereixen conèixer exactament i a priori les característiques estadístiques d'emissió, mentre que d'altres van adquirint aquest coneixement

d'una manera adaptativa a partir de les pròpies dades emeses. Un exemple dels primers és el codificador de Huffman i dels segons, el codificador de Ziv-Lempel.

En tots dos casos, després del procés de compressió s'obté una seqüència de bits independents, que caracteritzarem amb una font binària equivalent. El procés següent és mapejar aquests bits en els símbols de l'alfabet d'entrada del sistema modulador, mitjançant la codificació elegida. En aquest punt, el problema es redueix a la transmissió d'aquests símbols al receptor, que farà el procés de descodificació invers convertint-los en una seqüència de bits que idealment coincidirà amb l'emesa. La màxima velocitat a què es pot transmetre aquesta seqüència de bits d'una manera fiable s'anomena *capacitat del canal* i fou establerta també per Shannon [COV06].

1.2. Continguts teòrics

- Teoria de la informació
  - Concepte d'informació
  - Entropia. Entropia conjunta. Entropia condicional
  - Informació mútua
  - Entropia d'una font amb memòria
- Codificació
  - Codis instantanis
  - Codis de Huffman
  - Codis de ràfegues
  - Codis aritmètics
  - Codis diccionari
- Capacitat de canal
  - Caracterització d'un canal discret
  - Capacitat d'un canal simètric sense memòria

1.3. Bibliografia

[ABR63] Abranson, N. (1963): *Information Theory and Coding*. McGraw-Hill Education. ISBN-10: 0070001456.

[HAN03] Hankerson, D.C.; Harris, G.; Johnson P.D. (2003): *Introduction to Information Theory and Data Compression*. 2a ed. Chapman & Hall. ISBN-10: 1584883138.

[COV06] Cover, T.; Thomas, J.A. (2006): *Elements of Information Theory*. 2a ed. Wiley-Inter Science. ISBN-10: 0471241954.

1.4. Problemes

Problema 1

Siguin $F_1 = \{1, 2, 3, 4\}$ y $F_2 = \{2, 4, 6, 8\}$ dues fonts equiprobables independents. Sigui una font (F) la sortida de la qual és el mínim comú múltiple de la sortida de les fonts anteriors $F = mcm(F_1, F_2)$.

a) Calculeu l'entropia de la font $H(F)$.

b) Calculeu la informació mútua $I(F, F_1)$.

c) Calculeu la longitud mitjana d'una codificació de Huffman de la font F.

d) Suposeu que us proposen endevinar F i, com a ajuda, us deixen escollir entre conèixer F_1 o conèixer F_2. Quina opció preferiríeu? Justifiqueu la resposta i calculeu la probabilitat d'endevinar F amb l'opció que heu escollit abans.

Solució

a) A continuació, es mostra una taula amb els resultats d'aplicar el *mcm*:

F_1	F_2	F
1	2	2
2	2	2
3	2	6
4	2	4
1	4	4
2	4	4
3	4	12
4	4	4
1	6	6
2	6	6
3	6	6
4	6	12
1	8	8
2	8	8
3	8	24
4	8	8

Taula 1.1: Generació de símbols de la font F

$F = \{2, 4, 6, 8, 12, 24\}$ amb les probabilitats següents:

$$P(2)=\frac{1}{8},\quad P(4)=\frac{1}{4},\quad P(6)=\frac{1}{4},\quad P(8)=\frac{3}{16},\quad P(12)=\frac{1}{8},\quad P(24)=\frac{1}{16}$$

$H(F)=2.453$ bits

b) $I(F,F_1)=H(F)-H(F|F_1)$

Calculem $H(F|F_1)$ per a tots els valors F_1 i fem la mitjana

$$F_1=\begin{cases}1\Rightarrow H(F|1)=2\\ 2\Rightarrow H(F|2)=2\\ 3\Rightarrow H(F|3)=\frac{1}{2}\cdot 1+\frac{1}{4}\cdot 2+\frac{1}{4}\cdot 2=1.5\\ 4\Rightarrow H(F|4)=1.5\end{cases}$$

$$H(F|F_1)=\frac{1}{2}\cdot 2+\frac{1}{2}\cdot 1.5=1.75 \text{ bits}$$

$$I(F,F_1)=H(F)-H(F|F_1)=2.453-1.75=0.703 \text{ bits}$$

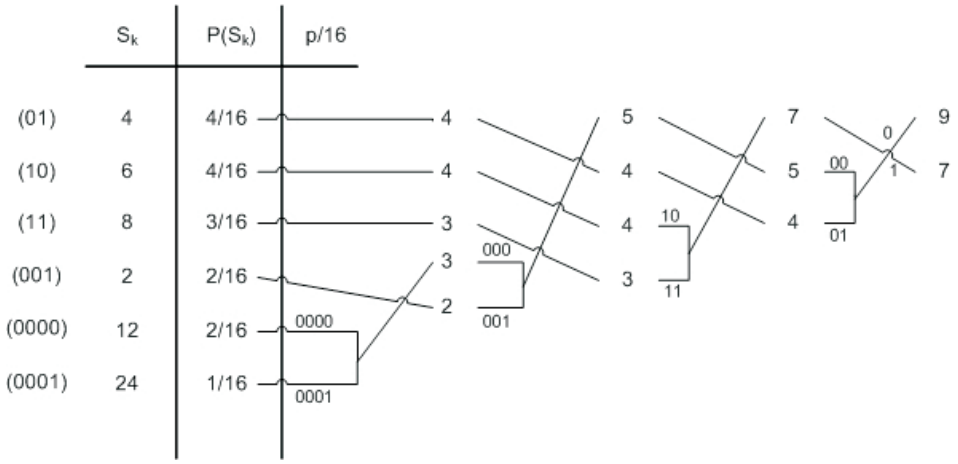


Fig. 1.1: Codificació de Huffman

c) Calculem una codificació de Huffman de F.

Fem la mitjana de la longitud de codificació de cada símbol per la seva probabilitat:

$$\bar{l}=\sum_k p(s_k)l_k=\frac{11}{16}\cdot 2+\frac{2}{16}\cdot 3+\frac{3}{16}\cdot 4=\frac{40}{16}=2{,}5 \text{ bits}$$

d) A l'apartat b, hem calculat $H(F|F_1)=1.75$. Aquí calculem $H(F|F_2)$.

$$F_2 = \begin{cases} 2 \Rightarrow H(F|2) = 1.5 \\ 4 \Rightarrow H(F|4) = \frac{3}{4} \cdot \log_2\left(\frac{4}{3}\right) + \frac{1}{4} \cdot 2 = 0.811 \\ 6 \Rightarrow H(F|6) = 0.811 \\ 8 \Rightarrow H(F|8) = 0.811 \end{cases}$$

$H(F|F_2) = 0.98325$ bits/símbol

Com que $H(F|F_2) < H(F|F_1)$, és més fàcil endevinar F coneixent F_2 (hi ha menys incertesa). A la taula 1.2, es calcula la probabilitat d'endevinar F, si es coneix F_2. Llistem el valor de F que triem com a més probable per a cadascun dels possibles valors de F_2, així com la probabilitat d'endevinar corresponent.

Trio			p(endevinar)
$F_2 = 2$	$\longrightarrow$	$F = 2$	1/2
$F_2 = 4$	$\longrightarrow$	$F = 4$	3/4
$F_2 = 6$	$\longrightarrow$	$F = 6$	3/4
$F_2 = 8$	$\longrightarrow$	$F = 8$	3/4

Taula 1.2: Valors de F seleccionats en funció dels valors de F_2

Finalment, ponderant per les diferents probabilitats:

$$p\,(\text{endevinar}) = \frac{1}{4} \cdot \frac{2}{4} + \frac{3}{4} \cdot \frac{3}{4} = \frac{11}{16} = 0.6875$$

Problema 2

Dues fonts d'informació, S_1 i S_2, emeten símbols d'un alfabet $\{A, B, C, D, E, F, G, H, I\}$ amb una probabilitat

$P(A) = 1/3;\ P(B) = P(C) = P(D) = P(E) = P(F) = 1/9; P(G) = P(H) = P(I) = 1/27$

Ambdues fonts fan servir, respectivament, un canal de comunicacions ternari per transmetre la informació. Per maximitzar l'explotació de l'ample de banda del canal, s'utilitza en cada cas un codificador de font els codis del qual fan servir símbols de l'alfabet **{–1, 0, 1}**

a) Determineu si existeix un codi instantani en què la codificació de tots els símbols de font doni lloc a paraules codi de longitud 2.

b) Quina és la longitud mitjana mínima de les paraules codi per a una font, S_1 o S_2?

c) Calculeu, mitjançant l'algoritme de Huffman, les paraules codi per a cadascun dels símbols de font. Quina és l'eficiència del codi resultant?

d) Quina seria una cota superior de l'entropia conjunta de les fonts S_1 i S_2 en bits?

S'observa en la generació de símbols de les fonts que hi ha una dependència entre les fonts S_1 i S_2. Aquesta dependència es manifesta de la manera següent:

I) Quan S_1 emet A, llavors S_2 tan sols emet A.
II) Quan S_1 emet B, C o D, llavors S_2 tan sols emet B, C o D.
III) Quan S_1 emet E, F, G, H o I, llavors S_2 tan sols emet E, F, G, H o I.

e) Tenint en compte la dependència entre les fonts, calculeu l'entropia de la font S_2 en bits per als casos en què la font S_1 pren el valor: $S_1 = A$ y $S_1 = C$.

Solució

Dues fonts d'informació, S_1 i S_2

$$P(A) = \frac{1}{3}; \quad P(B) = P(C) = P(D) = P(E) = P(F) = \frac{1}{9}; \quad P(G) = P(H) = P(I) = \frac{1}{27}$$

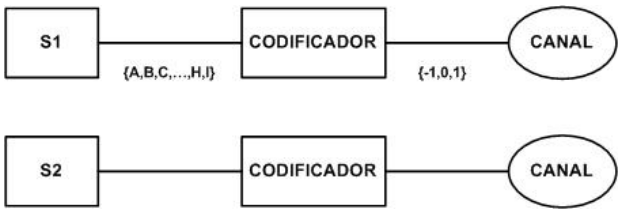


Fig. 1.2: Esquema de codificació

a) Perquè un codi sigui instantani, ha de complir la desigualtat de Kraft:

$$\sum_{k=1}^{n} D^{-L_k} \leq 1$$

En el nostre cas: $n = 9$ nombre de símbols de font
$D = 3$ nombre de símbols que fan servir els codis
$L_k = 2 \; \forall k$ longitud de tots els codis

$$\sum_{k=1}^{9} 3^{-2} = \sum_{k=1}^{9} \frac{1}{9} = 1 \leq 1$$

Per tant, hi ha un codi instantani les paraules del qual són de longitud 2.

b) La longitud mínima ve determinada per l'entropia de la font, $\overline{L}_{\min} = H$

Com que el codi és ternari, hem d'utilitzar base 3.

$$\overline{L}_{\min} = \sum_{k=1}^{9} p_k \cdot \log_3 \frac{1}{p_k} = -\sum_{k=1}^{9} p_k \cdot \log_3 p_k$$

$$= \frac{1}{3} \cdot \log_3 3 + 5 \cdot \frac{1}{9} \log_3 3^2 + 3 \cdot \frac{1}{27} \log_3 3^3$$

$$= \frac{1}{3} + \frac{10}{9} + \frac{1}{3} = 1{,}77 \text{ digits ternaris}$$

$\overline{L}_{\min} = 1{,}77$ dígits ternaris/símbol

c) Calculem la codificació per Huffman.

Ordenem per probabilitat	font reduïda 1 ordenada	font reduïda 2	font reduïda 2 ordenada	font reduïda 3 ordenada
$A \to 1/3$	$A \to 1/3$	$A \to 1/3$	$A \to 1/3$	$A \to 1/3$
$B \to 1/9$	$B \to 1/9$	$B \to 1/9$	$K \to 1/3$	$K \to 1/3$
$C \to 1/9$	$C \to 1/9$	$C \to 1/9$	$B \to 1/9$	$L \to 1/3$
$D \to 1/9$	$D \to 1/9$	$D \to 1/9$	$C \to 1/9$	
$E \to 1/9$	$E \to 1/9$	$K \to 1/3$	$D \to 1/9$	
$F \to 1/9$	$F \to 1/9$			
$G \to 1/27$	$J \to 1/9$			
$H \to 1/27$				
$I \to 1/27$				

I obtenim com a resultat:

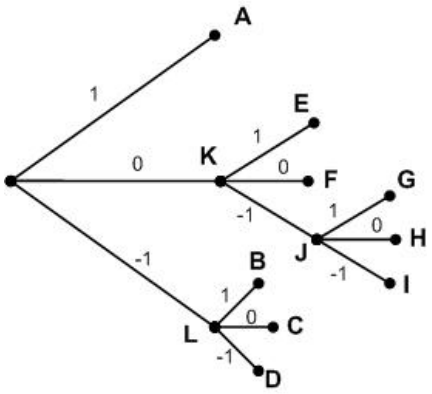


Fig. 1.3: Codificació ternària de Huffman

A	$\rightarrow$	1		
B	$\rightarrow$	-1	1	
C	$\rightarrow$	-1	0	
D	$\rightarrow$	-1	-1	
E	$\rightarrow$	0	1	
F	$\rightarrow$	0	0	
G	$\rightarrow$	0	-1	1
H	$\rightarrow$	0	-1	0
I	$\rightarrow$	0	-1	-1

Taula 1.3: Taula de codificació ternària

Atès que la longitud del codi de cada símbol coincideix amb la informació que proporciona (en base 3), llavors és immediat que: $\overline{L}_{\min} = 1{,}77 \implies E = \dfrac{H}{\overline{L}} = 1$

d) Una cota superior de $H(S_1, S_2)$ s'obté quan ambdues fonts són independents:

$H(S_1, S_2) \leq H(S_1) + H(S_2)|_{\{H(S_1)=H(S_2)\}} = 2 \cdot H(S_1) = 2 \cdot H(S_2)$. Per expressar la informació en bits, fem servir base 2:

$$H(S_1) = \frac{1}{3} \cdot \log_2 3 + \frac{5}{9}\log_2 3^2 + \frac{3}{27}\log_2 3^3 = 2{,}81 \text{ bits}$$

$$H(S_1, S_2) \leq 5{,}63 \text{ bits}$$

e) Quan

$S_1 = A \implies S_2 = A$
$S_1 = C \implies S_2 = B$ o $S_2 = C$ o $S_2 = D$

les probabilitats condicionades són: $P(S_2 = A|S_1 = A) = 1$

Per al cas $S_1 = C$, hi ha tres símbols. Considerant que aquests símbols mantenen la relació de probabilitats de la font S_2, llavors:

$$P(S_2 = B|S_1 = C) + P(S_2 = C|S_1 = C) + P(S_2 = D|S_1 = C) = 1$$

$$P(S_2 = B|S_1 = C) = \frac{P(S_2 = B)}{P(S_2 = B) + P(S_2 = C) + P(S_2 = D)} = \frac{1}{3}$$

De la mateixa manera, $P(S_2 = C|S_1 = C) = P(S_2 = D|S_1 = C) = \dfrac{1}{3}$.

Finalment,

$$H(S_2|S_1 = A) = P(S_2 = A|S_1 = A) \cdot \log_2 \frac{1}{P(S_2 = A|S_1 = A)} = 0$$

$$\begin{aligned} \mathrm{H}(S_2|S_1 = C) &= 3 \cdot P(S_2 = B|S_1 = C) \cdot \log_2 \frac{1}{P(S_2 = B|S_1 = C)} = 3 \cdot \frac{1}{3} \log_2 3 \\ &= 1{,}58 \text{ bits} \end{aligned}$$

Es pot comprovar que $H(S_2|S_1) = 1{,}23$ bits

$H(S_1, S_2) = H(S_1) + H(S_2|S_1) = 5{,}1$ bits

Problema 3

Una font binària simètrica F emet ràfegues de longitud L, amb $L > 0$, segons una distribució geomètrica de paràmetre p:

$$Prob[L = k] = p^{k-1}(1 - p), \quad \text{amb} \quad k = 1, 2, \ldots \text{i} \quad 0 < p < 1$$

a) Proposeu un model markovià de la font F, amb memòria 1, i avalueu-ne l'entropia H(F) per a un valor p genèric. Particularitzeu el resultat per a $p = 1/2$.

b) Aplicant una codificació de font per ràfegues, resulta una font F' els símbols de la qual representen la longitud de les ràfegues de F, $\{1, 2, 3, \ldots\}$.

I) Determineu l'entropia $H(F')$ per a $p = 1/2$.
II) Suposant que, a la pràctica, la font no genera ràfegues de longitud superior a 7 i, negligint la probabilitat d'aquests casos, feu una codificació binària de Huffman de F' per al cas $p = 1/2$.
III) A partir dels resultats obtinguts als apartats anteriors, analitzeu els avantatges i els inconvenients de la codificació per ràfegues per al cas $p = 1/2$.

Solució

a) La font F genera ràfegues de 0 i 1. Un model markovià amb memòria 1 de F seria:

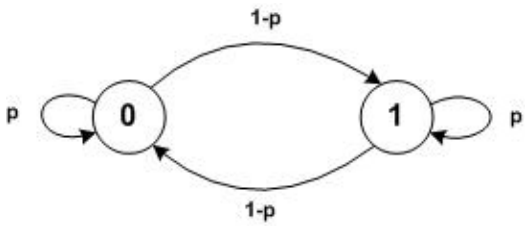


Fig. 1.4: Font markoviana de memòria 1

Per simetria: $Prob(F = 0) = Prob(F = 1) = \frac{1}{2}$

Per simetria: $H(F_n|F_{n-1}=1) = H(F_n|F_{n-1}=0) = H(\,p)$

Llavors: $H(F) = P(F=1)\cdot H(F_n|F_{n-1}=1) + P(F=0)\cdot H(F_n|F_{n-1}=0) = H(\,p)$

Si $p = 1/2 \;\Rightarrow\; H(F) = 1$ bit/símbol i la font no té memòria.

b) $F' = \{1,2,3,4,\ldots\}\; Prob(F'=k) = Prob[L=k] = p^{k-1}(1-p)$

I) $H(F') = p_1 \log_2 \dfrac{1}{p_1} + p_2 \log_2 \dfrac{1}{p_2} + p_3 \log_2 \dfrac{1}{p_3} + \cdots$

$$\begin{aligned} p_1 &= Prob[F'=1] = 1-p \\ p_2 &= Prob[F'=2] = (1-p)\,p \\ p_3 &= Prob[F'=3] = (1-p)^2 \\ \vdots &= \vdots \\ p_k &= Prob[F'=K] = (1-p)\,p^{k-1} \end{aligned}$$

$$H(F') = \sum_{k=1}^{\infty} p_k \log_2 \frac{1}{p_k} = \sum_{k=1}^{\infty} \left[(1-p)\,p^{k-1} \log_2 \frac{1}{(1-p)\,p^{k-1}} \right]$$

$$H(F') = (1-p)\sum_{k=1}^{\infty} - p^{k-1}\left[\log_2(1-p) + \log_2\, p^{k-1}\right]$$

$$H(F') = -(1-p)\left[\sum_{k=1}^{\infty} \log_2(1-p)\,p^{k-1} + \sum_{k=1}^{\infty} (k-1)\,p^{k-1} \log_2\, p \right]$$

$$= -(1-p)\log_2(1-p)\sum_{k=1}^{\infty} p^{k-1} - (1-p)\log_2\, p \sum_{k=1}^{\infty} (k-1)\,p^{k-1}$$

Atès que

$$\sum_{0}^{\infty} p^k = \frac{1}{1-p} \quad \text{y} \quad \sum_{0}^{\infty} k\,p^k = \frac{p}{(1-p)^2}$$

s'obté:

$$H(F') = -\frac{p}{1-p}\log_2\, p - \log_2(1-p)$$

Si $p = 1/2$, llavors

$$H(F') = -\log_2 \frac{1}{2} - \log_2 \frac{1}{2} = 2 \text{ bits } F'$$

II) $K = \{1,2,3,4,5,6,7\} \quad Prob[L \geq 8] \simeq 0$

Suposant $p = 1/2$, la codificació de Huffman serà

$p_1 = 0.5$
$p_2 = 0.250$
$p_3 = 0.125$
$p_4 = 0.0625$
$p_5 = 0.03125$
$p_6 = 0.015625$
$p_7 = 0.0078125$

Com que les probabilitats difereixen tant entre si, la codificació és directa.

En particular, es té que:

$p_A = (p_6 + p_7) = 0.0234375$
$p_B = (p_5 + p_A) = 0.0546$
$p_C = (p_4 + p_B) = 0.11718$
$p_D = (p_3 + p_C) = 0.242$
$p_E = (p_2 + p_D) = 0.492$

Desenvolupant la codificació de Huffman obtinguda, tenim:

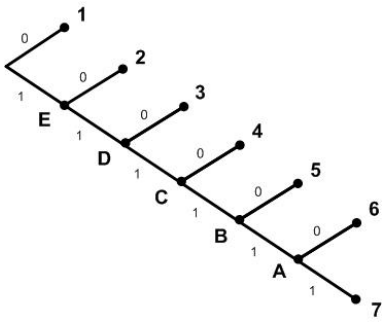


Fig. 1.5: Codificació de Huffman de la longitud de les ràfegues

i la taula de codificació que en resulta és:

$$
\begin{aligned}
1 &\rightarrow 0 \\
2 &\rightarrow 1\,0 \\
3 &\rightarrow 1\,1\,0 \\
4 &\rightarrow 1\,1\,1\,0 \\
5 &\rightarrow 1\,1\,1\,1\,0 \\
6 &\rightarrow 1\,1\,1\,1\,1\,0 \\
7 &\rightarrow 1\,1\,1\,1\,1\,1
\end{aligned}
$$

III) Observeu que, si no s'hagués truncat la longitud de les ràfegues, cada valor de longitud requereix un nombre de dígits de codificació igual a la mida de la ràfega. Per tant, aquesta codificació no ofereix cap avantatge respecte d'enviar el valor de cada símbol de F per a $p = 1/2$. De forma equivalent, si $p = 1/2$, la font no té memòria i els símbols són equiprobables, de manera que la codificació a ràfegues no té avantatges.

Problema 4

La trajectòria d'un cotxe es pot modelar com la d'un objecte que es mou a través d'una retícula quadriculada amb passos elementals, en direccions verticals o horitzontals, fent un sol pas cada vegada. Així, el seu moviment es pot representar com una successió de símbols del conjunt N, S, E, i W, que representen els passos successius en les direccions nord, sud, est i oest, respectivament.

El comportament d'aquest cotxe té memòria: el 50 % de les vegades repeteix el moviment anterior i, en la resta dels casos, fa un gir de 90° a la dreta (amb probabilitat 30 %) o a la esquerra (amb probabilitat del 20 %) respecte al pas anterior.

Es demana:

a) Modelar el procés que descriu el moviment.

b) Calcular la probabilitat de cadascun dels símbols.

c) Calcular l'índex d'entropia d'aquesta font d'informació.

d) Dissenyar un codificador Huffman d'aquesta font.

Solució

Abans \ Ara	N	S	E	W
N	0,5	–	0,3	0,2
S	–	0,5	0,2	0,3
E	0,2	0,3	0,5	–
W	0,3	0,2	–	0,5

a) Es pot modelar el procés amb una cadena de Markov, memòria 1, amb un diagrama de probabilitats de transmissió d'estats:

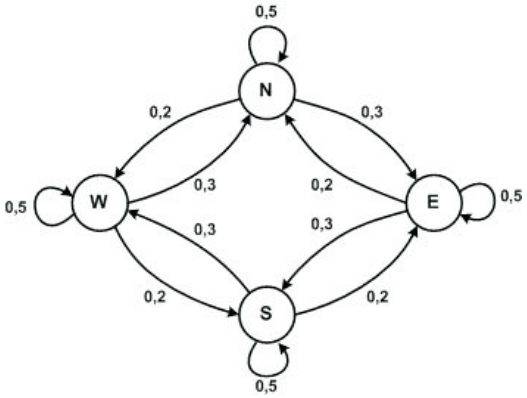


Fig. 1.6: Diagrama d'estats del procés de moviment del vehicle

b)

$$
\begin{aligned}
P(N) &= P(N|N)\cdot P(N) + P(N|S)\cdot P(S) + P(N|E)\cdot P(E) + P(N|W)\cdot P(W)\\
P(S) &= P(S|N)\cdot P(N) + P(S|S)\cdot P(S) + P(S|E)\cdot P(E) + P(S|W)\cdot P(W)\\
P(E) &= P(E|N)\cdot P(N) + P(E|S)\cdot P(S) + P(E|E)\cdot P(E) + P(E|W)\cdot P(W)\\
P(W) &= P(W|N)\cdot P(N) + P(W|S)\cdot P(S) + P(W|E)\cdot P(E) + P(W|W)\cdot P(W)
\end{aligned}
$$

$$
\begin{aligned}
0.5\cdot P(N) &= 0.2\cdot P(E) + 0.3\cdot P(W) \longrightarrow P(N) = 0.4\cdot P(E) + 0.6\cdot P(W)\\
0.5\cdot P(S) &= 0.3\cdot P(E) + 0.2\cdot P(W) \longrightarrow 2P(S) = 0.6\cdot P(E) + 0.4\cdot P(W)\\
0.5\cdot P(E) &= 0.3\cdot P(N) + 0.2\cdot P(S) \longrightarrow 2P(E) = 0.6\cdot P(N) + 0.4\cdot P(S)\\
0.5\cdot P(W) &= 0.2\cdot P(N) + 0.3\cdot P(S) \longrightarrow 2P(W) = 0.4\cdot P(N) + 0.6\cdot P(S)
\end{aligned}
$$

Resolent:

$$P(N) + P(S) = P(E) + P(W)$$

$$P(N) + P(S) + P(E) + P(W) = 1 \longrightarrow 2\cdot P(N) + 2\cdot P(S) = 1$$

$$P(N) + P(S) = \frac{1}{2}$$

$$P(E) + P(W) = \frac{1}{2}$$

$$
\begin{aligned}
P(N) &= 0.4\cdot (\overbrace{0.6\cdot P(N) + 0.4\cdot P(S)}^{P(E)}) + 0.6\cdot (\overbrace{0.4\cdot P(N) + 0.6\cdot P(S)}^{P(W)})\\
&= 0.24\cdot P(N) + 0.16\cdot P(S) + 0.24\cdot P(N) + 0.36\cdot P(S)\\
&= 0.48\cdot P(N) + 0.52\cdot P(S)
\end{aligned}
$$

$$0.52 \cdot P(N) = 0.52 \cdot P(S) \implies P(N) = P(S) \implies P(N) = P(S) = \frac{1}{4}$$

$$P(E) = 0.6 \cdot (\overbrace{0.4 \cdot P(E) + 0.6 \cdot P(W)}^{P(N)}) + 0.4 \cdot (\overbrace{0.6 \cdot P(E) + 0.4 \cdot P(W)}^{P(S)})$$

$$= 0.24 \cdot P(E) + 0.36 \cdot P(W) + 0.24 \cdot P(E) + 0.16 \cdot P(W)$$

$$P(E) = P(W) \implies P(E) = P(W) = \frac{1}{4}$$

c) $H(F) = H(F|N) \cdot P(N) + H(F|S) \cdot P(S) + H(F|E) \cdot P(E) + H(F|W) \cdot P(W)$

Totes les entropies condicionades són iguals, atès que les probabilitats de transició a tots els estats són iguals.

$$\begin{aligned} H(F|N) &= H(F|S) = H(F|E) = H(F|W) \\ H(F|N) &= P(N|N) \cdot \log_2\left(\frac{1}{P(N|N)}\right) + P(S|N) \cdot \log_2\left(\frac{1}{P(S|N)}\right) + \\ &+ P(E|N) \cdot \log_2\left(\frac{1}{P(E|N)}\right) + P(W|N) \cdot \log_2\left(\frac{1}{P(W|N)}\right) \\ &= 0.5 \cdot \log_2\left(\frac{1}{0,5}\right) + 0.3 \cdot \log_2\left(\frac{1}{0.3}\right) + 0.2 \cdot \log_2\left(\frac{1}{0.2}\right) \\ &= 0.5 + 0.5211 + 0.4644 = 1.4855 \text{ [bits} \end{aligned}$$

d) El codi Huffman no preveu que la font tingui memòria:

N 1/4	A 1/2	A 1/2	N 01
S 1/4	N 1/4	B 1/2	S 00
E 1/4	S 1/4		E 11
W 1/4			W 10

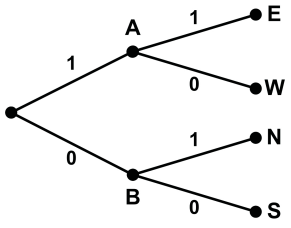


Fig. 1.7: Codificació binària de Huffman

Problema 5

Una font binària amb memòria 1 envia, de forma periòdica, símbols a un codificador de font cada T_F.

El codificador aplica una extensió de font concatenant aquests símbols de dos en dos, de manera que treballa amb un alfabet $\{X, \overline{X}, Y, \overline{Y}\}$. El comportament de la font estesa es pot modelar mitjançant la cadena de Markov:

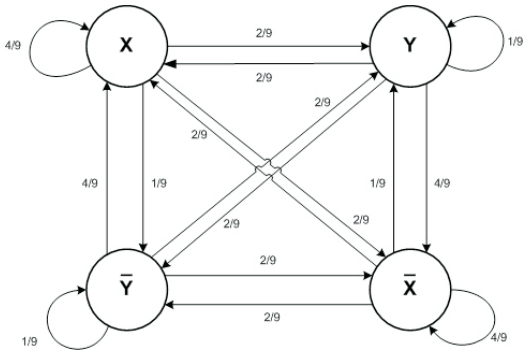


Fig. 1.8: Cadena de Markov de la font estesa

a) Per al règim estacionari, Calculeu la probabilitat que la font estesa generi cadascun dels símbols. Tingueu en compte les simetries de la cadena de Markov per al càlcul.

b) Determineu l'entropia de la font estesa en bits, H(Fe).

c) Suposant que la codificació de la font estesa obté una longitud mitjana d'1,88 dígits binaris per símbol, trobeu el valor mínim de T_F per a un canal de 64 Kbps.

d) Tenint en compte que la font binària es pot modelar amb la cadena de Markov:

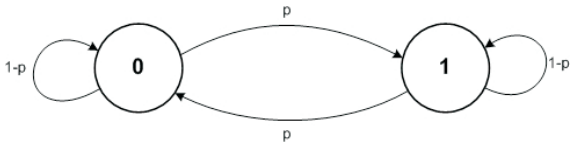


Fig. 1.9: Cadena de Markov de la font binària

Identifiqueu el valor de p a partir del model de font estesa i l'associació entre els valors de l'alfabet de la font estesa i els parells de símbols binaris (tingueu en compte que els valors $X - \bar{X}$ i $Y - \bar{Y}$ són complementaris entre si).

e) Per a un valor de $p = 1/3$, trobeu la relació entre entropies de la font estesa i la font binària. Discutiu els valors obtinguts respecte al cas sense memòria.

Solució

a) S'observa que $P(X) = P(\overline{X})$, $P(Y) = P(\overline{Y})$

S'ha de complir $P(X) + P(\overline{X}) + P(Y) + P(\overline{Y}) = 1$

i d'aquí es deriva que $P(X) + P(Y) = 1/2$

Per tant, falta una equació, que es deriva de la cadena de Markov. Per exemple, per a l'estat X, es verifica en règim estacionari que

$$P(X) \cdot \left[\frac{2}{9} + \frac{2}{9} + \frac{1}{9}\right] = P(Y) \cdot \frac{2}{9} + P(\overline{Y}) \cdot \frac{4}{9} + P(\overline{X}) \cdot \frac{2}{9}$$

Simplificant:

$$5P(X) = 2P(Y) + 4P(\overline{Y}) + 2P(\overline{X}) \quad \Rightarrow \quad P(X) = 2P(Y)$$

Resolent:

$$P(X) = \frac{1}{3}, \quad P(\overline{X}) = \frac{1}{3}, \quad P(Y) = \frac{1}{6}, \quad P(\overline{Y}) = \frac{1}{6}$$

b) $H(F_e) = P(X) \cdot H(F_e|X) + P(\overline{X}) \cdot H(F_e|\overline{X}) + P(Y) \cdot H(F_e|Y) + P(\overline{Y})H(F_e|\overline{Y})$

$$H(F_e|X) = P_{X/X} \log_2 \frac{1}{P_{X/X}} + P_{\overline{X}/X} \log_2 \frac{1}{P_{\overline{X}/X}} + P_{Y/X} \log_2 \frac{1}{P_{Y/X}} + P_{\overline{Y}/X} \log_2 \frac{1}{P_{\overline{Y}/X}}$$

$$H(F_e|X) = \frac{4}{9}\log_2 \frac{9}{4} + \frac{2}{9}\log_2 \frac{9}{2} + \frac{2}{9}\log_2 \frac{9}{2} + \frac{1}{9}\log_2 9$$

$$H(F_e|X) = \frac{4}{9}\log_2 \frac{9}{4} + \frac{4}{9}\log_2 \frac{9}{2} + \frac{1}{9}\log_2 9$$

$$H(F_e|X) = \frac{4}{9}(\log_2 9 - 2) + \frac{4}{9}(\log_2 9 - 1) + \frac{1}{9}\log_2 9$$

$$H(F_e|X) = \log_2 9 - \frac{12}{9} = 2\log_2 3 - \frac{4}{3} = 1{,}83 \text{ bits } F_e$$

Atès que tots els estats tenen el mateix conjunt de probabilitats de transició,

$$H(F_e|X) = H(F_e|\overline{X}) = H(F_e|Y) = H(F_e|\overline{Y})$$

de manera que:

$$H(F) = H(F_e|X) = 2\log_2 3 - \frac{4}{3} = 1{,}83 \text{ bits } F_e$$

c) $L_{F_e} = 1{,}88$ dig bin/sim F_e

La velocitat màxima de la font estesa serà:

$$\upsilon_{F_e} = \frac{C}{L_{F_e}} = \frac{64.000}{1.88} = 34042{,}55 \text{ sim } F_e/\text{s}$$

La velocitat màxima de la font serà:

$\upsilon_F = 2 \cdot \upsilon_{F_e} = 68.085{,}10$ sim F/s

$T_F = \frac{1}{\upsilon_F} = 1.468 \cdot 10^{-5} = 14.68\ \mu$s (temps mitjà mínim entre símbols)

d) L'alfabet estès serà $\{00, 01, 10, 11\}$.

La font estesa es troba a l'estat 00 quan les dues últimes generacions de la font elemental han estat 0. Això implica que, quan es fa una transició des de l'estat 00 de la font estesa, la font elemental es troba a l'estat 0 i fa dues noves generacions. Per a aquest cas, les quatre possibilitats són:

I) $X = 00 \longrightarrow X = 00$: succeeix quan la font elemental des de l'estat 00 fa dues generacions de 0, amb una probabilitat $(1-p)^2$.

II) $X = 00 \longrightarrow X = 01$: succeeix quan la font elemental des de l'estat 0 genera un altre 0 i després un 1, amb una probabilitat $(1-p)\,p$.

III) $X = 00 \longrightarrow X = 10$: succeeix quan la font elemental des de l'estat 0 genera un 1 i després torna a generar un altre 0, amb una probabilitat p^2.

IV) $X = 00 \longrightarrow X = 11$: succeeix quan la font elemental des de l'estat 0 genera dos 1 repetidament, amb una probabilitat $p\,(1-p)$.

Gràficament, es representen les transicions des de l'estat 00.

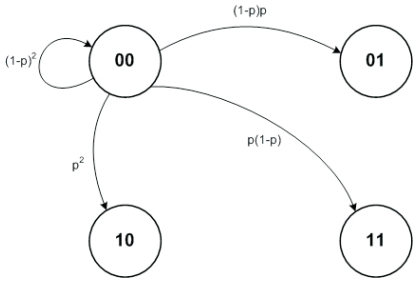


Fig. 1.10: Diagrama de transició d'estats

Ateses les simetries del model de la font estesa, hi podem identificar dues solucions distintes:

$$\text{I)}\ X = 00,\ \overline{X} = 11,\ Y = 10,\ \overline{Y} = 01 \quad \Rightarrow \quad \begin{cases} p(1-p) = \dfrac{2}{9} \\ p^2 = \dfrac{1}{9} \end{cases} \quad \Rightarrow \quad p = 1/3$$

$$\text{II)}\ X = 01,\ \overline{X} = 10,\ Y = 00,\ \overline{Y} = 11 \quad \Rightarrow \quad \begin{cases} p(1-p) = \dfrac{2}{9} \\ p^2 = \dfrac{4}{9} \end{cases} \quad \Rightarrow \quad p = 2/3$$

e) $p = 1/3$

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

$$P(0) = P(1) = 1/2 \text{ per simetria}$$

$$H(F|0) = H(p) = \frac{1}{3}\log_2 3 + \frac{2}{3}\log_2 \frac{3}{2}$$

$$H(F|0) = \frac{1}{3}\log_2 3 + \frac{2}{3}\log_2 3 - \frac{2}{3}\log_2 2$$

$$H(F|0) = \log_2 3 - \frac{2}{3}$$

La probabilitat de transició és la mateixa per a l'estat 1, de manera que

$$SH(F) = H(F|0) = \log_2 3 - \frac{2}{3} = 0{,}9183 \text{ bits } F$$

La solució serà:

$$\frac{H(F_e)}{H(F)} = \frac{2\log_2 3 - \dfrac{4}{3}}{\log_2 3 - \dfrac{2}{3}} = 2 \text{ (concatenació de 2 símbols)}$$

Si F no tingués memòria, $p = 1/2$, la font estesa seria linealment de símbols independents de F, de manera que l'entropia creix linealment amb el nombre de símbols concatenats. Així:

$$H(F_e) = 2H(F)$$

Per tant, es manté la mateixa relació, com es podia esperar, atès que la font estesa no afegeix cap desordre.

Problema 6

Es vol fer la compressió d'un fitxer que té aquest contingut:

A B D B D A D C A C C A D C B B

Suposant que s'ha fixat a priori per a cada símbol de la font l'associació binària següent de dos bits:

$$\{A = '00',\ B = '01',\ C = '10',\ D = '11'\}$$

a) Indiqueu quina és la longitud mínima en bits del resultat de la compressió del fitxer.

b) Expresseu en hexadecimal el resultat de la compressió del fitxer quan:

I) Es fa servir l'algoritme LZ-77 amb una memòria d'emmagatzematge de 8 posicios (3 bits de direccionament).
II) Es fa servir l'algoritme LZ-78 amb un diccionari de 64 posicions (longitud final igual a 6 bits de direccionament).
III) Es fa servir l'algoritme LZW amb un diccionari de 256 posicions (8 bits de direccionament).

Solució

a) Hi ha 16 símbols de font al fitxer. Si suposem que són equiprobables, necessitaríem $16 \cdot 2$ bits $= 32$ bits. Al fitxer, apareixen els símbols amb probabilitat 1/4, de manera que són equiprobables. Llavors, de la mateixa manera, amb l'estadística del fitxer, necessitaríem almenys 32 bits.

b) I) LZ-77 $\rightarrow$ (Pos, Long, Caràc)

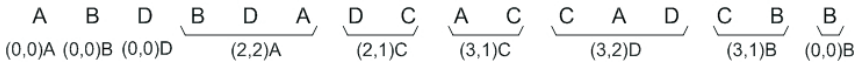


Fig. 1.11: Diagrama de transició d'estats

		Pos	Long	Car		
(0, 0) A	$\longrightarrow$	000	000	00	$\longrightarrow$	00h
(0, 0) B	$\longrightarrow$	000	000	01	$\longrightarrow$	01h
(0, 0) D	$\longrightarrow$	000	000	11	$\longrightarrow$	03h
(2, 2) A	$\longrightarrow$	010	010	00	$\longrightarrow$	48h
(2, 1) C	$\longrightarrow$	010	001	10	$\longrightarrow$	46h
(3, 1) C	$\longrightarrow$	011	001	10	$\longrightarrow$	66h
(3, 2) D	$\longrightarrow$	011	010	11	$\longrightarrow$	6Bh
(3, 1) B	$\longrightarrow$	011	001	01	$\longrightarrow$	65h
(0, 0) B	$\longrightarrow$	000	000	01	$\longrightarrow$	01h

II) LZ78 → (Pos, Caràc)

A	B	D	B D	A D	C	A C	C A	D C	B B
(0,A)	(0,B)	(0,D)	(2,D)	(1,D)	(0,C)	(1,C)	(6,A)	(3,C)	(2,B)

posició	caràcter
000001	A
000010	B
000011	D
000100	BD
000101	AD
000110	C
000111	AC
001000	CA
001001	DC
001010	BB

(0, A)	⟶	00000000	⟶	00h
(0, B)	⟶	00000001	⟶	01h
(0, D)	⟶	00000011	⟶	03h
(2, D)	⟶	00001011	⟶	0Bh
(1, D)	⟶	00000111	⟶	07h
(0, C)	⟶	00000010	⟶	02h
(1, C)	⟶	00000110	⟶	06h
(6, A)	⟶	00011000	⟶	18h
(3, C)	⟶	00001110	⟶	DEh
(2, B)	⟶	00001001	⟶	09h

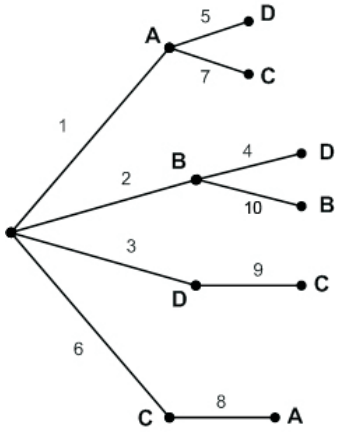


Fig. 1.12: Codificació LZ78

III) LZW

A	B	D	B D	A	D	C	A	C	C A	D C	B	B
0	1	3	5	0	3	2	0	2	10	9	1	1

diccionari			codificació		
0	⟶	A	0	⟶	00h
1	⟶	B	1	⟶	01h
2	⟶	C	3	⟶	03h
3	⟶	D	5	⟶	05h
4	⟶	AB	0	⟶	00h
5	⟶	BD	3	⟶	03h
6	⟶	DB	2	⟶	02h
7	⟶	BDA	0	⟶	00h
8	⟶	AD	2	⟶	02h
9	⟶	DC	10	⟶	0Ah
10	⟶	CA	9	⟶	09h
11	⟶	AC	1	⟶	01h
12	⟶	CC	1	⟶	01h
13	⟶	CAD			
14	⟶	DCB			
15	⟶	BB			

Problema 7

Sigui una font d'informació sense memòria l'alfabet de la qual és de 3 símbols $\{A, B, C\}$, amb $P(A) = 0.5 \qquad P(B) = P(C) = 0.25$

a) Calculeu el temps mínim necessari per transmetre 10.000 símbols de font a través d'un canal ($W = 3$ KHz) amb una relació senyal a soroll a l'entrada del receptor de $S/N = 7$ (en escala lineal).

b) Codifiqueu la seqüència *ABACAA* mitjançant un codificador de Huffman.

c) Codifiqueu la seqüència *ABACAA* mitjançant un codificador aritmètic.

d) Descodifiqueu la seqüència 0011426 mitjançant un codificador de LZW, amb un diccionari carregat inicialment amb *A* a la posició 0, *B* a la 1 i *C* a la 2.

e) Quina de les codificacions anteriors considereu més apropiada per a la font en qüestió. Raoneu la resposta.

Solució

a) En el cas millor (temps de transmissió mínim): *i*) No podrem transmetre per sobre de la capacitat de canal (C). *ii*) Cada símbol de font el podrem comprimir, de mitjana, fins al valor de l'entropia.

$$V_{t_{màx}} = C = W \log_2 \left(1 + \frac{S}{N}\right) = 9.000 \text{ bps} \qquad L_{\min} = 10.000 \cdot H = 15.000 \text{ bits}$$

$$H = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1{,}5 \text{ bits}$$

$$t_{\min} = \frac{L_{\min}}{V_{t_{màx}}} = \frac{15.000}{9.000} = \frac{5}{3} \text{s}$$

b) Codificació de Huffman de la seqüència *ABACAA*:

A	0,25	0,5	0
B	0,25	0,5	1
C	0,25		

De manera que $A \rightarrow 0, B \rightarrow 1\,0, C \rightarrow 1\,1$

I la seqüència $ABACAA \rightarrow 0\,1\,0\,0\,1\,1\,0\,0$

c) Codificació aritmètica de la seqüència:

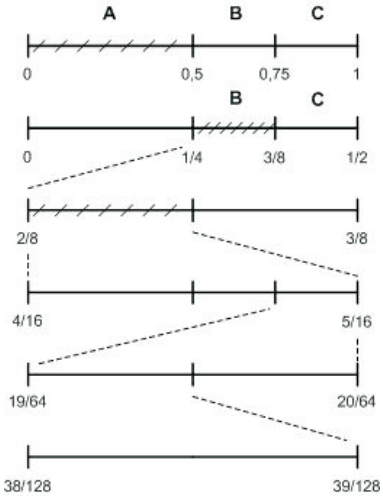


Fig. 1.13: Codificació aritmètica

La seqüència $ABACAA \in \left[\frac{38}{128}, \frac{39}{128}\right)$. Per tant, qualsevol punt dins d'aquest segment permet codificar aquesta seqüència d'entrada amb un únic valor.

d) RX: 0 0 1 1 4 2 6
sortida: *A A B B AB C BA*
AFEGIR DICC: — *AA AB BB BA ABC CB*

DIC:

0	*A*	3	*AA*	6	*BA*
1	*B*	4	*AB*	7	*ABC*
2	*C*	5	*BB*	8	*CB*

sortida: *AABBABCBA*

e) En aquest cas, a la codificació de Huffman, $\bar{l} = H$, de manera que és el més apropiat.

Problema 8

Un sistema de transmissió de dades fa servir un codificador de font i un xifrador de flux basat en un simple LFSR. La font F que fa servir el sistema no té memòria i emet símbols de l'alfabet $\{A, B\}$ amb unes probabilitats de generació $p_A = 0.9$ i $p_B = 0.1$. La transmissió es fa sobre un canal que té una capacitat de C bps. La codificació binària aplicada fa servir una extensió de font d'ordre 2 (concatenació de símbols de 2 en 2) i l'algorisme de Huffman. El xifrador de flux emet una seqüència xifrant K en què els valors 1 i 0 són equiprobables. El flux binari de sortida del codificador de font s'ha anomenat X i l'entregat al canal Y, resultat de $X \oplus K$.

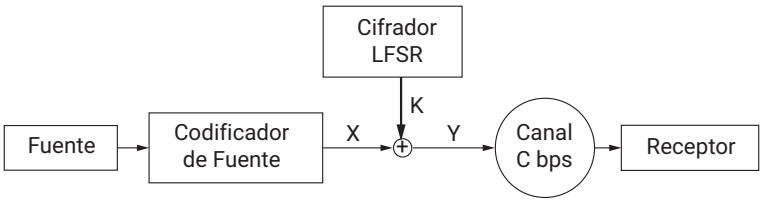


Fig. 1.14: Esquema de transmissió de dades amb un xifrador-aleatoritzador

a) Determineu l'entropia de la font $H(F)$.
b) Determineu l'entropia de la font estesa $H(F^2)$.
c) Trobeu la codificació de Huffman de la font estesa i calculeu-ne l'eficiència resultant E_{F^2}.
d) Per a un canal amb C = 64 Kbps, determineu la màxima velocitat d'emissió de símbols de la font estesa per segon (v_F) que accepta el sistema.
e) Calculeu $H(Y|X)$, $H(Y|K)$ y $H(X, Y)$.
f) Determineu el valor de la informació mútua $I(X; K)$.

Solució

a) Font $\{A, B\}$: $p_A = 0.9; p_B = 0.1$

$$H(F) = p_A \log \frac{1}{p_A} + p_B \log \frac{1}{p_{AB}} = 0{,}469 \text{ bits } F$$

b) Font estesa $F^2 = \{AA, AB, BA, BB\}$

$H(F^2) = 2 \cdot H(F) = 0{,}938$ bits estès F^2

c) Huffman de F^2

Ord. probabilitat	Font reduïda 1	Font reduïda 2
$AA \rightarrow 0.81$	$AA \rightarrow 0.81$	$AA \rightarrow 0.81$
$AB \rightarrow 0.09$	$C \rightarrow 0.1$	$D \rightarrow 0.19$
$BA \rightarrow 0.09$	$AB \rightarrow 0.09$	
$BB \rightarrow 0.01$		

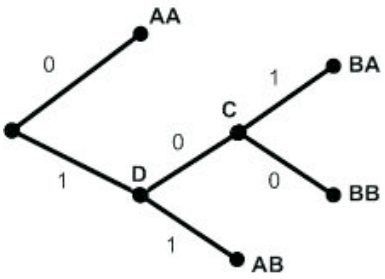


Fig. 1.15: Codificació binària de Huffman

Codificació: $AA \rightarrow 0$
$AB \rightarrow 1\ 1$
$BA \rightarrow 1\ 0\ 1$
$BB \rightarrow 1\ 0\ 0$

$$L_{F^2} = 0.81 \cdot 1 + 0.09 \cdot 2 + 0.09 \cdot 3 + 0.01 \cdot 3$$
$$= 1.29 \text{ dígits binaris/símbol estès } F^2$$

$$E_{F^2} = \frac{H(F^2)}{L_{F^2}} = \frac{0.938}{1.29} = 0.727$$

Observeu que l'eficiència ha augmentat notablement respecte de la codificació de la font F.

d) T_F = temps de símbol de font, $v_F = \dfrac{1}{T_F}$

$$\frac{L_{F^2}}{2 \cdot T_F} \leq C \quad \Longrightarrow \quad \frac{L_{F^2}}{2} \cdot v_F \leq C \quad \Longrightarrow \quad v_{F_{\text{màx}}} = \frac{2 \cdot C}{L_{F^2}} = 99.224{,}8 \text{ símbols de F/s}$$

Observeu que, si s'aplica directament la codificació de Huffman, la velocitat d'emissió de la font és igual a la capacitat del canal, per tant 64.000 símbols/s

e) Entropies, atès que X i K són independents:

I) $H(Y|X) = H(K) = 1$ bit/símbol binari X.

II) $H(Y|K) = H(X)$

Per trobar $H(X)$, es pot tenir en compte que el codificador de font no introdueix cap desordre i fa una transformació reversible. Per tant, s'ha de relacionar el nombre de símbols de X (dígits binaris) per símbol de F que fa la codificació. Aquesta relació queda expressada per la longitud mitjana de la codificació:

$L_{F^2} = 1{,}29$ dig bin/símbol $\quad F^2 = 1{,}29$ simb X/simb F^2

Considerant que el codificador fa una concatenació de 2 símbols de F:

$$\begin{aligned} H(X) &= H(F) \cdot \frac{\text{bits}}{\text{sim } F} \cdot \frac{2 \text{ sim } F}{1 \text{ sim } F^2} \cdot \frac{1 \text{ sim } F^2}{L_{F^2} \text{ sim } X} \\ &= 0.469 \cdot 2 \cdot \frac{1}{1.29} \cdot \frac{\text{bits}}{\text{sim } X} = 0{,}722 \text{ bits} \end{aligned}$$

S'observa que $H(X)$ no és més que l'eficiència de la codificació realitzada, és a dir, la mitjana d'informació transportada per dígit binari. Així:

$$H(X) = E_{F^2} = \lim_{n \to \infty} \frac{nH(F)}{\frac{1}{2} L_{F^2}} = \frac{2H(F)}{L_{F^2}}$$

III) $H(X;Y) = H(X) + H(Y|X) = H(X) + H(K)$

En les mateixes unitats, se suma:

$H(X,Y) = H(X) + H(K) = 0.72 + 1 = 1{,}72$ bits

f) Informació mútua

$I(X,K) = H(X) - H(X|K) = 0$ (independents)

Problema 9

Un sistema de transmissió de dades està compost per una font binària X i un canal binari amb esborraments, la sortida del qual anomenarem Y. La font emet el símbol 0 amb probabilitat α i el símbol 1 amb probabilitat 1-α. El canal es caracteritza per la matriu estocàstica:

$$Q = \begin{pmatrix} 1-\rho & \rho & 0 \\ 0 & \rho & 1-\rho \end{pmatrix}$$

on ρ és la probabilitat de rebre un esborrament (B) a la sortida del canal quan s'emet un símbol binari (0, 1).

a) Trobeu la relació entre $H(Y)$ i $H(X)$. Raoneu el resultat obtingut per als casos $\rho = 0$ i $\rho = 1$.
b) Calculeu $H(X|Y)$.
c) Determineu $H(Y|X)$.
d) Indiqueu quin és el valor de la informació mútua $I(X;Y)$.
e) Especifiqueu quin és el valor de la capacitat C del canal amb esborraments en bits per símbol.

Nota: Intenteu expressar els resultats utilitzant $H(\alpha)$ i $H(\rho)$.

Solució

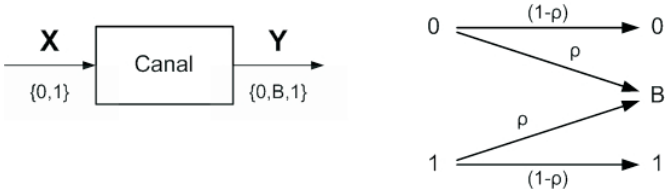


Fig. 1.16: Esquema de transmissió de dades sobre el canal amb esborrament

a) $H(X) = \alpha \cdot \log_2\left(\frac{1}{\alpha}\right) + (1-\alpha) \cdot \log_2\left(\frac{1}{1-\alpha}\right) = H(\alpha)$

$H(Y) = \sum_i P(Y=i) \cdot \log_2\left(\frac{1}{P(Y=i)}\right)$, on $i \in \{0, B, 1\}$

$P(Y=0) = (1-\rho) \cdot P(X=0) + 0 \cdot P(X=1) = (1-\rho) \cdot \alpha$

$P(Y=B) = \rho \cdot P(X=0) + \rho \cdot P(X=1) = \rho$

$P(Y=1) = 0 \cdot P(X=0) + (1-\rho) \cdot P(X=1) = (1-\rho) \cdot (1-\alpha)$

$$H(Y) = (1-\rho)\cdot\alpha\cdot\log_2\frac{1}{(1-\rho)\cdot\alpha} + \rho\cdot\log_2\frac{1}{\rho} + (1-\rho)\cdot(1-\alpha)\cdot\log_2\frac{1}{(1-\rho)\cdot(1-\alpha)}$$

$$\begin{aligned} H(Y) =& (1-\rho)\cdot\alpha\cdot\left[\log_2\frac{1}{1-\rho} + \log_2\frac{1}{\alpha}\right] + \rho\cdot\log_2\frac{1}{\rho} + (1-\rho)\cdot(1-\alpha)\cdot \\ & \cdot\left[\log_2\frac{1}{1-\rho} + \log_2\frac{1}{1-\alpha}\right] = \\ =& \alpha\cdot\left[(1-\rho)\log_2\frac{1}{1-\rho}\right] + (1-\rho)\cdot\left[\alpha\cdot\log_2\frac{1}{\alpha}\right] + \rho\cdot\log_2\frac{1}{\rho} + \\ & + (1-\alpha)\cdot\left[(1-\rho)\cdot\log_2\frac{1}{1-\rho}\right] + (1-\rho)\cdot\left[(1-\alpha)\cdot\log_2\frac{1}{1-\alpha}\right] \\ =& H(\rho) + (1-\rho)\cdot H(\alpha) \end{aligned}$$

$H(Y) = H(\rho) + (1-\rho)\cdot H(\alpha)$

Casos particulars:

Si $\rho = 0 \Longrightarrow H(Y) = H(\alpha) = H(X)$ canal sense errors

Si $\rho = 1 \Longrightarrow H(Y) = 0$, canal sense capacitat de transmissió, sempre es rep un esborrament

b) $H(X|Y) = \sum_i P(Y=i)\cdot\sum_j P(X=j|Y=i)\cdot\log_2\frac{1}{P(X=j|Y=i)}$,

on $i \in \{0, B, 1\}$, $j \in \{0, 1\}$

Calculem primer l'entropia condicional per un valor concret de la sortida Y:

$$H(X|Y=i) = \sum_j P(X=j|Y=i)\cdot\log_2\frac{1}{P(X=j|Y=i)}$$

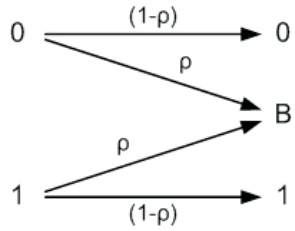


Fig. 1.17: Esquema de transmissió de dades

Per trobar l'entropia condicional de cada valor, es determinen les probabilitats de l'entrada per a un valor de la sortida:

$$\left.\begin{array}{l} P(X=0|Y=0)=1 \\ P(X=1|Y=0)=0 \end{array}\right\} \Longrightarrow H(X|Y=0)=0$$

$$\left.\begin{array}{l} P(X=0|Y=B)=\dfrac{p(\alpha)}{p(\alpha)+p(1-\alpha)}=\alpha \\ P(X=1|Y=B)=\dfrac{p(1-\alpha)}{p(\alpha)+p(1-\alpha)}=1-\alpha \end{array}\right\} \Longrightarrow H(X|Y=B)=H(\alpha)$$

$$\left.\begin{array}{l} P(X=0|Y=1)=0 \\ P(X=1|Y=1)=1 \end{array}\right\} \Longrightarrow H(X|Y=1)=0$$

Finalment, obtenim:

$$H(X|Y)=P(Y=B)\cdot H(\alpha)=\rho\cdot H(\alpha)$$

c) $H(Y|X)=\sum_j P(X=j)\cdot\sum_i P(Y=i|X=j)\cdot\log_2\dfrac{1}{P(Y=i|X=j)}$,

on $j\in\{0,\,1\}$, $i\in\{0,\,B,\,1\}$ Calculem l'entropia condicional de la sortida per a cada

possible valor d'entrada:

$$H(Y|X=j)=\sum_i P(Y=i|X=j)\cdot\log_2\frac{1}{P(I=i|X=j)}$$

$$\begin{aligned} H(Y|X=0) &= P(Y=0|X=0)\cdot\log_2\left(\frac{1}{P(Y=0|X=0)}\right)+ \\ &+ P(Y=B|X=0)\cdot\log_2\left(\frac{1}{P(Y=B|X=0)}\right) \end{aligned}$$

$$H(Y|X=0)=(1-\rho)\cdot\log_2\frac{1}{1-\rho}+\rho\cdot\log_2\frac{1}{1-\rho}=H(\rho)$$

$$H(Y|X=1)=H(\rho),\quad \text{per simetria}$$

Llavors,

$$H(Y|X)=\alpha\cdot H(\rho)+(1-\alpha)\cdot H(\rho)=H(\rho)$$

Com es podia esperar, l'entropia a la sortida quan es coneix l'entrada depèn només de la probabilitat d'esborrament del canal:

$$H(Y|X)=H(\rho)$$

d) La informació mútua es pot derivar a partir de les entropies condicionals que hem trobat abans:

$$I(X;Y) = H(X) - H(X|Y) = H(\alpha) - \rho \cdot H(\alpha) = (1-\rho) \cdot H(\alpha)$$

o també:

$$I(X;Y) = H(Y) - H(Y|X) = H(\rho) + (1-\rho) \cdot H(\alpha) - H(\rho)$$

$$I(X;Y) = (1-\rho) \cdot H(\alpha)$$

e) La capacitat del canal s'obté directament a través de la seva definició:

$$C = \text{màx}_{\alpha}(1-\rho) \cdot H(\alpha) = (1-\rho) \cdot H_{\text{màx}}$$

$$H_{\text{màx}} = 1, \text{ quan } \alpha = \frac{1}{2}$$

$$C = (1-\rho) \text{ bits}$$

Problema 10

Un sistema de transmissió de dades utilitza un regenerador de senyal. El regenerador té com a entrades (X) símbols que pertanyen a l'alfabet $\{1,\ 0,\ -1\}$. Les probabilitats de recepció dels símbols són:

$$P[X=1] = \alpha,\ P[X=0] = 1-\alpha-\beta,\ P[X=-1] = \beta$$

per a $0 < \alpha + \beta <= 1$.

El regenerador restitueix els valors dels esborraments ($X = 0$) en valors de sortida $Y = 1$ o $Y = -1$, amb la mateixa proporció amb què es generen, i manté el mateix valor ($Y = X$) quan les entrades són $X = 1$ o $X = -1$. Així, el sistema de transmissió de dades regenerador es pot caracteritzar a través de la matriu estocàstica de probabilitats de transició:

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 \\ \frac{\alpha}{\alpha+\beta} & \frac{\beta}{\alpha+\beta} \\ 0 & 1 \end{pmatrix} \quad 0 < \alpha + \beta \leq 1$$

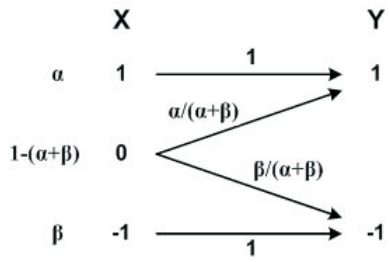


Fig. 1.18: Esquema de transmissió de dades del regenerador de símbols

a) Determineu $H(Y)$.
b) Calculeu $H(Y|X)$.
c) Trobeu $I(X;Y)$.
d) Calculeu la capacitat del sistema regenerador en bits per símbol per als casos:
I) $\alpha = \beta$
II) $\alpha = 2 \cdot \beta$

Solució

a) Determinem $H(Y)$:

$$P(Y=1) = \alpha + [1-(\alpha+\beta)] \cdot \frac{\alpha}{\alpha+\beta} = \alpha + \frac{\alpha}{\alpha+\beta} - \alpha = \frac{\alpha}{\alpha+\beta}$$

$$P(Y=-1) = 1 - P(Y=1) = \frac{\beta}{\alpha+\beta}$$

$$H(Y) = \frac{\alpha}{\alpha+\beta} \cdot \log_2 \frac{\alpha+\beta}{\alpha} + \frac{\beta}{\alpha+\beta} \cdot \log_2 \frac{\alpha+\beta}{\beta} \triangleq H\left(\frac{\alpha}{\alpha+\beta}\right)$$

b) Trobem $H(Y|X)$:

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

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

atès que els altres sumands són 0, ja que no hi ha incertesa quan $X=1$ o $X=-1$. Així:

$$H(Y|X) = [1-(\alpha+\beta)] \cdot H\left[\frac{\alpha}{\alpha+\beta}\right] = [1-(\alpha+\beta)] \cdot H(Y)$$

c) $I(X;Y) = H(Y) - H(Y|X) = H(Y) - [1-(\alpha+\beta)]H(Y) = (\alpha+\beta) \cdot H(Y)$

$$I(X;Y) = (\alpha+\beta) \cdot H\left(\frac{\alpha}{\alpha+\beta}\right) = (\alpha+\beta) \cdot \left[\frac{\alpha}{\alpha+\beta} \cdot \log_2 \frac{\alpha+\beta}{\alpha} + \frac{\beta}{\alpha+\beta} \cdot \log_2 \frac{\alpha+\beta}{\beta}\right]$$

d) Ara $\alpha = \beta$

$$I(X;Y) = 2 \cdot \alpha \cdot \left[\frac{1}{2} \cdot \log_2 2 + \frac{1}{2} \cdot \log_2 2\right] = 2 \cdot \alpha, \qquad \alpha + \beta \leq 1 \Rightarrow \alpha \leq 1/2$$

$$C = \text{màx}_\alpha \, I(X;Y), \text{ amb } 0 < \alpha \leq \frac{1}{2}$$

$$C = I(X;Y)|_{\alpha = \frac{1}{2}} = 1 \text{ bit}$$

En aquest cas, el repetidor mai no rep esborraments.

Per a $\alpha = 2{\cdot}\beta$, no es reben esborraments si $1{-}\alpha{-}\beta = 0$, de manera que $1 - 3 \cdot \beta = 0 \Rightarrow \beta = \frac{1}{3}$ y $\alpha = \frac{2}{3}$

$$I(X;Y)|_{\alpha=2\cdot\beta} = \beta \cdot [3 \cdot \log_2 3 - 2] \Rightarrow C = \frac{1}{3}[3 \cdot \log_2 3 - 2] = 0{,}91 \text{ bits}$$

Problema 11

Es vol analitzar el comportament de n canals binaris simètrics (BSC), amb una probabilitat d'error p, connectats en sèrie, com es mostra a la figura 1.19.

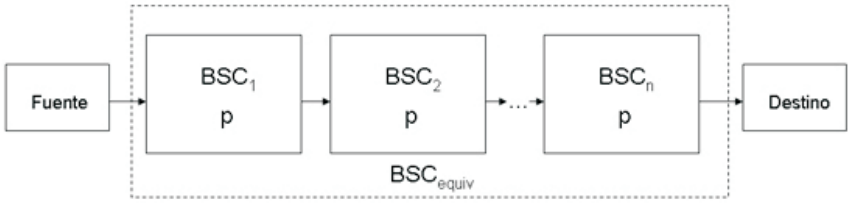


Fig. 1.19: Canals binaris simètrics en sèrie

Responeu les preguntes següents:

a) Per al cas de dos canals BSC en cascada ($n = 2$), determineu la matriu estocàstica de probabilitats del canal BSC equivalent.

b) Determineu la probabilitat d'error del BSC equivalent, p_{equiv}, quan $n = 2$. Trobeu la capacitat del canal BSC equivalent per a aquest cas, $n = 2$.

c) Per al cas general, en què $p \ll 1/n$, obtingui un valor aproximat de p_{equiv} que depengui només de n y p. Per a aquest cas, especifiqueu una expressió simple de la capacitat del canal BSC equivalent.

Solució

a) $n = 2$

$$Q_{BSC_1} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \triangleq Q_{n=1}$$

En cascada:

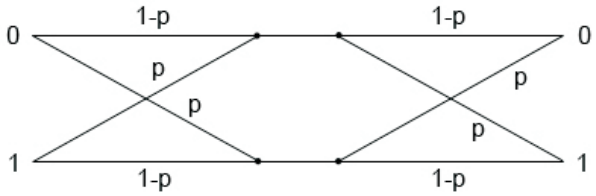


Fig. 1.20: Esquema de transició de dades per a dos canals BSC

$$p(s=0|e=0) = (1-p)^2 + p^2$$
$$p(s=1|e=0) = p(1-p) + (1-p)p = 2p(1-p)$$
$$p(s=1|e=1) = (1-p)^2 + p^2$$
$$p(s=0|e=1) = p(1-p) + (1-p)p = 2p(1-p)$$

$$Q_{n=2} = \begin{bmatrix} (1-p)^2 + p^2 & 2p(1-p) \\ 2p(1-p) & (1-p)^2 + p^2 \end{bmatrix} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \cdot \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

S'observa que $Q_{n=2} = Q_{n=1}^2$

En general, $\boxed{Q_n = Q_n^n = 1}$

b) $n = 2$

$$Q_{\text{equiv}} = \begin{bmatrix} 1-p_{\text{equiv}} & p_{\text{equiv}} \\ p_{\text{equiv}} & 1-p_{\text{equiv}} \end{bmatrix} = \begin{bmatrix} (1-p)^2 + p^2 & 2p(1-p) \\ 2p(1-p) & (1-p)^2 + p^2 \end{bmatrix}$$

Identificant $p_{\text{equiv}} = 2p(1-p) = 2p - 2p^2$.

La capacitat per al BSC és $C = 1 - H(p)$.

Per al $\text{BSC}_{\text{equiv}}$ serà $C = 1 - H(p_{\text{equiv}}) = 1 - H(2p - 2p^2)$.

c) Si $p \ll 1/n < 1$, llavors $p^i \ll p$, amb $i = 2,\ 3,\ 4,\ \ldots$

Considerant que es produeix un error en la recepció quan hi ha un nombre senar d'errors als n canals, podem trobar l'expressió general. Així:

$$p_i \triangleq prob[i \text{ errors en } n \text{ canals}] = \binom{n}{i} p \frac{1}{2} (1-p)^{n-1}$$

$$p_{\text{equiv}} = p_1 + p_3 + p_5 + \cdots + p_{2k-1} \quad k = \left\lfloor \frac{n+1}{2} \right\rfloor$$

$$p_{\text{equiv}} = \sum_{k=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor} p_{2k-1} = \sum_{k=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor} \binom{n}{2k-1} p^{2k-1} (1-p)^{n-2k+1}$$

Aproximant amb $p \gg p^3 \gg p^5 \ldots$ $p_{\text{equiv}} \simeq n\, p\, (1-p)^{n-1}$

Considerant que $1 - p \simeq 1$, llavors $p_{\text{equiv}} \simeq n\, p$ y $C = 1 - H(np)$

Problema 12

Considereu tres canals discrets amb els següents diagrames de transicions:

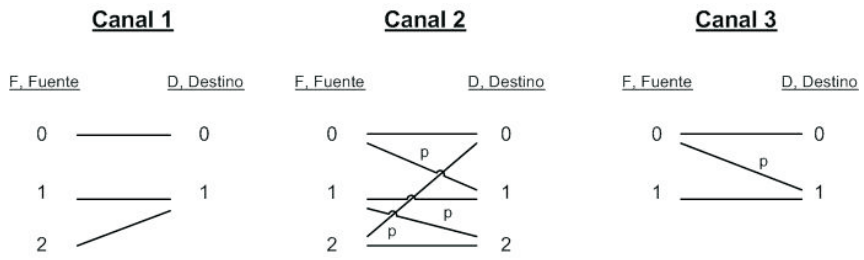


Fig. 1.21: Diagrames de transició

a) Calculeu la capacitat de canal per a cada canal. Expresseu-la en funció de p per als canals 2 i 3.

b) Calculeu les tres capacitats de canal anteriors per a $p = 1/2$. Amb quin canal es pot transmetre més informació per cada ús que se'n faci?

Nota: Perquè la solució sigui més clara, anomeneu

$$H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p}$$

Solució

a) Trobem les matrius de probabilitat de transició $p(D|F)$ per a cada canal, com es mostra a la Taula 1.4:

Canal 1	Canal 2	Canal 3
$P(D\|F) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$	$P(D\|F) = \begin{pmatrix} 1-p & p & 0 \\ 0 & 1-p & p \\ p & 0 & 1-p \end{pmatrix}$	$P(D\|F) = \begin{pmatrix} 1-p & p \\ 0 & 1 \end{pmatrix}$
Canal simètric respecto a la entrada	Canal simètric	

Taula 1.4: Matrius de probabilitats de transició

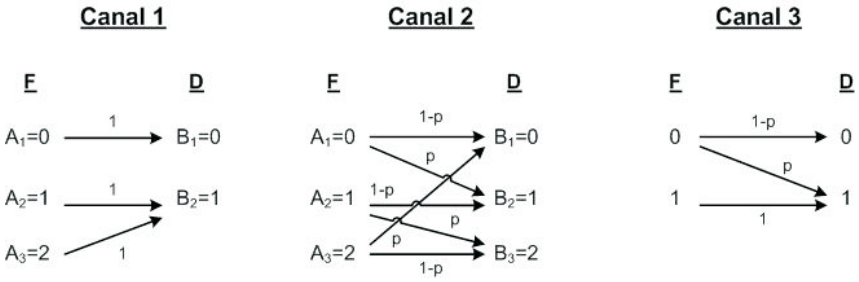


Fig. 1.22: Diagrames de transició

b) Calculem la informació mútua de la font a l'entrada respecte de la sortida del canal. Aquesta informació mútua o transmissió d'informació és la disminució de l'entropia a l'entrada del canal si en coneixem la sortida. També és la disminució de l'entropia a la sortida del canal si en coneixem l'entrada.

$$I(F;D) = H(F) - H(F|D) = H(D) - H(D|F) \text{ [bits]}$$

La capacitat de canal es defineix com la màxima transmissió d'informació, de manera que

$$C = \text{m x}_{p\{A_i\}} I(F;D) = \text{m x}_{p\{A_i\}} [H(D) - H(D|F)] \text{ [bits]}$$

on $p\{A_i\}$ és el conjunt de probabilitats dels símbols emesos per la font F.

Canal 1

$$H(D|F) = \sum_i p(A_i) \cdot H(D|A_i) = \{\overbrace{H(D|A_1) = H(D|A_2) = H(D|A_3) 1 \cdot \log_2 1 = 0}^{\text{Canal determinista} \Rightarrow H(D|F)=0}\}$$

$$= 0 = H(D|A_1)$$

Es tracta d'un canal determinista, en el qual, coneguda l'entrada, la sortida queda determinada:

$$H(D|F) = 0$$

$$H(D) = \sum_j P(B_j) \cdot \log_2 \frac{1}{P(B_j)}$$

Per tant, per trobar la capacitat de canal cal maximitzar l'entropia a la sortida, en funció de l'estadística de la font d'entrada.

$$C = \mathrm{m\,x}_{p\{A_i\}}[H(D) - H(D|F)] = \mathrm{m\,x}_{p\{A_i\}} H(D)$$

$$p(B = 0|A = 1) = P(B = 0|A = 2) = 0$$

$$p(B = 0|A = 0) = 1$$

$$p(B = 0) = p(B = 0|A = 0) \cdot p(A = 0) + p(B = 0|A = 1) \cdot p(A = 1) + \\ + p(B = 0|A = 2) \cdot p(A = 2) = p(A = 0)$$

$$p(B = 1|A = 0) = 0$$

$$p(B = 1|A = 1) = p(B = 1|A = 2) = 1$$

$$p(B = 1) = p(B = 1|A = 0) \cdot p(A = 0) + p(B = 1|A = 1) \cdot p(A = 1) + \\ + p(B = 1|A = 2) \cdot p(A = 2) = p(A = 1) + p(A = 2)$$

$$C = \mathrm{m\,x}_{p\{A_i\}}[H(D) - H(D|F)] = \mathrm{m\,x}_{p\{A_i\}} H(D)$$

Per fer màxima la informació mútua $I(F;D)$, hem de maximitzar la $H(D)$. Podem provar si hi ha una F, amb $p(A_i)$ coherents, tal que la font sigui equiprobable: $p(B = 0) = p(B = 1)$.

$$\left\{ \begin{array}{c} p(B = 0) = p(B = 1) = p(A = 0) = p(A = 1) + p(A = 2) \\ p(B = 0) + p(B = 1) = 1 \end{array} \right\} \Rightarrow$$

$$\Rightarrow p(B = 0) = p(B = 1) = p(A = 0) = 1/2, \quad p(A = 1) + p(A = 2) = 1/2$$

Serà per a una F tal que $p\{A_i\}$ tinguin els valors anteriors. Per tant, si que hi ha una F tal que $H(D)$ arriba al valor màxim possible. En cas contrari, s'hauria de maximitzar l'expressió resultant.

Llavors, $H(D) = 2 \cdot \frac{1}{2} \log_2 2 = 1$ bit/símbol

$C = 1$ bit

Canal 2

$$H(D|F) = \sum_i p(A_i) \cdot H(D|A_i)$$

$$H(D|A_1) = H(D|A_2) = H(D|A_3) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} = H(p)$$

de manera que

$$H(D|F) = \sum_i p(A_i) \cdot H(D|A_i) = H(p) \cdot \sum_i P(A_i) = H(p)$$

$$H(D) = \sum_j p(B_j) \cdot \log_2 \frac{1}{p(B_j)}$$

$$\begin{cases} p(B=0) = p(A=0) \cdot (1-p) + p(A=2) \cdot p \\ p(B=1) = p(A=0) \cdot p + p(A=1) \cdot (1-p) \\ p(B=2) = p(A=2) \cdot (1-p) + p(A=1) \cdot p \end{cases}$$

$$C = \mathrm{m\,x} I(F;D) = \mathrm{m\,x}_{p\{A_i\}}[H(D) - H(D|F)] = \mathrm{m\,x}_{p\{A_i\}} H(D) - H(p)$$

on veiem que $H(p)$ és constant i independent de $P\{A_i\}$.

Per obtenir C, hem de fer $H(D)$ màxima $\Rightarrow$ Podem provar si hi ha una F, $p(A_i)$ tal que faci que D sigui equiprobable, $p\{B_j\} = 1/3\ \forall j$:

$\exists\ F,\ p\{A_i\} \mid p\{B_j\} = 1/3$?

Si, per a $p\{A_i\} = \frac{1}{3}, \forall i \ \Rightarrow\ P\{B_j\} = \frac{1}{3}\ \forall j$, tal com veiem a les equacions $p(B=0)$, $p(B=1)$ y $p(B=2)$.

Llavors, $H(D) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = \log_2 3 = 1{,}5849$ bits

$C = (1.5849 - H(p))$ [bits/símbol]

Canal 3

$$H(D|F) = \sum_i p(A_i) \cdot H(D|A_i) = p(A=0) \cdot H(D|A=0) + p(A=1) \cdot H(D|A=1)$$

$$H(D|A=0) = \sum_j p(B_j|A=0) \cdot \log_2 \frac{1}{p(B_j|A=0)} = (1-p) \cdot \log_2 \frac{1}{1-p} +$$

$$+ \quad p \cdot \log_2 \frac{1}{p} = H(p)$$

$$H(D|A=1) = \sum_j p(B_j|A=1) \cdot \log_2 \frac{1}{p(B_j|A=1)} = 0 + 1 \cdot \log_2 1 = 0$$

$$H(D|F) = p(A=0) \cdot H(p) + p(A=1) \cdot 0 = p(A=0) \cdot H(p)$$

Veiem que $H(D|F)$ no és constant, ja que depèn de $p(A=0)$, és a dir, de l'estadística de la font F.

$$\begin{aligned} H(D) &= \sum_j p(B_j) \cdot \log_2 \frac{1}{p(B_j)} \\ &= \{p(B=0) = (1-p) \cdot p(A=0),\ p(B=1) = p \cdot p(A=0) + p(A=1)\} \\ &= (1-p) \cdot p(A=0) \cdot \log_2 \frac{1}{(1-p) \cdot p(A=0)} + \\ &+ (p \cdot p(A=0) + p(A=1)) \cdot \log_2 \frac{1}{p \cdot p(A=0) + p(A=1)} \end{aligned}$$

$$\begin{aligned} C &= \mathrm{m\,x}_{p\{A_i\}}[H(D) - H(D|F)] = \{\text{sigui } z = p(A=0)\} \\ &= \mathrm{m\,x}_{p\{A_i\}}[(1-p) \cdot z \cdot \log_2 \frac{1}{(1-p) \cdot z} + (p \cdot z + (1-z)) \cdot \\ &\cdot \log_2 \frac{1}{p \cdot z + (1-z)} - z \cdot H(p)] \Longrightarrow C(z) \end{aligned}$$

Per a què $p\{A_i\}$ la $I(F;D)$ es fa màxima? Hem de maximitzar $C(z)$ i aquest valor màxim ens donarà C:

$$C(z) = (1-p) \cdot z \cdot \log_2 \frac{1}{(1-p) \cdot z} + (z \cdot p + 1 - z) \cdot \log_2 \frac{1}{(z \cdot p + 1 - z)} - z \cdot H(p)$$

(Vegeu la **nota 2**)

$$\begin{aligned}
\text{C'(z)} &= (1-p)\cdot\log_2\frac{1}{(1-p)z}+\frac{(1-p)^2\cdot z^2}{\ln 2}\cdot\left(\frac{-1\cdot(1-p)}{(1-p)^2z^2}\right)+(p-1)\cdot\\
&\cdot\ \log_2\frac{1}{zp+1-z}+\frac{(zp+1-z)^2}{\ln 2}\cdot\left(\frac{-p+1}{(zp+1-z)^2}\right)-H(p)\\
&= (1-p)\log_2\frac{1}{(1-p)\cdot z}-\frac{1-p}{\ln 2}+(p-1)\cdot\log_2\frac{1}{zp+1-z}+\frac{1-p}{\ln 2}-H(p)\\
&= (1-p)\cdot\left[\log_2\frac{1}{(1-p)\cdot z}-\log_2\frac{1}{1-(1-p)\cdot z}\right]-H(p)\\
&= (1-p)\log_2\frac{1-(1-p)\cdot z}{(1-p)\cdot z}-H(p)
\end{aligned}$$

$$C'(z)=0\longrightarrow\log_2\frac{1-(1-p)\cdot z}{(1-p)\cdot z}=\frac{H(p)}{1-p}\longrightarrow 2^{\frac{H(p)}{1-p}}=\frac{1-(1-p)\cdot z}{(1-p)\cdot z}$$

$$2^{\frac{H(p)}{1-p}}\cdot(1-p)\cdot z=1-(1-p)\cdot z$$

$$\left(2^{\frac{H(p)}{1-p}}+1\right)\cdot(1-p)\cdot z=1$$

$$z_{\text{màx}}=\frac{1}{(1-p)\cdot\left(2^{\frac{H(p)}{1-p}}+1\right)}=p(A=0)$$

(Vegeu la **nota 1**)

Ja hem trobat la font F, amb una distribució de probabilitats $p\{A_i\}$ que maximitza $I(F;D)$:

$p(A=0)=z_{\text{màx}}(p)$

$p(A=1)=1-z_{\text{màx}}(p)$ Així, la capacitat de canal, $C(Z=Z_{\text{m x}})$ té aquesta expressió,

que depèn del paràmetre p.

$$\begin{aligned}
C(p) &= (1-p)\cdot z_{\text{màx}}\cdot\log_2\frac{1}{(1-p)z_{\text{màx}}}+(p\cdot z_{\text{màx}}+(1-z_{\text{màx}}))\cdot\\
&\cdot\ \log_2\frac{1}{p\cdot z_{\text{màx}}+(1-z_{\text{màx}})}-z_{\text{màx}}\cdot H(p)\ [\text{bits}]
\end{aligned}$$

c) $p=1/2$

Canal $1 \rightarrow C_1 = 1$ bit

Canal $2 \rightarrow C_2 = 1.5849 - H(\,p = 1/2) = 0{,}5849$ bits

Canal $3 \rightarrow H(\,p = 1/2) = \frac{1}{2}(\log_2 2) \cdot 2 = 1$

$$z_{\text{màx}} = p(A = 0) = \frac{1}{\frac{1}{2}(2^{\frac{1}{1/2}} + 1)} = \frac{2}{5} = 0.4;\ \ p(A = 1) = 0.6$$

$$p(B = 0) = \frac{1}{2} \cdot 0.4 = 0.2$$

$$p(B = 1) = \frac{1}{2} \cdot 0.4 + 0.6 = 0.8$$

$$\begin{aligned} C_3 &= \frac{1}{2} \cdot 0.4 \cdot \log_2 \frac{2}{0.4} + \left(\frac{1}{2} \cdot 0.4 + 0.6\right) \cdot \log_2 \frac{1}{0.8} - 0.4 \\ &= 0.2 \cdot \log_2 5 + 0.8 \cdot \log_2 1.25 - 0.4 = 0{,}3219 \text{ bits} \end{aligned}$$

Amb el canal 1, podem transmetre més quantitat d'informació per cada ús que se'n faci.

Nota 1: Essent estrictes, mancaria comprovar que $z_{\text{màx}}$ ofereix un màxim a $F(z)$:

$F''(z_{\text{màx}} < 0)$

Una altra manera de veure-ho és si $F(z) < C$ per a un $z < z_{\text{màx}}$ i un $z > z_{\text{màx}}$, i que només $F(z_{\text{màx}}) = C$.

Com que $(z_{\text{màx}} = 0.6)$, $F(0.3) = 0.3008 < C = 0.3219$

De la mateixa manera, $F(0.5) = 0.3115 < C = 0.3219$

Nota 2

$$\log_a x = \frac{\ln x}{\ln a}, \quad (\ln x)' = \frac{1}{x}, \quad (\log_a x)' = \left(\frac{\ln x}{\ln a}\right)' = \frac{1}{\ln a} \cdot \frac{1}{x}$$

Problema 13

Una font emet dos símbols (A, B) i queda completament caracteritzada per les següents probabilitats d'emissió condicionades:

$p(A|A) = 0.6$
$p(A|B) = 0.3$

Aquesta font travessa un canal binari simètric, **C**, amb un índex d'error de $p = 0.2$.

Es demana:

a) Quina és l'entropia de la font?

b) Quina és l'entropia a la sortida del canal? Comenteu-ne el resultat. Es decideix utilitzar tres canals idèntics a C en paral·lel, d'acord amb l'esquema:

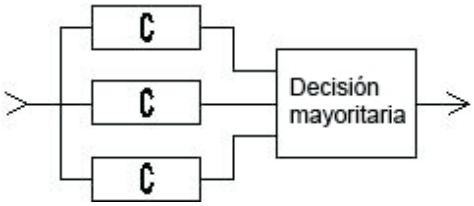


Fig. 1.23: Disposició dels canals

c) Quina és la capacitat del nou canal mostrat a la Fig. 1.23?

d) Quina és l'entropia a la sortida del nou canal? Comenteu-ne el resultat.

Solució

a) Primer, es calculen les entropies condicionades:

$$H(X|A) = 0.6 \log_2 \frac{1}{0.6} + 0.4 \log_2 \frac{1}{0,4} = 0{,}971 \text{ bits}$$

$$H(X|B) = 0.7 \log_2 \frac{1}{0.7} + 0.3 \log_2 \frac{1}{0.3} = 0{,}881 \text{ bits}$$

A continuació, es calcula la probabilitat de cada estat de font:

$$P(A) = P(A|A)P(A) + P(A|B)P(B)$$

$$P(A) + P(B) = 1$$

$$P(A) = P(A)0.6 + 0.3(1 - P(A)) \Rightarrow P(A) = 0.429,\ P(B) = 0.571$$

Finalment, es combinen les entropies condicionades per tal d'obtenir-ne el total:

$$H = H(X|A)P(A) + H(X|B)P(B) = 0.971 \cdot 0.429 + 0.881 \cdot 0.571 = 0{,}92 \text{ bits/simb}$$

b) L'entropia a la sortida s'obtindrà combinant les entropies condicionades:

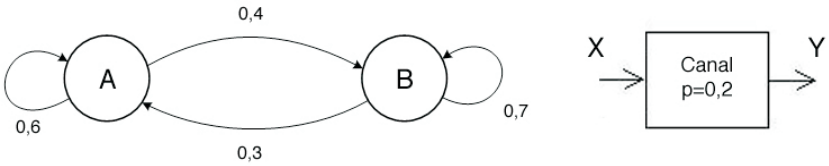


Fig. 1.24: Probabilitats de transició

$$H = H(Y|X=A)\cdot P(A) + H(Y|X=B)\cdot P(B)$$

$$\begin{aligned} H(Y|X=A) &= P(Y=A|X=A)\cdot \log_2 \frac{1}{P(Y=A|X=A)} + \\ &+ P(Y=B|X=A)\cdot \log_2 \frac{1}{P(Y=B|X=A)} \end{aligned}$$

$$\begin{aligned} H(Y|X=B) &= P(Y=A|X=B)\cdot \log_2 \frac{1}{P(Y=A|X=B)} + \\ &+ P(Y=B|X=B)\cdot \log_2 \frac{1}{P(Y=B|X=B)} \end{aligned}$$

$$\begin{aligned} P(Y=A|X=A) &= P(A|A)\cdot(1-p) + P(B|A)\cdot p \\ P(Y=B|X=A) &= 1 - P(Y=A|X=A) \\ P(Y=B|X=B) &= P(A|B)\cdot p + P(B|B)\cdot(1-p) \\ P(Y=A|X=B) &= 1 - P(Y=B|X=B) \end{aligned}$$

Resolent:

$$\begin{aligned} P(Y=A|X=A) &= 0.56 \\ P(Y=B|X=A) &= 0.44 \\ P(Y=B|X=B) &= 0.62 \\ P(Y=A|X=B) &= 0.38 \end{aligned}$$

$$H(Y|X=A) = 0.990$$
$$H(Y|X=B) = 0.958$$
$$H(Y) = 0{,}972 \text{ bits}$$

Com que el canal genera incertesa, l'entropia a la sortida és més gran.

c) El no canal es comportarà com un canal binari simètric, amb una probabilitat d'encreuament que haurà de ser menor. La probabilitat d'encreuament del nou

canal serà la probabilitat que als canals en paral·lel es produeixin dos o tres encreuaments.

$$p_e = \binom{3}{2}p^2(1-p) + \binom{3}{3}p^3 = 3 \cdot p^2(1-p) + 1 \cdot p^3 = 3p^2 - 2p^3 = 0.104$$

$$\text{capacitat del nou canal} = 1 - \left[0.104 \log_2 \frac{1}{0.104} + 0.896 \log_2 \frac{1}{0.896}\right]$$
$$= 0{,}518 \text{ bits}$$

d) Repetint l'apartat *b* amb $p = 0.104 \Rightarrow H(Y) = 0{,}95$ bits

En ser un canal millor, l'entropia a la sortida és menor.

Problema 14

Un codi ternari utilitza les longituds ($l_1 = 3, l_2 = 2, l_3 = 3, l_4 = 3, l_5 = 3, l_6 = 3$) per a uns símbols amb probabilitats d'ocurrència ($p_1 = 1/4$, $p_2 = 1/6$, $p_3 = 1/12$, $p_4 = 1/6$, $p_5 = 1/4$, $p_6 = 1/12$), respectivament. Sense estendre la font, es pot dir que:

a) La longitud mitjana és inferior a $H + 1$.
b) Compleix la desigualtat de Kraft, de manera que és instantani.
c) No hi ha cap altre codi amb una longitud mitjana menor.
d) Cap de les respostes anteriors és correcta.

Solució

a) La longitud mitjana de codificació serà:

$$\overline{L} = 3 \cdot \frac{1}{4} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{12} + 3 \cdot \frac{1}{6} + 3 \cdot \frac{1}{4} + 3 \cdot \frac{1}{12} = \overline{L} = \frac{2}{6} + 3 \cdot \frac{5}{6}$$
$$= 2{,}833 \text{ dígits ternaris/símbol}$$

$$H + 1 = \sum_{\forall i} p_i \cdot \log_3 \; p_i + 1 = \cdots = 1.551 + 1$$
$$= 2{,}55 \text{ dígits ternaris/símbol} \rightarrow a \text{ falsa}$$

b) Que el codi compleixi la desigualtat de Kraft no garanteix que sigui instantani, sinó que existeix un codi amb aquestes mateixes longituds que ho és. Per tant, *b* és falsa.

c) Per inspecció a l'arbre

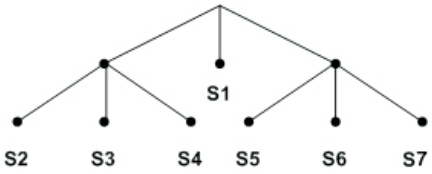


Fig. 1.25: Codificació ternària de Huffman

$\rightarrow \overline{L} = 2 \cdot \frac{2}{6} + 1 \cdot \frac{2}{6} = 1{,}75$ dígits ternaris/símbol. Per tant, c és falsa.

2
Codificació de canal

2.1. Introducció

El contingut teòric corresponent a aquest capítol presenta els principals conceptes, tècniques i algorismes que es fan servir en la codificació i la descodificació de la informació transmesa. En moltes situacions, l'índex d'error del sistema de transmissió sense codificar és massa alt. En aquest cas, cal recórrer a tècniques de codificació de canal, ja sigui per detectar errors (i fer una retransmissió de les dades), o bé per corregir-les [COST83, GITL92].

Els mètodes de codificació de canal es basen sempre en la introducció d'una certa redundància a la seqüència d'informació, cosa que implica una disminució de l'índex de transmissió, a igual esquema modulador. A la recepció, el descodificador aprofita la redundància per determinar si hi ha hagut errors i, si és així, intentar corregir-los. Els codificadors es poden dividir en dues categories bàsiques: codis bloc (sistema combinacional o sense memòria) i codis convolucionals (sistema seqüencial o amb memòria) [SKLA88].

Els codis bloc treballen amb una quantitat fixa de símbols d'informació i afegeixen una certa quantitat de símbols redundants en funció del nombre de símbols que poden corregir o detectar. Els codis convolucionals es poden interpretar com un filtre digital. Per tant, els codificadors convolucionals accepten la seqüència d'entrada de forma continuada i generen una sortida d'índex més gran [CARL86].

Es pot plantejar una altra estratègia pel que fa a la protecció de la informació que s'introdueix al canal. Així, la redundància es pot afegir al propi procés de modulació, augmenta el nombre de punts de la constel·lació i imbrica els processos de modulació i codificació. Aquest tipus de tècniques es coneix bàsicament amb el nom de TCM (*trellis-coded modulation* o modulació codificada d'enreixat) i té la propietat interessant que no altera l'índex real de transmissió, a igual potència i ample de banda.

2.2. Continguts teòrics

Aquesta és la relació dels continguts teòrics que es tracten a la classe de transmissió de dades.

- Fonaments bàsics. Estratègia FEC (*forward error correction*) *versus* ARQ (*automatic repeat request*)
- Codis bloc
  - Capacitat correctora/detectora d'errors i correctora d'esborraments
  - Entrellaçat
  - Codis e-perfectes i de Hamming
  - Codis polinòmics i codis cíclics
- Codis convolucionals
- Modulació codificada

2.3. Bibliografia

[CARL86] Carlson, Bruce A. (2001): *Communication Systems*. 4a ed. McGraw-Hill Int. ISBN-10: 0070111278.

[COST83] Lin, S.; Costello, J. (1983): *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, ISBN-10: 013283796X.

[GITL92] Gitlin, Richard D.; Hayes, Jeremiah F.; Weinstein, Stephen B. (1992): *Data Communications Principles*. Nova York-Boston: Plenum Press. ISBN-10: 0306437775.

[SKLA88] Sklar, B. (2001): *Digital Communications. Fundamentals and Applications*. 2a ed. Prentice Hall. ISBN-10: 0130847887.

2.4. Problemes

Problema 1

Sigui un LFSR amb el polinomi de connexions primitiu $c(D) = 0103$ (en notació octal, més pes a l'esquerra). L'estat inicial del LFSR és D^2. Quant val $D^{192} \bmod c(D)$?

a) 1
b) D^3
c) D^5
d) Cap de les respostes anteriors és correcta.

Solució

És habitual expressar els polinomis de connexions en notació octal. Per trobar el polinomi, només cal expressar-lo en binari i associar coeficients de $c(D)$ a les potències corresponents als uns.

$c(D) = 0103$. Codificació de 0103 en binari $= 0\,0\,0|0\,0\,1\,|0\,0\,0|0\,1\,1| = D^6 + D + 1$

Per tant, $S^0(D) = D^2$. Per l'enunciat, sabem que el polinomi $c(D)$ és primitiu, de manera que produirà seqüències periòdiques de longitud màxima:

$L = L_{\text{màx}} = 2^m - 1 = 2^6 - 1 = 63$, essent m el grau del polinomi de connexions $c(D)$.

Com que sabem que $D^L \cdot p^0(D) \bmod c(D) = p^0(D)$, en particular també $D^L \bmod c(D) = 1$, escrivim:

$D^{192} \bmod c(D) = D^{3\cdot 63+3} \bmod c(D) = D^3 \bmod c(D) = D^3 \bmod D^6 + D + 1 = D^3$

Problema 2

Un bibliotecari està introduint els codis ISBN-10 de diversos llibres en una aplicació. En introduir l'ISBN del llibre *Digital Communications*, d'E. Lee i D. Messerschmitt, observa que hi ha un dígit raspat, impossible de llegir: $0792 * 93910$. Quina afirmació és certa?

a) El codi ISBN correcte és 0792893910.
b) El valor correcte de l'esborrament és 4.
c) No és possible corregir aquest esborrament.
d) Cap de les respostes anteriors és correcta.

Solució

El codi ISBN té capacitat correctora d'esborraments $\rho = 1$ igual a la capacitat detectora d'errors, $\delta = 1$. No corregeix cap error ($e = 0$).

Sigui $Z = 0792 * 93910$ la paraula rebuda, on $*$ indica un esborrament a la paraula. Com que el nombre d'esborraments no és superior a la capacitat correctora d'esborraments del codi ($1 \leq \rho = 1$), aquest esborrament es pot corregir.

Per corregir-lo, només cal igualar la síndrome associada a la paraula rebuda a 0:

$$\vec{s_r} = Z \cdot H^{\top} = \vec{0_r}$$

on H és la matriu de comprovació del codi ISBN vista a classe i r és la redundància del codi, $r = 1$. Anomenem a la incògnita, és a dir, el valor de l'esborrament.

$$s = Z \cdot H^T = 0$$

$$s = (0792a93910) \cdot \begin{pmatrix} 10 \\ 9 \\ 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix} = 235 + 6a = 0 \bmod 11$$, ya que el codi ISBN trabaja en Z_{11}

$Z_{11} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$, essent $X \equiv 10$

Provem múltiples d'11 tals que a sigui un enter que faci complir l'equació:

$(235 + 6a) \bmod 11 = 0$

¿$235 + 6a = 242$? $\Rightarrow$ $6a = 7$ No és a un enter.

¿$235 + 6a = 253$? $\Longrightarrow$ $6a = 18$ $\Longrightarrow$ $a = 3$

El codi ISBN correcte és 0792393910. La resposta correcta és *d*.

Problema 3

Sigui un codi de Hamming sistemàtic amb la matriu de comprovació següent, tal que $H = (-P^T | I_r)$:

$$H = \begin{pmatrix} 110 * * * * \\ 011 * * * * \\ 101 * * * * \end{pmatrix}$$

Es transmet $Y = 0000000$ i durant la transmissió es produeixen errors en les posicions 2, 3, 4 i 5. Quin missatge d'usuari descodificaríem?

a) $X = 0100$
b) $X = 0111$
c) $X = 0011$
d) $X =$ Cap dels anteriors.

Solució

Observem que $H_{r\times n} \longrightarrow r = 3$ files; $n = 7$ columnes $\Longrightarrow k = n - r = 4$

La matriu de comprovació d'un codi sistemàtic té la forma següent. Recordem que la matriu de comprovació $H_{r\times n}$ està formada per r vectors de n components, linealment independents. Així, H genera el subespai vectorial ortogonal al codi. Es compleix que $G_{k\times n} \cdot H^T_{n\times r} = \varnothing_{k\times r}$ és la matriu nul·la de k files i r columnes. Ambdues matrius són ortogonals.

Per a $H = (-P^T|I_r)$, es compleix:

$$H_{r\times n} = (-P^T|I_r) \Longrightarrow H = \left(\begin{array}{c:c} 110* & 100 \\ 011* & 010 \\ 101* & 001 \end{array}\right) \Longrightarrow \begin{pmatrix} * \\ * \\ * \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Veiem que aquesta és la columna que falta, ja que un codi de Hamming ha de tenir totes les columnes de H diferents per poder corregir els n errors simples. Ja coneixem H:

$$\Longrightarrow H = \left(\begin{array}{c:c} 1101 & 100 \\ 0111 & 010 \\ 1011 & 001 \end{array}\right)$$

Paraula codi enviada: $Y = 0\ \underline{0}\ \underline{0}\ \underline{0}\ \underline{0}\ 0\ 0 \Longrightarrow Z = 0\ 1\ 1\ 1\ 1\ 0\ 0$ és la paraula rebuda, atès que les posicions assenyalades experimenten errors.

Trobem la síndrome associada a Z:

$$\vec{s}_r = Z \cdot H^T = (0\ 1\ 1\ 1\ 1\ 0\ 0) \cdot H^T = \begin{pmatrix} 101 \\ 110 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{pmatrix} = (1\ 1\ 0) = 2^{\text{a}} \text{ fila de } H^T \Longrightarrow$$

$$\Longrightarrow \hat{\vec{e}} = 0\ 1\ 0\ 0\ 0\ 0\ 0$$

Veiem que $\vec{s}_r$ coincideix amb la segona fila de H^T, de manera que es resol que el vector d'error deuria ser un $\vec{e}_n$ amb $n - 1$ zeros i un 1 a la posició de l'error, el segon bit.

Finalment, com que la paraula rebuda Z és el resultat de sumar el vector d'error a la paraula enviada Y, és a dir:

$$Z = Y \oplus \vec{e}$$

podem aïllar la paraula que considerem que va ser enviada:

$$\hat{Y} = Z \oplus \hat{\vec{e}} = 0111100 + 0100000 = \underbrace{0011}_{k=4}100$$

El missatge estimat, en ser un codi sistemàtic, coincideix amb els k primers bits de la paraula codi estimada:

$$\hat{X} = 0011$$

Problema 4

Sigui un codi polinòmic sistemàtic (7,4), amb polinomi generador $g(D) = 1 + D + D^3$. Trobeu la matriu generadora.

a) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

d) Cap de les respostes anteriors és correcta.

Solució

Es tracta d'un codi cíclic sistemàtic (7,4) $\longrightarrow$ $r = n - k = 3$, ja que $n = 7$ i $k = 4$

En ser sistemàtic, la matriu generadora té aquesta forma:

$$G_{k\times n} = (I_k|P_{k\times r}) = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & - & - & - \\ 0 & 1 & 0 & 0 & - & - & - \\ 0 & 0 & 1 & 0 & - & - & - \\ 0 & 0 & 0 & 1 & - & - & - \end{array}\right)$$

En un codi cíclic sistemàtic, es compleix:

$R(D) = D^r \cdot X(D) \bmod g(D)$

$Y(D) = D^r \cdot X(D) + R(D)$

essent $X(D)$ el missatge d'usuari i $C(D)$ el polinomi de connexions, escrits tots dos de forma polinòmica.

Per tant, per obtenir la matriu generadora $G_{k\times n}$, n'hi ha prou a obtenir la codificació dels quatre missatges d'usuari 1000, 0100, 0010 i 0001, corresponents a la base canònica del conjunt de missatges d'usuari.

a) $X = 1000 \equiv D^3 = X(D),\ D^r \cdot X(D) = D^6$

$R(D) = D^r \cdot X(D) \bmod g(D) = D^6 \bmod (D^3 + D + 1) = D^2 + 1$

D^6 | D^3+D+1

$D^6+D^4+D^3$ | D^3+D+1

D^4+D^3

D^4+D^2+D

D^3+D^2+D

D^3+D+1

$D^2+1=R(D)$

$Y(D) = D^r \cdot X(D) + R(D) = D^6 + D^2 + 1 \equiv 1000|101$

b) $X = 0100 \equiv D^2 = X(D),\ D^r \cdot X(D) = D^5$

$R(D) = D^r \cdot X(D) \bmod g(D) = D^5 \bmod (D^3 + D + 1) = D^2 + D + 1$

$Y(D) = D^r \cdot X(D) + R(D) = D^5 + D^2 + D + 1 \equiv 0100|111$

c) $X = 0010 \equiv D = X(D),\ D^r \cdot X(D) = D^4$

$R(D) = D^r \cdot X(D) \bmod g(D) = D^4 \bmod (D^3 + D + 1) = D^2 + D$

D^4 | D^3+D+1

D^4+D^2+D | D

$D^2+D=R(D)$

$Y(D) = D^r \cdot X(D) + R(D) = D^4 + D^2 + D \equiv 0010|110$

d) $X = 0001 \equiv 1 = X(D),\ D^r \cdot X(D) = D^3$

$R(D) = D^r \cdot X(D) \bmod g(D) = D^3 \bmod (D^3 + D + 1) = D + 1$

$$\begin{array}{l|l} D^3 & D^3+D+1 \\ \hline D^3+D+1 & 1 \\ \hline D+1=R(D) & \end{array}$$

$Y(D) = D^3 + D + 1 \equiv 0001|011$

Finalment, aquesta és la matriu generadora, de manera que la resposta correcta és la a.

$$G_{k\times n} = (I_k|P_{k\times r}) = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

Problema 5

Sigui un codi (7,4) de Hamming, que té com a matriu de comprovació (a la qual li falta una columna per determinar, marcada amb asteriscs):

$$H = \left(\begin{array}{ccccccc} 0 & 1 & * & 1 & 1 & 0 & 0 \\ 1 & 1 & * & 1 & 0 & 1 & 0 \\ 1 & 1 & * & 0 & 0 & 0 & 1 \end{array}\right) = (-P^T|I_r)$$

El desmodulador detecta una alta presència de soroll en dues mostres, que marca com a a i b. En cada cas, es rep la paraula Z i s'estima el missatge d'usuari X. Quin cas pot ser que s'hagi produït?

a) $Z = 1a0b101,\ X = 1101$
b) $Z = ab11011,\ X = 0111$
c) $Z = 1ab0110,\ X = 1010$
d) Cap de les respostes anteriors és correcta.

Solució

En ser un codi de Hamming (1-perfecte), la capacitat correctora d'errors és $e = 1$. El vector d'error (errors corregibles) $\vec{e_n}$ tindrà un únic component no nul. Les síndromes associades a cada error corregible coincideixen amb les columnes de $H_{r\times n}$, de manera que aquestes han de ser diferents. Així, cada error corregible té una síndrome associada diferent.

$$\vec{s_r} = Z \cdot H^\top = (Y + \vec{e}) \cdot H^\top = Y \cdot H^\top + \vec{e} \cdot H^\top = \vec{e_n} \cdot H^\top_{n\times r}$$

Hamming ⇒ e=1 ⇒ H té les 7 columnes diferents.

Per tant, la columna que falta a $H_{r\times n}$ és la terna de bits que queda disponible:

$$\begin{pmatrix} * \\ * \\ * \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Hamming $\longrightarrow$ 1-perfecte $\longrightarrow \left\{ \begin{array}{l} d_{min} = 2e + 1 = 3 \\ \rho = d_{min} - 1 = 2 \end{array} \right\} \Longrightarrow$ sempre pot corregir fins a dos esborraments.

Per corregir els esborraments que hi ha en una paraula rebuda Z_n, n'hi ha prou a forçar que la síndrome associada $\vec{s}_r$ sigui nul·la:

$\vec{s}_r = Z_n \cdot H^{\top}_{n\times r} \equiv 0$

Un cop corregida Z_n, el missatge estimat $\hat{X}_k$ es correspon amb els $k = 4$ primers bits de Z_n.

a) $\vec{s}$=Z·H^T=(1a0b101)$\cdot \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1 + a + b, 1 + a + b, a) \equiv (000) \quad \Rightarrow$

$\left\{ \begin{array}{l} a = 0 \\ b = 1 \end{array} \right\} \quad \Rightarrow \quad X = 1001$. No coincideix.

b) $\vec{s} = Z \cdot H^T = (b,\ a + b,\ a + b) \equiv (000) \quad \Longrightarrow \quad a = b = 0 \quad \Longrightarrow \quad X = 0011.$

No coincideix.

c) $\vec{s} = Z \cdot H^T = (1+a+b,\ a,\ 1+a+b) \equiv (000) \quad \Longrightarrow \quad \left\{ \begin{array}{l} a = 0 \\ b = 1 \end{array} \right\} \quad \Rightarrow \quad X = 1010.$

Resposta correcta.

Problema 6

Un sistema de transmissió fa servir un codi corrector de Hamming (7,4). Si la probabilitat d'error de bit al canal és 10^{-4}, quant val l'índex d'error de bit a nivell d'usuari?

Solució

Els codis de Hamming són 1-perfectes, és a dir, corregeixen fins a un error i no en corregeixen cap més. Per tant, perquè es produeixi almenys un error en el bloc, després de descodificar cal que es produeixin dos errors o més en el bloc rebut.

$$p_E(\text{bloc}) = \sum_{i=2}^{7} \binom{n}{i} p^i (1-p)^{7-i}.$$

Aquesta expressió, com que el valor de p és prou baix, es pot aproximar per

$$p_E(\text{bloc}) \approx \binom{7}{2} p^2(1-p)^5 = 21 \cdot (10^{-4})^2(1-10^{-4})^5 \approx 21 \cdot 10^{-8}$$

Ara bé, quan es produeixen dos errors en el bloc, el codificador de Hamming ho interpreta com un error simple, sempre en una posició diferent d'on es trobaven els dos errors, ja que la síndrome que obté és la suma de les dues columnes de la matriu de comprovació en què es van produir els errors. Com que la suma de qualsevol columna d'aquesta matriu sempre és una tercera columna, el descodificador introduirà un nou error, de manera que apareixeran en total tres errors en el bloc descodificat.

Per tot això, la probabilitat d'error de bit serà:

$$\begin{aligned} p_e(\text{bit}) &= \frac{\#\text{bits erronis}}{\#\text{bits totals}} = \frac{3 \cdot \#\text{blocs erronis}}{7 \cdot \#\text{blocs totals}} \\ &= \frac{3}{7} \cdot 21 \cdot 10^{-8} = 9 \cdot 10^{-8} = \frac{3}{7} \cdot 21 \cdot 10^{-8} = 9 \cdot 10^{-8} \end{aligned}$$

Problema 7

En un codi de Hamming (7,4) sistemàtic, es pot afirmar que:

a) La submatriu de paritat pot tenir dues files iguals.
b) La submatriu de paritat pot tenir dues columnes iguals.
c) La matriu de comprovació pot tenir dues files iguals.
d) No es pot afirmar res de l'anterior.

Solució

En ser de Hamming, totes les columnes de H han de ser diferents, atès que és 1-perfecte:

$$H(3\times 7)=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}=(-P^T|I_r)$$

$$G(7\times 4)=\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&1\end{pmatrix}=(I_k|P)$$

on la segona submatriu de G és la submatriu de paritat P. Per tant les files de P només poden ser (1 0 1), (1 1 1), (1 1 0) i (0 1 1) en qualsevol ordre

a) 2 files de P iguals $\Longrightarrow$ 2 columnes de H iguals $\Longrightarrow$ impossible.

b) 2 columnes de P iguals $\Longrightarrow$ les 4 files de P són 4 vectors particulars i no es pot aconseguir reordenant les files o columnes.

c) impossible, pues està I_r en $H \Longrightarrow$ 2 files de H no són mai iguals.

Problema 8

El polinomi de connexions d'un LFSR és $D^4 + D + 1$. Indiqueu la resposta *falsa*:

a) La seqüència generada és $D^{11} + D^8 + D^7 + D^5 + D^3 + D^2 + D + 1$.
b) La probabilitat que existeixi un 0 és de 7/15.
c) La seqüència generada té ràfegues de quatre 1 i tres 0.
d) Alguna de les respostes anteriors és falsa.

Solució

Com que $D^4 + D + 1$ és primitiu, genera una seqüència de màxim període (MLSR), en aquest cas igual a $2^4 - 1 = 15$. A més, en aquest tipus de seqüències, la probabilitat d'emetre un 0 és $p(0) = 7/15$ i la d'emetre un 1 és $p(1) = 8/15$. Per tant, *b* és certa.

La seqüència de sortida es pot calcular amb l'operació següent:

$$D^{15}+1 \;\big|\; D^4+D+1$$
$$0 \qquad\qquad D^{11}+D^8+D^7+D^5+D^3+D^2+D+1 \Longrightarrow \text{a) cierta}$$

de manera que *a* és certa.

Del resultat anterior, s'obté que la seqüència de sortida és 000100110101111, és a dir, *c* és certa.

Per tot això, es conclou que *d* és *falsa*.

Problema 9

Sigui un codi (n, k) que es caracteritza perquè la distància entre dues paraules qualssevol és quatre. Es pot afirmar que:

a) El codi és 2-perfecte.
b) El codi és 4-perfecte.
c) El codi és 1-perfecte.
d) Res de l'anterior és cert.

Solució

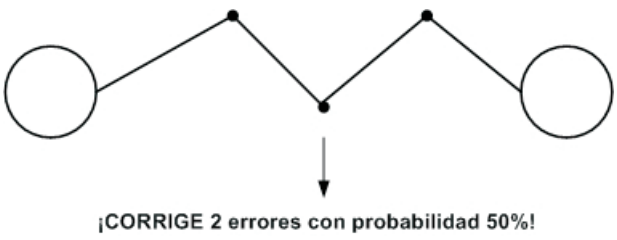


Fig. 2.1: Esquema de correcció per a un codi e-perfecte

Un codi és *e*-perfecte quan corregeix fins a *e* errors i mai $e + 1$. Si la distància del codi és parell, quan es rebi una n-pla a distància $\frac{d_{\text{mín}}}{2} > e = \left\lfloor \frac{d_{\text{mín}-1}}{2} \right\rfloor$, es corregirà en el 50 % dels casos, de manera que cap codi amb distància parell pot ser perfecte. Per tant, es conclou que la resposta correcta és la *d*.

Problema 10

Un codi de Hamming (7,4) s'ha estès amb 1 bit de paritat global per utilitzar-lo en un canal amb una probabilitat d'error de bit de 10^{-4} i una probabilitat d'esborrament de 10^{-3}. La probabilitat p de rebre un error i un esborrament és:

a) $p \geq 0.044 \cdot 10^{-3}$
b) $0.044 \cdot 10^{-3} > p \geq 0.033 \cdot 10^{-3}$
c) $0.033 \cdot 10^{-3} > p \geq 0.022 \cdot 10^{-3}$
d) $0.022 \cdot 10^{-3} > p$

Solució

Per fer aquest càlcul, cal trobar un nombre de paraules amb un esborrament i un error, és a dir, $\binom{8}{2}$ multiplicat per 2 (no és el mateix un esborrament a la posició i i un error a la j que un esborrament a la posició j i un error a la i).

Qualsevol d'aquests casos en què es produeix un esborrament i un error té una probabilitat que succeeixi igual a $p_e \cdot p_b\,(1-(p_e+p_b))^6$. És a dir:

$$2\cdot\binom{8}{2}p_e\cdot p_b\,(1-(p_e+p_b))^6 = 2\cdot\binom{8}{2}p_e^2\cdot(1-2p_e)^6$$
$$= \{\text{on } p_b = p_e = 10^{-3}\} = 0.055\cdot 10^{-3}$$

Per tant, la solució correcta és *a*.

Problema 11

Es disposa d'un codi (6,3) binari lineal i sistemàtic, corrector d'errors, i siguin Y_1, Y_2 paraules codi, on $Y_1 = 110110$ y $Y_2 = 101011$. Calculeu:

a) Capacitat correctora del codi. És un codi perfecte?
b) Com es codifica el missatge 111?
c) Indiqueu si la matriu següent pot ser de comprovació:

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

d) Suposem que s'ha rebut la paraula $Z = 001001$. Quina seria la decisió del descodificador si s'utilitza el codi com a corrector?

Solució

Com que es tracta d'un codi corrector d'errors $\Rightarrow \left\{ \begin{array}{c} e \geq 1 \\ d_{\text{mín}} \geq 3 \end{array} \right\} \Rightarrow W_{\text{mín}} \geq 3$

Disposem de dues paraules codi $Y_1 = 110110$ i $Y_2 = 101011$, però el codi és $(6, 3)$ lineal $\Rightarrow$ en necessitaríem una més, independent de les anteriors, per disposar d'una base (ja que $k = 3$). Intentem veure ara les possibilitats de les vuit paraules codi ($k = 3$). Per a això, tindrem en compte que el codi sigui sistemàtic, lineal i corrector d'errors:

$\underline{X}$		$\underline{Y}$
000		000 000
001		001 abc $\rightarrow$ Y_3
010		010 $\overline{a}b\overline{c}$ $\rightarrow$ $Y_1 + Y_2 + Y_3$
011	$\longrightarrow$	011 101 $\rightarrow$ $Y_1 + Y_2$
100		100 $a\overline{b}\overline{c}$ $\rightarrow$ $Y_1 + Y_3$
101		101 011 $\rightarrow$ Y_1
110		110 110 $\rightarrow$ Y_2
111		111 $\overline{a}\overline{b}c$ $\rightarrow$ $Y_2 + Y_3$

¿a, b, c? La taula següent mostra totes les combinacions possibles. Posteriorment, n'anirem eliminant aquelles que no facin que $d_{\text{mín}} \geq 3$:

a	b	c
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$Y_3 \rightarrow$ del conjunt (a, b, c), almenys dues han de ser iguals a 1.

$Y_1 + Y_2 + Y_3 \rightarrow$ Del conjunt ($\overline{a}$, b, $\overline{c}$) almenys dues han de ser iguals a 1.

Casos possibles:

Primera fila: No, Y_3 tindria $W_H = 1$

Segona fila: No, Y_3 tindria $W_H = 2$

Tercera fila: No, Y_3 tindria $W_H = 2$

Quarta fila: No, $Y_1 + Y_3$ tindria $W_H = 1$

Cinquena fila: No, Y_3 tindria $W_H = 2$

Sisena fila: No, $Y_1 + Y_2 + Y_3$ tindria $W_H = 1$

Setena fila: Sí

Vuitena fila: No, $Y_1 + Y_2 + Y_3$ tindria $W_H = 2$

$(a, b, c) = (1, 1, 0)$

$d_{\text{mín}} = 3 \Rightarrow e_c = 1$

Podem generar tot el codi:

000	000	2
001	110	3
010	011	2
011	101	2
100	101	3
101	011	2
110	110	6
111	000	2

a) Com que $d_{\text{mín}} = 3 \rightarrow e = \dfrac{d_{\text{mín}} - 1}{2} = 1$ ($e = 1$ ja que agafem el sencer inferior del resultat que n'obtenim).

Es pot veure fàcilment que no és un codi 1-perfecte. En ser binari i $e = 1$, per ser perfecte hauria de complir que $2^r = 1 + n$ i, en aquest cas, $r = 3$, $n = 6$. De fet, aquest codi és un codi retallat, obtingut a partir del codi(7,4) de Hamming, que sí que és 1-perfecte.

b) $X = 111 \rightarrow Y = X \cdot G$

$$G_{kxn} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$Y = (111) \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = 111000$$

c) S'ha de complir que $G \cdot H^T = 0$

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

d) $Z = 001001$

$$\vec{s} = Z \cdot H^T = 001001 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 001 \rightarrow$$ No coincideix amb cap fila de H^T, així que no es correspon amb un error simple.

De fet, veiem que Z és a una distància 2 de diverses Y, però no podem triar una Y a distància mínima. En aquesta Z, hi ha hagut més errors que la capacitat correctora del codi, $e = 1$. El codi no considera aquest error múltiple amb un error simple, així que no el pot corregir. És millor així, perquè si ho fes es podria equivocar e introduir un altre error. El codi sí que detecta que aquesta Z rebuda és errònia, perquè la seva síndrome coneguda $\vec{s}$ no és nul·la.

3
Criptografia

3.1. Introducció

La proliferació del correu electrònic o dels serveis web ha comportat un canvi substancial en la manera de difondre la informació, que combina informació multimèdia amb enllaços que faciliten el salt a una altra pàgina o objecte. La funcionalitat correcta d'aquests serveis exigeix una implantació adequada de mesures de seguretat. La implantació sistemàtica de serveis de seguretat a les xarxes existents requereix utilitzar protocols i tècniques de seguretat adequades, compatibles amb les especificacions actuals. Els serveis de seguretat bàsics en les comunicacions són: autenticació, control de accés, confidencialitat, integritat de les dades i no repudi [PAS08].

La criptografia és un mecanisme fonamental per implementar els serveis de seguretat esmentats. La criptografia, coneguda des d'antic com l'art de l'escriptura secreta, s'ha convertit avui en una companya imprescindible del desenvolupament de la societat de la informació. Els objectius principals de la criptografia són la confidencialitat, la integritat i l'autenticitat en el tractament de la informació en format electrònic. Una de les aplicacions més notables d'aquesta disciplina és el comerç electrònic segur [SCH96].

A la figura 3.1, es presenta un esquema de la transmissió segura d'un missatge M entre dues entitats, a través d'un canal insegur.

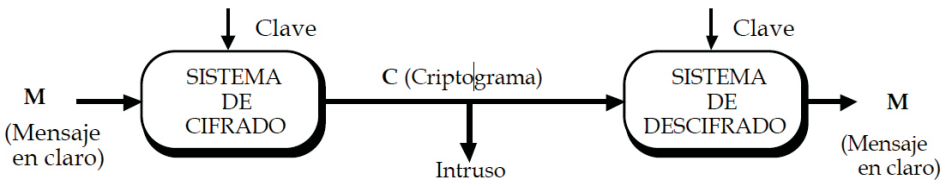


Fig. 3.1: Esquema de transmissió segura d'un missatge

Els sistemes criptogràfics d'aquest esquema s'encarreguen de calcular el missatge xifrat C, a partir del missatge en clar M i de la "clau de xifratge", i de fer el procés invers, el desxifratge, i determinar així M a partir del missatge encriptat i la "clau de desxifratge". Aquestes dues claus, com veurem més endavant, no han de ser necessàriament

iguals. Quan un sistema criptogràfic utilitza en el desxifratge la mateixa clau que en el xifratge, es diu que fa servir un "xifratge simètric" o, més precisament, "de clau simètrica". Per contra, si la clau de desxifratge és diferent de la clau de xifratge, el sistema està fent servir u "de clau asimètrica" [RIF91].

Un sistema de criptografia simètric és una família de transformacions invertibles, en què l'emissor i el receptor fan servir la mateixa clau K. La clau K s'ha hagut de donar a conèixer prèviament a les dues parts mitjançant l'ús d'un canal secret. Aquesta clau, doncs, ha de ser distribuïda amb antelació a la comunicació. El cost i el retard que aquesta necessitat imposa són els obstacles principals per a la utilització de la criptografia de clau secreta a les grans xarxes [STA00].

Entre els algoritmes simètrics, podem destacar els de xifratge en bloc i els de xifratge de flux. Aquests darrers són els més indicats per a entorns d'alta velocitat de transmissió. Els simètrics de xifratge en bloc són els més utilitzats a les xarxes de dades, i es poden classificar entre "de domini public" (es publica l'algorisme amb tot detall) o "propietari" (en què es manté en secret l'algorisme). A l'ambient acadèmic es prefereixen els algorismes de domini públic que han estat sotmesos a un intens escrutini per part de la comunitat criptogràfica i no s'han vist compromesos (diversos algoritmes propietaris d'ús comercial han estat vulnerats per mètodes d'enginyeria inversa).

Probablement l'algorisme criptogràfic més utilitzat és l'AES (Advanced Encryption Standar, 2001) que és de domini públic i el substitut de l'antic DES (Data Encryption Standar, 1977). Tot i la seva antiguitat, encara se segueix utilitzant en alguns entorns.

En els sistemes de "xifrat asimètric", també coneguts com de "clau pública", el xifrador fa servir una clau P, mentre que el desxifrador fa servir una clau diferent S. La clau P és pública i la clau S és privada i incalculable a partir de P en un temps prudencial (encara que molts sistemes d'aquest tipus resultaran vulnerables davant l'eventual ús d'un computador quàntic) El sistema asimètric possibilita la comunicació en un sentit; per realitzar la comunicació en sentit contrari, es necessita un altre parell de claus secreta-pública. La característica principal que fa que aquests mètodes siguin interessants per davant dels sistemes criptogràfics simètrics és que no cal cap intercanvi de secrets entre els dos comunicants. Els algoritmes de clau pública es basen en la teoria de nombres i de cossos finits. Gràcies a aquest fonament matemàtic, és possible demostrar la seguretat computacional d'aquests mètodes. Un dels algoritmes asimètrics més utilitzats és l'RSA (Rivest-Shamir-Adleman).

Tot i el seu ús generalitzat, resulta vulnerable davant de la computació quàntica, per la qual cosa s'estan desenvolupant sistemes basats en la "Post-quantum cryptography"

3.2. Continguts teòrics

- Introducció: seguretat computacional v. seguretat incondicional
- Serveis de seguretat: privacitat, autenticitat, verificabilitat
- Clau simètrica o secreta
  - Criptografia clàssica
  - Xifratge de bloc
  - Xifratge de flux
- Clau pública o asimètrica
  - Conceptes bàsics
  - Diffie-Hellman
  - RSA
- Funcions de *hash*
- Signatura digital
- Autenticació

3.3. Bibliografia

[PAS98] Pastor, J.; Sarasa, M.A. (1998): *Criptografía digital. Fundamentos y aplicaciones*. Prensas Universitarias de Zaragoza.

[RIF91] Rifà, J.; Huguet, Ll. (1991): *Comunicació digital*. Masson.

[SCH96] Schneier, B. (1996): *Applied Cryptography*. 2a ed. John Wiley & Sons.

[STA00] Stallings, W. (2000): *Network Security Essentials*. Prentice Hall.

3.4. Problemes

Problema 1

Es disposa d'un xifrador de quatre bits d'entrada i quatre bits de sortida que, per a una determinada clau k, té la següent relació d'entrada i sortida $[M, Ek(M)]$

M	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
$C = E_k(M)$	7	4	1	E	B	8	5	2	F	C	9	6	3	0	D	A

Taula 3.1: Relación entrada salida del cifrador

Es demana:

a) Quina és la mida mínima de la clau perquè el xifratge es pugui considerar perfectament aleatori?

b) El xifratge del missatge **FFF** és **6A6**. Raoneu perquè es pot assegurar que el xifratge no s'està utilitzant en mode natiu o ECB.

c) Quan es fa un encadenament, com en aquest cas, és usual utilitzar un vector d'inicialització. Indiqueu quines alternatives faríeu servir per a aquest vector inicial i quins avantatges aporten.

d) Sabent que les úniques operacions que s'han fet servir són $E_k(\cdot)$ i XOR, trobeu de forma raonada les equacions del xifrador i del desxifrador. Quant val el vector inicial?

Com a funció de *hash* d'un missatge de **n** blocs, es fa servir l'algoritme:

$$h_i = E_k(M_i + h_{i-1}), \qquad i = 1 \ldots 0, \qquad h_0 = 0, \qquad H = h_n$$

e) Calculeu el *hash* del missatge **FFF**. Quants missatges de tres blocs generaran el mateix *hash* que **FFF** i diferiran només en els dos primers blocs del missatge? (M_1 i M_2 diferents de F)

f) Obtingueu, de forma raonada, i no per proves exhaustives, el valor de M que fa que el missatge **M1F** tingui el mateix *hash* que **FFF**.

Solució

a) Per tal que un xifrador es pugui considerar perfectament aleatori, hi ha d'haver almenys una clau per a cada bijecció possible. D'aquesta manera, i com que el nombre de bijeccions possibles és $16! = 20.922.789.888.000$, la mida mínima en bits de la clau ha de ser: Nombre de bits $\geq \log_2 16! = 44.25 \Longrightarrow$ longitud $=$ 45 bits

b) Perquè el xifratge d'un missatge uniforme produeix un criptograma no uniforme.

c) Es pot utilitzar un número de seqüència o una estampació de temps. L'avantatge que aporten és que no es produeixen missatges estereotipats, és a dir, el mateix text clar genera criptogrames diferents a cada ocasió.

d) Possibilitats d'encadenament:

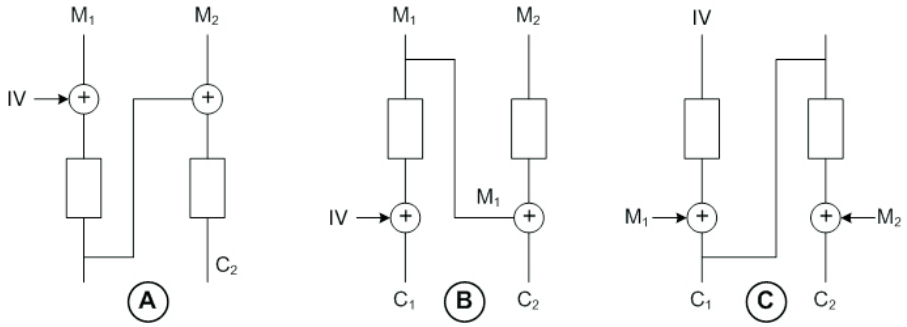


Fig. 3.2: Formes d'encadenament

Per a cadascuna d'aquestes possibilitats, es poden plantejar les equacions següents:

$$\left.\begin{array}{l} M_1 = F \\ M_2 = F \\ C_1 = 6 \\ C_2 = A \end{array}\right\} \begin{array}{ll} A) & E_k[C_1 + M_2] = E_k[6 + F] = E[9] = C \neq C_2 = A \implies NO \\ B) & E_k[M_2] + M_1 = E_k[F] + F = 5 \neq C_2 = A \implies NO \\ C) & E_k[C_1] + M_2 = E[6] + F = 5 + F = A = C_2 = A \implies OK \end{array}$$

i, per tant, les equacions del xifrador i del desxifrador són, respectivament:

$$C_i = M_i + E_k(C_{i-1})$$
$$M_i = C_i + E_k(C_{i-1})$$

Per trobar IV, de l'Apartat C, de la figura es dedueix l'equació següent:

$$IV = D_k[C_1 + M_1] = D_k[6 + F] = D_k[9] = A$$

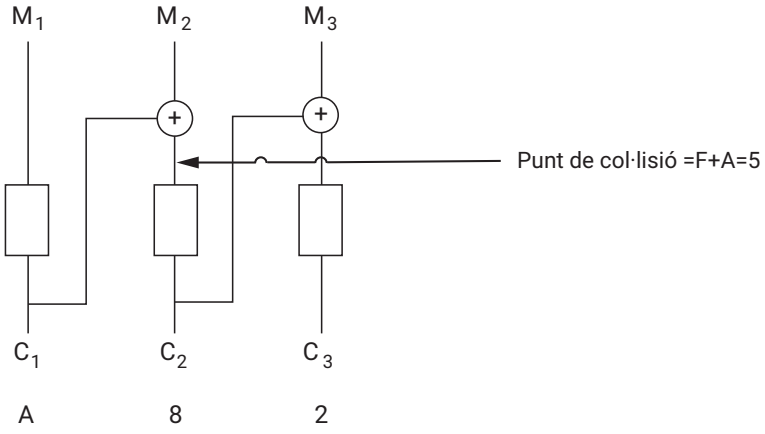


Fig. 3.3: Col·lisió de les funcions de hash

e) Utilitzant l'equació del càlcul de *hash*:

$$h_1 = E_k[F] = A$$
$$h_2 = E_k[F + A] = E_k[5] = 8$$
$$h_3 = E_k[F + 8] = E_k[7] = 2 = H$$

De la figura 3.3 anterior, es dedueix que tots els valors de M_1 i M_2 que satisfacin que en el punt de col·lisió s'obtingui un 5 donaran com a *hash* el valor F.

Per tant, deixant lliure M_1(diferent de F), sempre es pot trobar un valor $M_2(\neq \text{F})$ que generi $H = 2$, de manera que el nombre de possibles valors per a M_1 és 15 (ja que, si M_1 =F, llavors M_2 també ha de valer F).

f) $E_k[M] + 1 = 5 \implies E_k[M] = 4 \implies M = D_k[4] = 1$

Problema 2

Dissenyeu un registre de desplaçament de longitud 4 que generi una seqüència de període màxim.

Solució

Es tracta de trobar un polinomi primitiu de grau 4. Aquest polinomi indicarà les connexions que cal fer en el registre de desplaçament per obtenir una seqüència de longitud màxima.

Recordeu que una condició necessària perquè un polinomi sigui primitiu és que sigui irreductible. Per això, començarem trobant els polinomis irreductibles de graus 1, 2 i 3 i després obtindrem els de grau 4, i d'entre ells en cercarem un de primitiu. Recordeu, també, que per a qualsevol grau hi ha almenys un polinomi primitiu.

Grau 1

De grau 1, només hi ha dos polinomis possibles, que són:

1 D
2 $D + 1$

Grau 2

De grau 2, tindrem quatre possibles polinomis:

1 D^2
2 $D^2 + 1$
3 $D^2 + D$
4 $D^2 + D + 1$

Està clar que el polinomi 1 és divisible per D; per tant, no pot ser irreductible. El mateix passa per a qualsevol altre polinomi que no tingui un terme independent. D'aquesta manera, d'ara endavant podrem eliminar la meitat dels candidats (d'aquesta llista, n'eliminem pel mateix motiu el polinomi 3).

Vegem què passa amb el polinomi 2. D'una banda, qualsevol polinomi que tingui un nombre parell de termes satisfarà que $p(1) = 0$, ja que $1^x = 1$ per a qualsevol valor de x. Dit d'una altra manera, tot polinomi que tingui un nombre parell de coeficients en tindrà 1 com a arrel i, per tant, serà divisible per $D + 1$. Per a $D^2 + 1$, en tractar-se d'un cos de característica 2, passa que $D^2 + 1 = (D + 1)^2$: la característica 2 fa que, en elevar al quadrat un polinomi, no apareguin dobles productes, és a dir, que el quadrat de la suma sigui igual a la suma de quadrats. Per exemple:

$$(D + 1)^2 = D^2 + 2D + 1 = D^2 + 1$$

de manera que qualsevol polinomi que només tingui potències parells serà un quadrat perfecte i, per tant, no serà irreductible. Vegem-ne un exemple:

$$(D^2 + D + 1)^2 = D^4 + D^2 + 1$$

Com a resum, podem dir que cap polinomi que compleixi alguna d'aquestes característiques serà irreductible.

De tot això, es dedueix que cap dels polinomis 1, 2 i 3 pot ser primitiu, perquè són reductibles. Per tant, el polinomi 4 ha de ser irreductible i primitiu (recordeu que sempre existeix almenys un polinomi primitiu per a qualsevol grau).

Grau 3

De grau 3, tindrem vuit possibles polinomis:

1 D^3
2 $D^3 + 1$
3 $D^3 + D$
4 $D^3 + D + 1$
5 $D^3 + D^2$
6 $D^3 + D^2 + 1$
7 $D^3 + D^2 + 1$
8 $D^3 + D^2 + D + 1$

Els polinomis 1, 3, 5 i 7 no són irreductibles, perquè són divisibles per D. Els polinomis 2, 3, 5 i 8 tampoc no ho són, perquè tenen un nombre parell de termes i, en conseqüència, són divisibles per $D + 1$. Per tant, ens queden com a únics candidats a polinomis irreductibles:

4 $D^3 + D + 1$
6 $D^3 + D^2 + 1$

Tots dos han de ser primitius, perquè si un polinomi és primitiu el seu recíproc també ho és. És recíproc d'un polinomi $C(D)$ de grau n, i es denota per $C^*(D)$, aquell que satisfà que $C^*(D) = D^n C\left(\frac{1}{D}\right)$. Si un és primitiu, l'altre també ho ha de ser i, per tant, tots dos ho han de ser, atès que almenys un d'ells ho ha de ser.

Grau 4

De grau 4, tindrem setze possibles polinomis:

1	D^4	9	$D^4 + D^3$
2	$D^4 + 1$	10	$D^4 + D^3 + 1$
3	$D^4 + D$	11	$D^4 + D^3 + D$
4	$D^4 + D + 1$	12	$D^4 + D^3 + D + 1$
5	$D^4 + D^2$	13	$D^4 + D^3 + D^2$
6	$D^4 + D^2 + 1$	14	$D^4 + D^3 + D^2 + 1$
7	$D^4 + D^2 + D$	15	$D^4 + D^3 + D^2 + D$
8	$D^4 + D^2 + D + 1$	16	$D^4 + D^3 + D^2 + D + 1$

La propietat "no tenir terme independent" elimina els polinomis 1, 3, 5, 7, 9, 11, 13 i 15, i els polinomis 2, 3, 5, 8, 9, 12, 14 i 15 són eliminats per la propietat "tenir un nombre parell de termes". En aquest cas, la propietat "tenir només potències parells" elimina els polinomis 2, 5 i 6. Ens queden com a candidats a irreductibles:

4	$D^4 + D + 1$
10	$D^4 + D^3 + 1$
16	$D^4 + D^3 + D^2 + D + 1$

vspace-5mm D'aquests, veiem que els polinomis 4 i 10 són recíprocs i que el 16 és auto-recíproc. Triem el polinomi 4 (també podríem triar el 10) perquè té menys coeficients. Provarem si és divisible pels polinomis irreductibles de grau inferior a 4 que hem anat trobant, és a dir:

$$D^2 + D + 1$$
$$D^3 + D + 1$$
$$D^3 + D^2 + 1$$

Començant la prova, tenim que:

$(D^4 + D + 1) \mod (D^2 + D + 1) = 1$

$$
\begin{array}{l|l}
D^4+D+1 & D^2+D+1 \\
\cline{2-2}
D^4+D^3+D^2 & D^2+D \\
\cline{1-1}
D^3+D^2+D+1 & \\
D^3+D^2+D & \\
\cline{1-1}
1 &
\end{array}
$$

$(D^4 + D + 1) \mod (D^3 + D + 1) = D^2 + 1$

$$
\begin{array}{l|l}
D^4+D+1 & D^3+D+1 \\
\cline{2-2}
D^4+D^2+D & D \\
\cline{1-1}
D^2+1 &
\end{array}
$$

$(D^4 + D + 1) \mod (D^3 + D^2 + 1) = D^2$

$$
\begin{array}{l|l}
D^4+D+1 & D^3+D+1 \\
\cline{2-2}
D^4+D^3+D & D+1 \\
\cline{1-1}
D^3+1 & \\
D^3+D^2+1 & \\
\cline{1-1}
D^2 &
\end{array}
$$

En conseqüència, en no ser divisible per cap dels polinomis irreductibles de grau menor, el polinomi $D^4 + D + 1$ és necessàriament irreductible.

A manera de resum, tenim els resultats següents:

$D^4 + D + 1$	$\mod (D^2 + D + 1) = 1$ $\mod (D^3 + D + 1) = D^2 + 1$ $\mod (D^3 + D^2 + 1) = D^2$
$D^4 + D^3 + 1$	$\mod (D^2 + D + 1) = D$ $\mod (D^3 + D + 1) = D^2$ $\mod (D^3 + D^2 + 1) = D + 1$
$D^4 + D^3 + D^2 + D + 1$	$\mod (D^2 + D + 1) = D + 1$ $\mod (D^3 + D + 1) = D$ $\mod (D^3 + D^2 + 1) = D^2 + 1$

Com es veu, els tres polinomis anteriors són irreductibles. Provarem si $D^4 + D + 1$ és primitiu. Si no ho fos, tampoc no ho seria el seu recíproc $(D^4 + D^3 + 1)$ i, per tant, $D^4 + D^3 + D^2 + D + 1$ hauria de ser forçosament primitiu.

Perquè $D^4 + D + 1$ sigui primitiu no ha de dividir cap polinomi de la forma $D^\lambda + 1$ per a $\lambda < 2^n - 1 = 15$. Si $\lambda < 4$, és clar que cap polinomi de la forma $D^\lambda + 1$ podrà ser múltiple de $D^4 + D + 1$.

λ	$D^\lambda+1$	mod(D^4+D+1)
4	D^4+1	D
5	D^5+1	D^2+D+1
6	D^6+1	D^3+D^2+1
7	D^7+1	D^3+D
8	D^8+1	D^2
9	D^9+1	D^3+D+1
10	$D^{10}+1$	D^2+D
11	$D^{11}+1$	D^3+D^2+D+1
12	$D^{12}+1$	D^3+D^2+D
13	$D^{13}+1$	D^3+D^2
14	$D^{14}+1$	D^3
15	$D^{15}+1$	0

Taula 3.2: Verificació del polinomi $D^4 + D + 1$

Això demostra que el polinomi D^4+D+1 és primitiu. De fet, no hauria calgut calcular tota la llista anterior, atès que els valors parells de λ fan que $D^\lambda + 1$ sigui el quadrat de $D^{\frac{\lambda}{2}} + 1$ i, per tant, si aquest no n'era múltiple, el seu quadrat tampoc no ho podria ser. Així, no calia comprovar els valors de λ igual a 4, 6, 8 10, 12 i 14.

En realitat, els únics valors que cal comprovar són els divisors de 15, que són {1,3,5,15}, per la qual cosa n'hi havia prou de comprovar el valor 5.

Si haguéssim provat amb el polinomi $D^4 + D^3 + D^2 + D + 1$, hauríem comprovat que divideix $D^5 + 1$. Això és fàcil de comprovar:

$(D^5 + 1) \mod (D^4 + D^3 + D^2 + D + 1) = 0$

$$
\begin{array}{l|l}
D^5 + 1 & D^4+D^3+D^2+D+1 \\
\cline{2-2}
D^5+D^4+D^3+D^2+D+1 & D+1 \\
\cline{1-1}
\quad D^4+D^3+D^2+D+1 & \\
\quad D^4+D^3+D^2+D+1 & \\
\cline{1-1}
\qquad\qquad 0 &
\end{array}
$$

D'aquí es dedueix que cap polinomi que estigui complet (que tingui totes les potències) pot ser primitiu, ja que, si té grau n dividirà el polinomi $D^{n+1} + 1$.

Problema 3

a) Sigui un sistema RSA amb els paràmetres següents per a un usuari A ($p = 47$, $q = 59$, $d = 157$). Per a la codificació dels missatges de text, substituïm cada lletra per un nombre de dos dígits, d'acord amb la codificació següent: espai=00, A = 01, B = 02, ..., Z = 26, i codifiquem dues lletres per bloc. Codifiqueu el missatge M = 920 per transmetre'l confidencialment a l'usuari A.

b) Feu un xifratge de Vigenère del missatge M = HOLA amb la clau obtinguda en desxifrar el criptograma generat a l'apartat anterior amb la clau privada de A.

c) El coneixement de la funció d'Euler $\phi(n)$ permet factoritzar n en un sistema RSA. Factoritzeu $n = p \cdot q = 2782799$, sabent que $\phi(n) = 2779440$. AJUDA: Obtingueu $p+q$ com una determinada funció de n i $\phi(n)$. Feu servir la identitat $(p-q)^2 = (p+q)^2 - 4 \cdot p \cdot q$.

Solució

a) $p = 47; q = 59$
$n = p \cdot q = 47 \cdot 59 = 2.773$
$d = 157, \phi(2.773) = 46 \cdot 58 = 2.668$
$e = 17$
Espai en blanc = 00
A = 01, B = 02, ..., I = 09, T = 20, M = 920,
$C = M^{17} \mod n = 920^{17} \mod 2.773 = 948$

NOTA: Aquest exemple numèric el van presentar l'any 1977 Rivest, Shamir i Adleman a l'article original en què van presentar l'algoritme RSA.

b) $c_i = n_i + k_{i \mod d} \mod 27$

En aquest cas, la longitud de la clau és $d = 2$.

C=QHUU

H	O	L	A		8	15	12	1
I	T	I	T		9	20	9	20
					17	35	21	21 mod 27

0	1	2	3	4	5				10				15				20				25
_	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

c) $N = 1.879 \cdot 1.481 = 2.782.799$

$\phi(n) = 1.878 \cdot 1.480 = 2.779.440$

Factoritza N.

$p + q = n - \phi(n) + 1 = 3.360$

$p - q = \sqrt{(p+q)^2 - 4 \cdot p \cdot q} = \sqrt{(3.660)^2 - 4 \cdot 2.782.799} = 398$

$2 \cdot p = (p+q) + (p-q) = 3.758 \Rightarrow p = 1.879, \quad q = 1.481$

Això també apareixia a l'article de Rivest, Shamir i Adleman.

Problema 4

Sigui $H(M)$, amb una sortida de k bits, que es calcula de la manera següent:

1) Al final del missatge s'afegeix el nombre de zeros necessaris perquè la longitud del missatge sigui múltiple de k.
2) El missatge es divideix en n blocs de k bits, m_i $0 \leq i \leq n-1$.
3) $H(M)$ es calcula iterativament de la manera següent:

$$h_0 = m_0$$

$$h_{i+1} = h_i + m_{i+1} \; 0 \leq i \leq n-2 \text{ (XOR bit a bit)}$$

$$H(M) = h_{n-1}$$

a) Indiqueu les propietats que ha de complir una funció de *hash* criptogràficament robusta, i digueu quines d'elles compleixen la funció proposada.

b) Sigui el missatge M = 10101010101010101010. Calculeu $H(M)$ per a $k = 6$.

c) Sigui un sistema de RSA en què tots els usuaris fan servir $e = 23$. Genereu un parell de claus RSA amb $p = 11$, $q = 13$. Indiqueu quines serien la clau privada i la pública.

d) Signeu digitalment el missatge de l'apartat *b* amb el sistema de claus generat a l'apartat *c* i la funció de *hash* proposada (considereu sempre que els bits de menys pes són els de la dreta). Indiqueu quins serveis de seguretat ofereix la signatura digital.

e) Suposeu que sou un atacant que voleu modificar un missatge signat digitalment amb el sistema anterior. Indiqueu la manera més eficient de fer-ho i genereu un missatge que genere la mateixa signatura que M.

Solució

a)

PROPIETATS	COMPLIMENT
Entrada qualsevol longitud	Sí
Sortida longitud fixa	Sí
Donat m, és fàcil de calcular $H(m)$	Sí
Donada $H(m)$, no podem trobar un m que la generi	NO
No és possible trobar dos m que generen la mateixa $H(m)$	NO

b)

$$\begin{aligned} M &= 1\ 0\ 1\ 0\ 1\ 0 \longrightarrow m_0 \\ &= 1\ 0\ 1\ 0\ 1\ 0 \longrightarrow m_1 \\ &= 1\ 0\ 1\ 0\ 1\ 0 \longrightarrow m_2 \\ &= 1\ 0\ 0\ 0\ 0\ 0 \longrightarrow m_3 \\ H(m) &= 0\ 0\ 1\ 0\ 1\ 0 = 10 \text{ (en decimal)} = m_0 + m_1 + m_2 + m_3 \end{aligned}$$

Nota: Amb la funció de *hash* definida, és molt fàcil trobar missatges que donin una funció determinada. Vegeu, per exemple, l'apartat *e* d'aquest exercici.

c) Es tracta d'un exemple clàssic de generació de claus RSA:

$N = p \cdot q = 143; P_A : e_A = 23, N_A$=143 clau pública

$ed = 1 \mod \phi(N)$ {algoritme d'Euler estès $\phi(N) = 120\} \Longrightarrow d = 47$

$S_A : d = 47$ clau privada

d) $M \| E_{SA}(H(m)) = M \| 10^{47} \mod 143 : M \| 43$

SIGNATURA $= E_{SA}(H(m)) = M^d \mod 143$

Missatge signat: 10101010101010101010101011

La signatura digital ofereix autenticació, integritat i suport contra el repudi.

e) La forma més eficient és generar un missatge que generi la mateixa $H(m)$.

Per exemple: m' =0 0 1 0 1 0

m' pot suplantar m.

Hi ha moltes altres possibilitats de generar fàcilment un altre m'' tal que $H(m'') = H(m)$. Per exemple, afegint al missatge dos blocs de k bits iguals, o blocs de zeros.

Problema 5

Un sistema de votació des de terminals mòbils fa servir l'algoritme RSA per proporcionar el servei de verificabilitat a l'aplicació. En aquest sistema, cada terminal mòbil disposa d'una clau RSA secreta K_s que es fa servir per signar la concatenació del missatge m i el resum r. La concatenació és un valor v de 7 bits que s'obté amb la unió dels quatre bits del missatge i els tres bits del resum, de major a menor pes ($v = 0\,x\ m_3\ m_2\ m_1\ m_0\ r_2\ r_1\ r_0$). Per determinar el valor del resum r, es fa servir un LFSR amb un estat inicial nul i un polinomi de connexions $1 + D + D^3$, el qual es nodreix amb els bits del missatge, començant amb el que pesa més. Tan bon punt s'ha operat en el LFSR amb tots els bits del missatge, el resum se deriva directament del polinomi d'estat del LFSR, com es mostra a la figura.

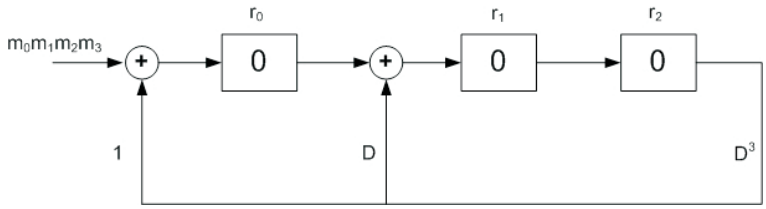


Fig. 3.4: Generació d'una funció resum mitjançant LFSR

Tenint en compte que en un terminal:

$K_s = (d, n) = (7,\ 221) \quad m = 14\ (0\text{x}1110)$

a) Calculeu la clau pública $K_p = (e,\ n)$ associada al terminal.

b) Trobeu el valor del resum en binari.

c) Especifiqueu el valor concatenat v en decimal. Determineu el resultat de la signatura de v.

d) Indiqueu quants bits són necessaris per enviar qualsevol possible valor de la signatura de v. Raoneu la resposta.

e) A partir de l'expressió polinòmica per al càlcul iteratiu de l'estat d'un LFSR, i amb un polinomi $M(D)$ de grau $n - 1$ com a alimentació externa, obtingueu la relació del polinomi d'estat en la iteració n, $P^n(D)$, amb el seu valor inicial $P^0(D)$ i amb el polinomi $M(D)$.

f) Particularitzeu l'expressió anterior per al cas en què l'estat inicial del LFSR sigui nul i el valor de $M(D)$ sigui $D^7 + D^6 + D^5 + D^4 + D^2 + 1$.

Solució

$k_s = (7, 221), \quad n = 13 \cdot 7 = p \cdot q = 221 \quad m = 14, \quad d = 7, \quad e = ?$

a) $K_p = (e, n)$

$d \cdot e = 1 \mod \phi(n)$

$\phi(n) = (p-1)(q-1) = 192$

$d \cdot e = 1 + K \cdot \phi(n)$

S'obté que $e = 55$ i $k = 2$ verifiquen l'equació $\Longrightarrow K_p = (55, 221)$

b) Càlcul del resum

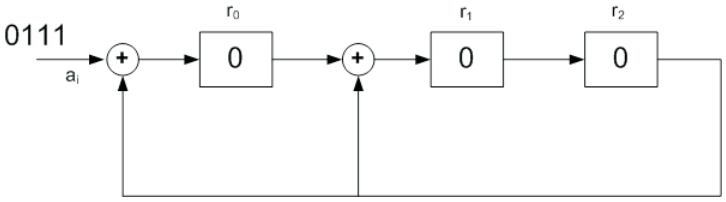


Fig. 3.5: Generació de la funció resum

r =0x101

i	a_i	r_0	r_1	r_2	$P^i(D)$
0		0	0	0	0
1	1	1	0	0	1
2	1	1	1	0	D+1
3	1	1	1	1	D^2+D+1
4	0	1	0	1	D^2+D

Taula 3.3: Càlcul de la funció resum

c) v =0x1110101=117 $f = v^d \mod n = 117^7 \mod 221 = 195$

d) Com que f es redueix modularment per n, es necessiten tants bits com calgui per codificar el valor $n-1$. En aquest cas, $n - 1 = 220$, que requereix vuit bits:

$f = 195 = \text{C3h} = \text{0x11000011}$

e) Suposant $M(D) = m_{n-1} \cdot D^{n-1} + m_{n-2} \cdot D^{n-2} + \cdots + m_0$

Expressió polinòmica per al càlcul iteratiu del LFSR:

$P^n(D) = D \cdot P^{n-1}(D) \mod C(D)$

En el nostre cas, cada iteració i dona com a resultat:

$P^1(D) = D \cdot P^0(D) \mod C(D) + m_{n-1} = (D \cdot P^0(D) + m_{n-1}) \mod C(D)$
$P^2(D) = D \cdot P^1(D) \mod C(D) + m_{n-2} = (D \cdot (D \cdot P^0(D) + m_{n-1}) + m_{n-2}) \mod C(D)$
$P^2(D) = (D^2 \cdot P^0(D) + m_{n-1} \cdot D + m_{n-2}) \mod C(D)$

Després de n iteracions, s'obtindrà:

$$P^n(D) = (D^n P^0(D) + m_{n-1}D^{n-1} + m_{n-2}D^{n-2} + \cdots + m_0) \mod C(D)$$

Agrupant:

$$P^n(D) = (D^n P^0(D) + M(D)) \mod C(D)$$

d) $P^0(D) = 0$

$M(D) = D^7 + D^6 + D^5 + D^4 + D^2 + 1$

$P^8(D) = M(D) \mod C(D)$

$D^7+D^6+D^5+D^4+D^2+1 \quad | \; D^3+D+1$
$D^7+\quad +D^5+D^4 \quad\quad D^4+D^3+D+1$
$/\;\; D^6+\;/\;+\;/+D^2+1$
$D^6+D^4+D^3$
$/\;+D^4+D^3+D^2+1$
$D^4\quad +D^2+D$
$/\quad D^3+\;/\;+D+1$
0

$M(D)$ és múltiple de $C(D)$.

Problema 6

Sigui un sistema de RSA en què la clau pública de l'usuari B val ($N = 7.663$, $e = 4.831$). Feu servir la taula adjunta quan ho considereu necessari:

a) Calculeu $X = 397^{1982} \mod 991$. Justifiqueu com heu fet el càlcul.

b) Descodifiqueu el criptograma $C = 000000000101$, enviat per l'usuari A a l'usuari B.

c) Xifreu el missatge $M = 222$ amb la seqüència generada per un LFSR caracteritzat pel polinomi primitiu $C(D) = D^7 + D + 1$. La clau de sessió determina l'estat inicial del LFSR (en aquest cas, $S(D) = D+1$). Indiqueu possibles febleses

d'aquest xifrador en flux síncron, com també la longitud màxima del missatge que es podria xifrar amb una mateixa clau de sessió.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233
239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337
347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557
563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653
659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	883
887	907	911	919	929	937	941	947	953	967	971	977	983	991	997		

Taula 3.4: Llista dels nombres primers menors de 1.000

Solució

a) A la taula adjunta, s'observa que 991 és un nombre primer. Per tant, $\phi(991) = 990$. Hi apliquem la propietat:

$M^{k\cdot\phi(N)} \mod N = 1 \quad \text{si } mcd(M, N) = 1$

Calculem $1.982 = 2 \cdot 990 + 2$

$X = 397^{1982}$
991 primer $\Longrightarrow \phi(991) = 990$
mcd (397, 991)=1 $\Longrightarrow 397^{\phi(991)} \mod 991 = 1$
$397^{k\cdot 990} \mod 991 = 1$
$397^{1982} \mod 991 = 397^{2\cdot 990} \cdot 397^2 \mod 991 = 397^2 \mod 991 = 40 = X$

Observeu que el càlcul directe mitjançant el mètode del camperol rus[1] resulta molt feixuc, de manera que és millor aplicar les propietats de la funció d'Euler.

b) Fem servir la taula de primers per factoritzar N (provant). Després, tenim un problema clàssic de RSA.

$N = 7663 = 79 \cdot 97$ (taula de primers), $\phi(N) = 78 \cdot 96 = 7488$
$e = 4831 \implies d = e^{-1} \mod \phi(N) = 31$ (algoritme d'Euclides estès)
$M = C^d \mod N = 5^{31} \mod 7.663 = 7.476$ (en binari): M=1110100110100

c) Criptograma=sortida + missatge

[1] Algoritme de multiplicació per duplicació que tan sols requereix sumar i fer meitats. Consisteix a descompondre nombres en potències de dos i aprofitar que la multiplicació és distributiva, de manera que una operació de resultat molt gran es transforma en diverses operacions de resultat menor.

Sortida:	0	0	0	0	0	1	1	0
Missatge:	1	1	0	1	1	1	1	0
Criptograma:	1	1	0	1	1	0	0	0

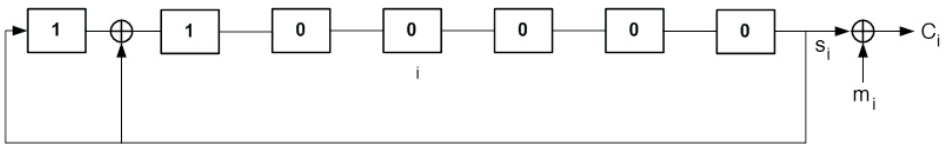


Fig. 3.6: Esquema del xifrador de flux

El xifrador de flux està format només per una estructura lineal. Per això, la criptoanàlisi no ha de ser complicada. D'altra banda, en ser el polinomi primitiu:

$L_{\text{màx}} = 2^N - 1 = 2^7 - 1 = 127$
Longitud màxima: $L_{\text{màx}} = 127$
Longitud del text < Long. màx

Problema 7

En un sistema simple de clau pública RSA, s'utilitza una entitat de certificació (*EC*) per obtenir les claus públiques de les entitats que hi intervenen. Aquest sistema fa servir a totes les claus públiques el mateix valor $e = 11$, de manera que les claus es redueixen a un únic valor n. S'ha esbrinat que en aquest sistema totes les claus públiques tenen un mateix factor primer i que la funció resum utilitzada és una reducció modular en un cos commutatiu. Sabent que la clau pública de la *EC* és $K_{P_{EC}} = 9.263$ i que un certificat d'una entitat A té per valor $K_{P_A}|F(R[K_{P_A}]) = 5.959|4.811$:

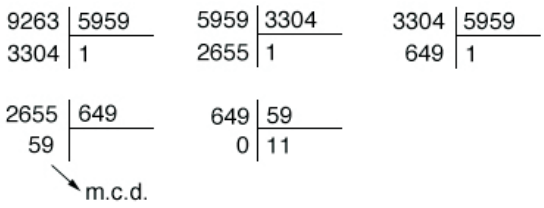
a) Trobeu la clau secreta ($K_{S_{EC}}$) de la *EC*.
b) Calculeu el resum d'una clau que inclogui el factor primer 127.
c) Trobeu la clau pública de valor mínim en aquest sistema que tingui la mateixa signatura que la clau anterior. Raoneu la validesa de la funció resum utilitzada.

Solució

Es determina el factor primer comú:

$$\begin{aligned} K_{P_{EC}} &= 9.263 = p \cdot q \\ K_{P_A} &= 5.959 = p \cdot q' \end{aligned} \qquad \text{m.c.d.}(K_{P_{EC}}, K_{P_A}) = p$$

Algoritme d'Euclides:



llavors $p = 59$ $\begin{cases} K_{P_{EC}} = 9.263 = 59 \cdot 151 \\ K_{P_A} = 5.954 = 59 \cdot 101 \end{cases}$

a) Derivem la $K_{P_{EC}}$:

$e \cdot d = 1 + k\,\Phi(K_{P_{EC}})$

$\Phi(K_{P_{EC}}) = 58 \cdot 156 = 9.048$

$11d = 1 + k\,9.048$

$K_1\,9.048 + K_2\,11 = 1$

Algoritme d'Euclides estès:

$9.048 \cdot 1 + 11 \cdot 0 = 9.048$

$9048 \cdot 0 + 11 \cdot 1 = 11 \quad (-822)$

$9.048 \cdot 1 + 11 \cdot (-822) = 6 \quad (-1)$

$9.048 \cdot (-1) + 11 \cdot (1 + 822) = 5 \quad (-1)$

$9.048 \cdot (1 + 1) + 11 \cdot (-822 - 823) = 1$

$9.048 \cdot 2 + 11 \cdot (-1645) = 1$

$K_2 = -1.645 \Rightarrow d = K_2 \mod 9.048 = 7.403$

$K_{S_{EC}}(d, n) = (7.403, 9.263)$

b) Operació modular realitzada:

$r = K_{S_A} \mod m$

Signatura obtinguda:

$f = E_{K_{S_{EC}}}(r) = 5.811 \Rightarrow r = D_{K_{S_{EC}}}(f)$

$r = 5.811^e \mod n = 4.811^{11} \mod 9.263 = 7$

S'ha de verificar: $5.959 \mod m = 7$ on m és un primer en treballar en un cos commutatiu.

De manera equivalent:

$5.959 = 7 + km$
$5.952 = km$

Trobem els factors primers de 5.952 i identifiquem:

$$5.952 = 2^6 \cdot 3 \cdot 31 = k\,m \Rightarrow \begin{cases} m = 31 \\ k = 2^6 \cdot 3 \end{cases}$$

$m = 31$ perquè ha de ser primer i $m > 7$. Per tant, l' operació resum és:

$r = K_p \bmod 31$
Per a una clau $K_p = 127 \cdot 59 = 7.493$ el resum serà, $r = 7.493 \bmod 31 = 22$

c) La K_p mínima que verifica:

$r = K_p \bmod 31 = 22$ s'obté provant factors primers q petits. Amb $q = 3$, tenim:

$K_p 59 \cdot 3 = 177$ y $r = K_p \bmod 31 = 22$

Una altra manera: $(59 \cdot q) \bmod 31 = 22 \Rightarrow 59q + 31k = ?$

$59 \cdot 10 - 31 \cdot 19 = 1$ Euclides estès

$59 \cdot 220 - 31 \cdot 418 = 22$ Multiplicat per 22

$59 \cdot 31 - 31 \cdot 59 = 0$ Equació trivial

Combinat les dues darreres equacions:

$59(220 - K_1\,31) - 31(418 - K_1\,49) = 22$

Es busca el valor primer més petit de q que compleixi:

$220 - K_1 31 = q \Rightarrow q = 3$ amb $K_1 = 7$

Problema 8

Es vol fer una comunicació d'una entitat A a una altra entitat B, de manera que els serveis de seguretat dissenyats garanteixin la integritat del missatge, l'autoria del missatge i la confidencialitat de la transmissió. Per proporcionar aquests serveis, les entitats A i B disposen cadascuna d'una clau secreta (K_{SA} i K_{SB}) i una clau pública (K_{PA} i K_{PB}) corresponents a l'algoritme RSA.

La informació generada per l'entitat A és un bloc de set bits el valor del qual és 1110110b (76h). La integritat d'aquesta informació es garanteix amb una funció resum de cinc bits el resultat de la qual per al valor de la informació esmentat és 01111b (Fh). La signatura digital es fa amb cinc bits a partir del valor obtingut a la funció resum.

El missatge del qual s'ha de garantir la confidencialitat en el canal de comunicacions disposarà de dotze bits. Els cinc bits de més pes es corresponen amb els cinc bits que resulten de la signatura digital i els set de menys pes, amb els set de la informació.

a) Tenint en compte: $K_{PA} = (e, n) = (17, 33)$; $K_{SA} = (d, n) = (13, 33)$

I) Determineu el valor de la signatura digital.

II) Expresseu en hexadecimal i en decimal el missatge de dotze bits compost per A.

III) Demostreu que l'elecció realitzada de les claus K_{PA} i K_{SA} permet que la signatura digital sigui de tan sols cinc bits.

b) Sabent que els paràmetres elegits per l'entitat B per calcular la seva clau pública K_{PB} i la seva clau secreta K_{SB} són:

$p = 59,\ q = 83,\ e = 11$

I) Raoneu per què e té un valor adequat, tenint en compte els valors de p i q elegits.

II) Trobeu la clau secreta $K_{SB} = (d, n)$.

III) Calculeu quin és el criptograma enviat per l'entitat A a l'entitat B. Expresseu-ne el valor en hexadecimal.

IV) Comenteu quin és el nombre de bits que s'ha d'assignar a un criptograma en aquest sistema, d'acord amb les claus elegides.

Solució

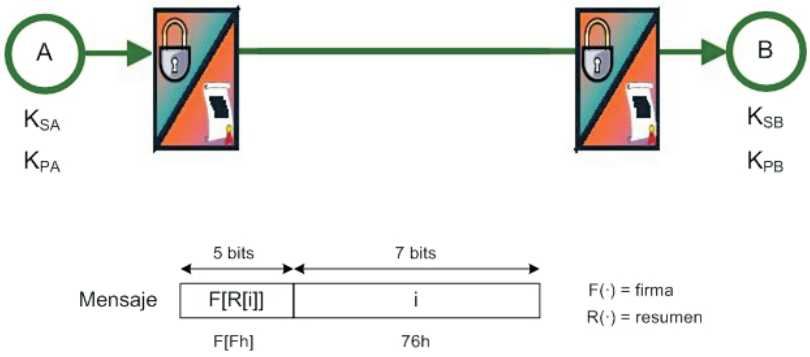


Fig. 3.7: Esquema criptogràfic i generació de la funció resum (*hash*)

a) $K_{PA} = (e, n) = (17, 33),\ K_{SA} = (d, n) = (13, 33)$

I) $F(Fh) = 15^{13} \mod 33$

$13 = 1.101_2$

$15^{13} = 15^{2^3+2^2+0\cdot 2^1+1} = \left((15^2 \cdot 15)^2\right)^2 \cdot 15$

$F(Fh) = 9 = 1.001_2$

II) $M = 10011110110_2$

$M = 4F6h$

$M = 1.270$

III) Si $n = 33$, les firmes podran tenir fins a sis bits ja que, segons el RSA:

$c = m^e \mod n < n$

Per tal que els xifratges de valors de cinc bits requereixin només cinc bits, cal que els xifratges de valors de sis bits donin lloc a valors de sis bits. Així,

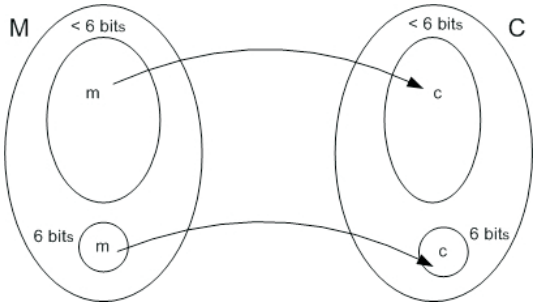


Fig. 3.8: Funció resum

En el nostre cas, l'únic missatge de sis bits és $m = 32$. Llavors, si es verifica:

$32 = 32^e \mod n$ o $32 = 32^d \mod n$, aquesta hipòtesi serà certa.

El nostre cas compleix que un xifratge de cinc o menys bits dona lloc a un resultat de cinc o menys bits.

En aquest cas: $32^{13} \mod 32 = \left((32^2 \cdot 32)^2\right)^2 \cdot 32 \mod 33 = 32$

b) K_{PB}, K_{SB} a partir de $p = 54$, $q = 83$, $e = 11$

I) m.c.d.$(e, \phi(n)) = 1$; per tant, es verifica que e i $\phi(n)$ són coprimers:

$\phi(n) = (p - 1) \cdot (q - 1) = 4.756 = 2^2 \cdot 29 \cdot 41$

$e = 11$ m.c.d.$(\phi(n), e) = 1$

II) $K_{PB} = (e, n) = (11, 4.897)$

$K_{SB} = (d, n) = (d, 4.897)$

A RSA, s'ha de verificar

$e \cdot d = 1 + k \cdot \phi(n) \implies d = e^{-1}$ en $\mathbb{Z}_{\phi(n)}$

Utilitzant l'algoritme d'Euclides estès:

$K_1 \cdot \phi(n) + K_2 \cdot e = 1 \implies K_2 = d = 3.459$

III) $C = m^e \mod n,\ K_{PB} = (e, n) = (11, 4.897)$

$C = 1.270^{11} \mod 4.897 = 4.104 = 1.008h$

IV) Per codificar n, necessitem tretze bits:

$n = 4.897 = 1.321h$

Com que hi ha valors de menys de tretze bits que donen lloc a criptogrames de tretze bits, hem d'assignar tretze bits per a l'enviament del criptograma.

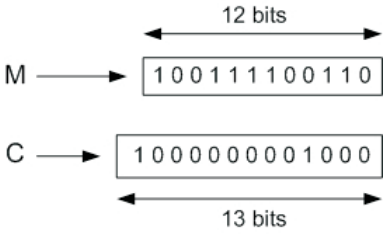


Fig. 3.9: Nombre de bits per assignar criptograma

Problema 9

Un sistema de signatures digitals utilitza RSA i, com a funció resum, l'algoritme anomenat El Gamal. Aquest algoritme manté un valor x en secret, que l'entitat signant ha de custodiar de la mateixa manera que la clau secreta K_s^{RSA}. La verificació de la signatura d'un missatge m es fa utilitzant la clau pública K_p^{RSA} junt amb una terna (g, y, p) que facilita la comprovació del missatge rebut d'acord amb el resum. En aquest sistema, caldrà que es facin públiques les claus K_p^{RSA} i les ternes (g, y, p) associades a cada entitat signant. Considereu que el resum r es concatena a continuació del missatge m de la forma $m|r$.

Completeu el càlcul i la validació del resum obtingut amb l'algoritme El Gamal que s'exposa, amb els passos següents:

1. Es determina un nombre primer $p = 23$ i dos nombres aleatoris $g = 15$ i $x = 2$.
2. Es deriva un valor y de la manera següent: $y = g^x \mod p$

   a) Determineu el valor de y.
3. Per trobar el resum r d'un missatge $m = 6$, es genera un nombre aleatori, coprimer amb $p - 1$, de valor $z = 3$. A partir d'aquest nombre, es deriva una primera part del resum, anomenada a, mitjançant l'expressió: $a = g^z \mod p$

   b) Calculeu el valor de a.

4. Es determina un valor auxiliar b', que és l'element invers de z a l'anell Z_{p-1}

   c) Trobeu el valor de b'.

5. El càlcul del resum es completa amb un valor b a Z_{p-1}, que verifica:

   $m = (x \cdot a + z \cdot b) \mod (p-1)$

   d) Trobeu el valor de b.

6. Es forma el resum amb la concatenació dels dos valors anteriors, $r = a|b$.

7. La comprovació d'un missatge m es fa en el receptor amb el resum r associat, verificant la igualtat: $y^a \cdot a^b = g^m \mod p$

   e) Comproveu que els càlculs anteriors han estat correctes, utilitzant el mecanisme de comprovació de l'algoritme.
   f) Escriviu gràficament el procediment de signatura que han seguit l'emissor i el receptor.
   g) Raoneu breument la validesa de la funció resum proposada.

Solució

- Es genera un nombre primer, $p = 23$.
- Es troben dos nombres aleatoris, $g = 15$ i $x = 2$.
- Es deriva: $y = g^x \mod p$

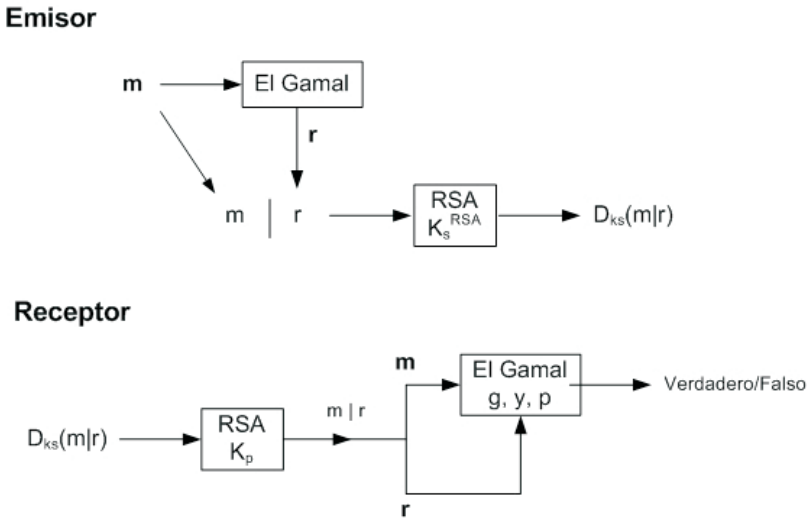


Fig. 3.10: Esquema del sistema de generació/verificació de signatura

a) Determinem la signatura pública (g, y, p): $y = 15^2 \mod 23 = 18$

- Missatge $m = 6$.
- S'obté un aleatori $z = 3$ coprimer amb $p - 1 = 22$.

- Es deriva un valor: $a = g^z \mod p$
- Es troba $b \in z_{p-1}$, que verifica: $m = (x \cdot a + z \cdot b) \mod p - 1$

b) Calculem a: $a = 15^3 \mod 23 = 17$

c) Trobem b' tal que $1 = z \cdot b' \mod p - 1$. De manera equivalent:

$$1 = z \cdot b' + k \cdot (p - 1)$$

$$1 = 3 \cdot b' + 22 \cdot k \implies \begin{cases} k = 1 \\ b' = -7 \equiv 15 \mod 22 \end{cases}$$

d) Atès que $b = (m - x \cdot a) \cdot b' \mod p - 1$, llavors: $b = (6 - 2 \cdot 17) \cdot 15 \mod 22 = 20$

e) $r = a|b = 17|20$

Comprovació: Si es verifica $y^a\, a^b = g^m \mod p$, el resum és correcte.

f) Comprovació:

$$y^a\, a^b = g^m \mod p$$

$$18^{17} \cdot 17^{20} = 15^6 \mod 23$$

$$18^{17} = 18^{10001_2} = ((18^2)^2)^2 \cdot 18 \equiv 8 \mod 23$$

$$17^{20} = 17^{10100_2} = (((17^2)^2 \cdot 17)^2)^2 \equiv 16 \mod 23$$

Es verifica:

$$\left.\begin{aligned} y^a \cdot a^b &= 8 \cdot 16 \mod 23 = 13 \\ g^m &\equiv 15^6 \mod 23 = 13 \end{aligned}\right\} OK$$

g) Validesa de la funció resum proposada:

- El resum és de longitud fixa, amb un valor de bits necessari per concatenar $a|b$.
- Donat m, és fàcil calcular r, encara que l'exponenciació utilitzada pot ser computacionalment lenta en alguns casos.
- Donat r, és impossible a la pràctica trobar m si no es coneix x.
- És poc probable que dos missatges, m i m', donin lloc al mateix r. Es pot controlar la probabilitat en funció de la mida de m màxim i del valor de p.
- Donat un m, és pràcticament impossible trobar-ne un altre m' que compleixi $r(m) = r(m')$ si no es coneix x.

Problema 10

Es vol fer un xifrador bloc de quatre bits mitjançant un LFSR de longitud 4. Per a això, es carrega com a estat del LFSR el quartet de bits per xifrar i es fa evolucionar **k** cicles, i l'estat que en resulta és el valor del quartet xifrat. Com a polinomi de connexions, s'utilitza un valor **C(D)** fix per a tots els valors de **k**.

Es demana:

a) Si **C(D)** és primitiu, quin és el nombre de claus diferents?

b) Para **k**=4, el xifratge de [0 0 0 1] (a totes les ternes, el pes més gran es troba a l'esquerra) és [0 0 1 1]. Quant val **C(D)**?

c) Per a **k**=7, quant val el xifratge de [0 0 0 1]?

d) Per a **k**=7, el xifratge del missatge [0 0 0 1] [0 0 0 1] [0 0 0 1] és [1 0 1 1] [0 0 1 0] [1 1 1 0]. Raoneu per què es pot assegurar que el xifratge no s'està fent servir en mode natiu o ECB.

e) Sabent que es tracta d'un xifratge CBC, quin n'és el vector inicial?

Solució

a) Vist en forma polinòmica, $\text{Cif}(M) = D^k\, M(D) \mod C(D)$. Si C(D) és primitiu, s'assoleixen tots els estats menys el 0; per tant, hi ha $2^4 - 1 = 15$ claus distintes.

b) De l'enunciat, es dedueix que, per a $k = 4$, $D^4 \cdot 1 \mod C(D) = D + 1$. Suposeu que $C(D) = D^4 + aD^3 + bD^2 + cD + 1$, on a, b i c són desconeguts. De l'equació anterior, es poden trobar plantejant la divisió:

$$\begin{array}{l|l} D^4 & D^4+aD^3+bD^2+cD+1 \\ \hline D^4+aD^3+bD^2+cD+1 & 1 \\ \hline aD^3+bD^2+cD+1 \end{array} \quad = D+1 \rightarrow a=0\,;\, b=0\,;\, c=1 \rightarrow C(D)= D^4+D+1$$

d'on es dedueix que $C(D) = D^4 + D + 1$.

c) De l'enunciat, es dedueix que, per a $k = 7$, s'ha de fer l'operació: $D^7 \cdot 1 = \mod D^4 + D + 1$. Per tant, es té:

$$D^4 \cdot D^3 = (D+1)D^3 = D^4 + D^3 = D^3 + D + 1 = [1\,0\,1\,1]$$

d) Perquè a ECB els blocs iguals provoquen xifratges iguals i, en aquest cas, no és així.

e) De l'apartat *c*, es té que, per a $k = 7$, el xifratge de [0 0 0 1] és [1 0 1 1] que constitueix el primer bloc de text clar i text xifrat de l'encadenament CBC. D'aquí es dedueix que el vector inicial ha de ser [0 0 0 0].

Problema 11

En un sistema de comunicacions sense fil, els terminals s'autentiquen fent servir un servidor central. Els terminals intercanvien entre si missatges curts de forma confidencial, utilitzant l'algoritme RSA. Atès que els terminals no disposen de claus públiques, es genera de forma dinàmica per a cada sessió, entre terminals A i B, una clau $K_{P_{AB}} = (e_{AB}, n_{AB})$, on e_{AB} és de valor constant 11 i n_{AB} és el producte de dos primers, p_{AB} i q_{AB}. Els valors d'aquests nombres primers es deriven utilitzant, per a cadascun d'ells, el mecanisme d'operació Diffie-Hellman per compartir un secret.

L'intercanvi de missatges entre els terminals A i B per a la compartició d'un secret (p_{AB} i q_{AB}) es fa utilitzant el servidor central com a intermediari. D'aquesta manera, es garanteix la identitat entre els terminals. Els missatges intercanviats s'envien del terminal al servidor de forma confidencial utilitzant la clau pública del servidor, K_{Serv}, corresponent a l'algoritme RSA. Quan el servidor rep el criptograma enviat per un terminal, el desxifra i el retransmet a l'altre terminal.

Considerant que:

1. L'operació del mecanisme Diffie-Hellman utilitza: $a = 5$ y $p = 97$.
2. Els valors aleatoris generats pels terminals per al secret compartit de cada nombre primer són:
   - p_{AB}: terminal A genera $x_1 = 2$; terminal B genera $y_1 = 5$
   - q_{AB}: terminal A genera $x_2 = 7$; terminal B genera $y_2 = 10$
3. La clau pública del servidor és $K_{\text{Serv}} = (e, n) = (3, 319)$.

Determineu:

a) El valor dels missatges xifrats amb RSA que s'envien del terminal A al servidor per a la generació de p_{AB} i q_{AB}, respectivament.

b) Els missatges enviats en clar del servidor al terminal A per a la generació de p_{AB} y q_{AB}, respectivament.

c) La clau pública $K_{P_{AB}}$ de la sessió RSA entre els terminals A i B a partir dels missatges rebuts per al terminal A i els nombres aleatoris generats per aquest terminal.

d) La clau secreta de la sessió RSA entre els terminals.

e) El criptograma enviat del terminal A al B quan el missatge en clar és 9.

Solució

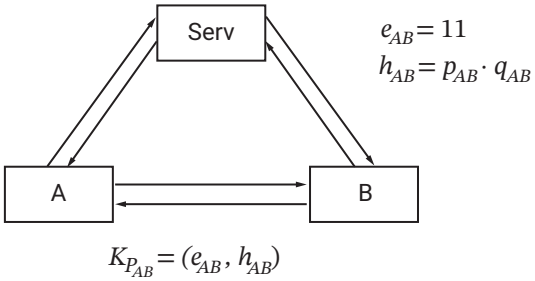


Fig. 3.11: Esquema proposat

1. Diffie-Hellman $q = 5$ y $p = 97$

2.

	p_{AB}	q_{AB}
A	$x_1 = 2$	$x_2 = 7$
B	$y_1 = 5$	$y_2 = 10$

3. $K_{\text{serv}} = (e, n) = (3, 319)$

a) Missatges xifrats RSA de A al servidor. Per a p_{AB}:

$m_1^A = a^{x_1} \mod p = 5^2 \mod 97 = 25$

Per a q_{AB}:

$m_2^A = a^{x_2} \mod p = 5^7 \mod 97 = 40$

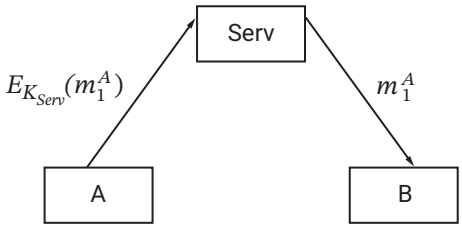


Fig. 3.12: Missatges RSA xifrats de A al servidor

Criptogrames:

$c_1^A = (m_1^A)^e \mod n = 25^3 \mod 319 = 313$

$c_2^A = (m_2^A)^e \mod n = 40^3 \mod 319 = 200$

b) Para p_{AB}.

$m_1^B = a^{y_1} \mod p = 5^5 \mod 97 = 21$

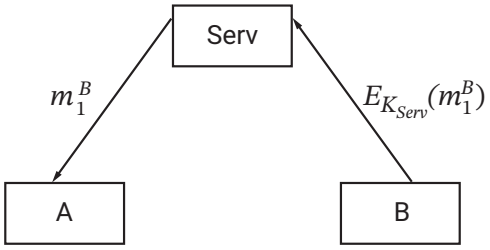


Fig. 3.13: Missatges enviats en clar del servidor al terminal A

Per a q_{AB}.

$m_2^B = a^{y_2} \mod p = 5^{10} \mod 97 = 53$

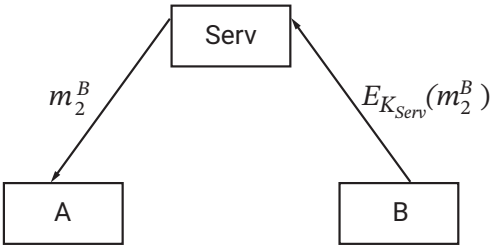


Fig. 3.14: Missatges enviats en clar del servidor al terminal A

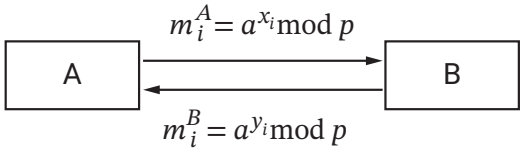


Fig. 3.15: Intercanvi Diffie-Hllman d'un secret

c) Indirectament, entre A i B s'ha fet l'intercanvi.

El secret compartit és:

$s_i = (m_i^B)^{y_i} \mod p = (m_i^B)^{x_i} \mod p = a^{x_i y_i} \mod p$

$s_1 = p_{AB} = (m_1^B)^{y_1} \mod p = 21^2 \mod 97 = 53$

$s_2 = q_{AB} = (m_2^B)^{y_2} \mod p = 53^7 \mod 97 = 3$

$n_{AB} = p_{AB} \cdot q_{AB} = 53 \cdot 3 = 159$

$K_{p_{AB}} = (e_{AB}, n_{AB}) = (11, 159)$

d) $K_s = (d, n)$

$e \cdot d + k\Phi(n) = 1$

$\Phi(n) = (p_{AB} - 1)(q_{AB} - 1) = 52 \cdot 2 = 104$

$11d + 104k = 1$

Algoritme d'Euclides estès:

1. $104 \cdot 1 + 11 \cdot 0 = 104 \qquad (104 = 11 \cdot 9 + 5)$
2. $104 \cdot 0 + 11 \cdot 1 = 11 \qquad (11 = 5 \cdot 2 + 1)$
3. $104 + (-9) \cdot 11 = 5$
4. $(-2) \cdot 104 + (1 + 18) \cdot 11 = 1$
   $k = -2$
   $d = 10 \mod 104 = 19 \quad \Rightarrow \quad K_{s_{AB}} = (19, 159)$

e) $c = m^{e_{AB}} \mod n_{AB} = 9^{11} \mod 159 = 123$

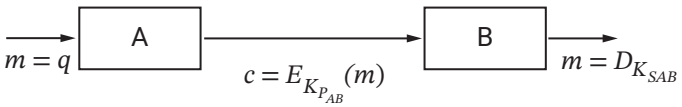


Fig. 3.16: Criptograma enviat

Problema 12

Un xifrador de flux consta d'un LFSR i una funció de sortida. Treballant en mode síncron, s'observa que la seqüència generada té un període de 2.047 bits.

a) Si el dissenyador indica que el nombre de cel·les és < 11, podem estar segurs que menteix?

b) Podríem afirmar que el nombre de cel·les és 11? Posteriorment, es configura un altre xifrador (també basat en LFSR i amb una funció de sortida) perquè operi en mode autosincronitzant. Quan s'han obtingut 2.047 bits, no s'ha trobat cap període.

c) És possible que el nombre de cel·les del LFSR sigui < 11?

Solució

a) Si el nombre de cel·les és < 11, el període seria, com a màxim, $2^{10} - 1 = 1.023$, ja que la funció de sortida no augmenta aquest període. Per tant, podem estar

segurs que, amb un nombre de cel·les ≤ 10, no es pot aconseguir aquest període. És a dir, podem garantir que el dissenyador menteix.

b) No, perquè si el nombre de cel·les és més gran i el polinomi no és primitiu, el període no serà $2^L - 1$, essent L el nombre de cel·les. És a dir, pot ser que el nombre de cel·les sigui > 11.

c) Sí, perquè, quan el xifrador treballa en mode autosincronitzant, la sortida no té per què ser periòdica, ja que en la realimentació influiran les dades de l'usuari.

Curricula

Mónica Aguilar Igartua és doctora enginyera en telecomunicació i professora titular d'universitat a la UPC des del 2001. Pertany al Grup de Recerca de Serveis Telemàtics del Departament d'Enginyeria Telemàtica. Treballa en xarxes vehiculars, serveis per a vehicle elèctric i desenvolupament d'eines per millorar la mobilitat urbana.

Jordi Forné Muñoz és catedràtic d'universitat de la UPC des del 2021. La seva recerca se centra en el camp de la seguretat i la privadesa de la informació.

Jorge Mata Díaz és doctor enginyer de Telecomunicació i professor titular d'universitat del Departament d'Enginyeria Telemàtica de la UPC des del 1997. La seva recerca se centra en l'estudi d'algorismes per a la transmissió d'informació a Internet.

Francisco Rico Novella és doctor enginyer de Telecomunicació per la UPC (1995). Des del 1997, és professor titular d'universitat adscrit a l'Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona (ETSETB). La seva recerca se centra en el camp de la criptografia, la codificació i les comunicacions de curt abast.

Alfonso Rojas Espinosa és doctor enginyer de Telecomunicació per la UPC i profesor titular d'universitat adscrit a l'ETSETB. Els seus interessos investigadors están relacionats amb la transmissió de dades.

Miquel Soriano Ibáñez és catedràtic d'universitat de la UPC des del 2007. La seva recerca se centra en la seguretat de la informació i la protecció dels drets d'autor. Ha participat i ha dirigit molts projectes finançats per l'Administració (nacional i internacional) i per empreses privades.