

TRANSMISSIÓ DE DADES

Límit de Shannon $C [\text{bits/s}] = W \log_2 (1 + \text{SNR})$

W : ample de banda canal [Hz]

$$C [\text{bits/s}] = v_m [\text{simb/s}] \cdot H [\text{bits/simb}]$$

Eficiència espectral $\epsilon = \frac{C}{W}$

2: CODIFICACIÓ DE FONT

$$H [\text{bits/simb}] = \sum_{i=1}^F p(s_i) \log_2 \frac{1}{p(s_i)}$$

$$L \geq H$$

$$L [\text{bits}] = \sum_{i=1}^F p(s_i) L s_i$$

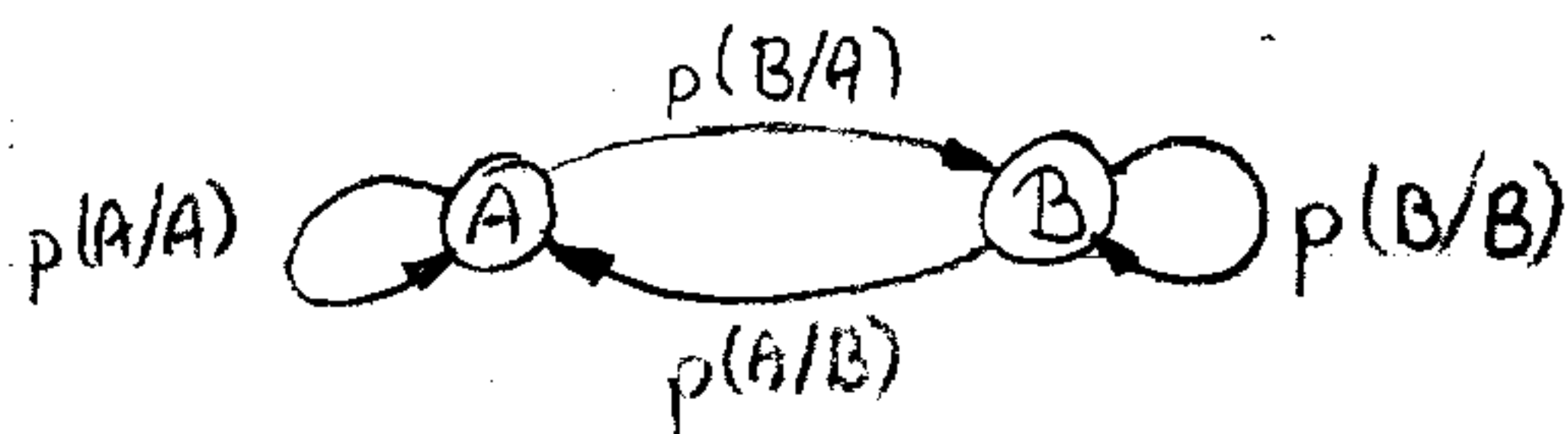
Eficiència d'un codi

$$\eta = \frac{H}{L}$$

Codi instantani: cap paraula codi és prefixe d'un altre.

Desigualtat Kraft:

$$\sum_{i=1}^F 2^{-l_i} \leq 1 \Rightarrow \exists \text{ codi instantani}$$

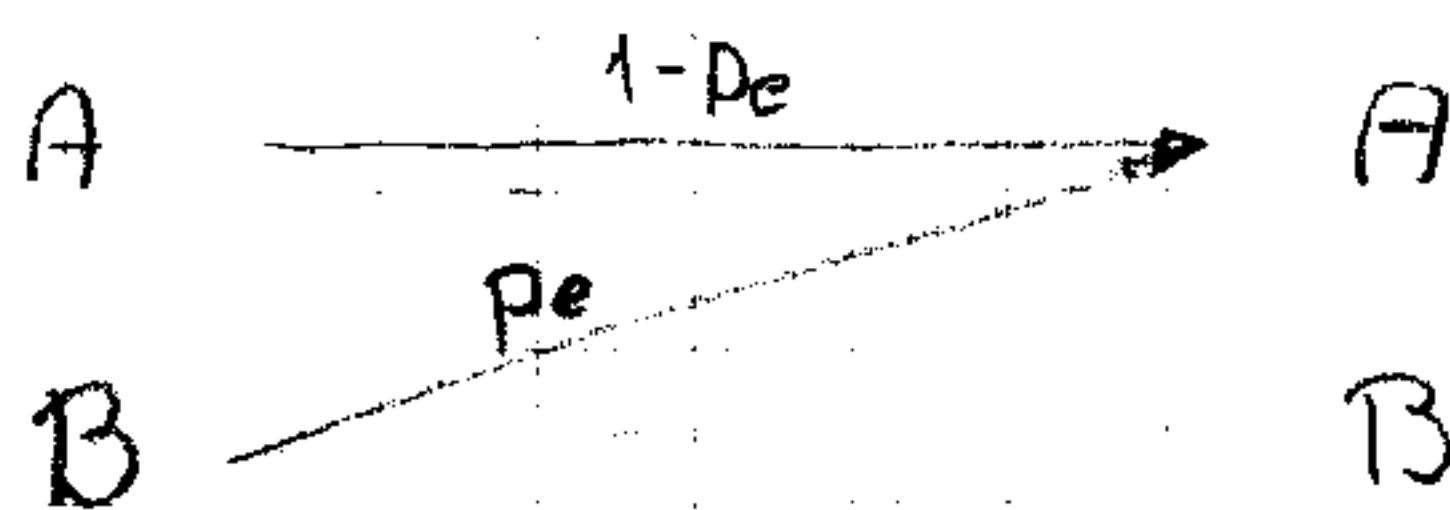
Foncs amb memòria

$$\begin{aligned} P(A) &= P(A/A)P(A) + P(A/B)P(B) \\ P(A) + P(B) &= 1 \\ P(A/A) + P(B/A) &= 1 \end{aligned}$$

$$H(F) = H(F/A)P(A) + H(F/B)P(B)$$

$$H(F/A) = \sum_{i=1}^F P(s_i/A) \log_2 \frac{1}{P(s_i/A)}$$

- Canal amb prob. d'error p_e



$$P_o(A) = P(A)(1-p_e) + P(B)p_e$$

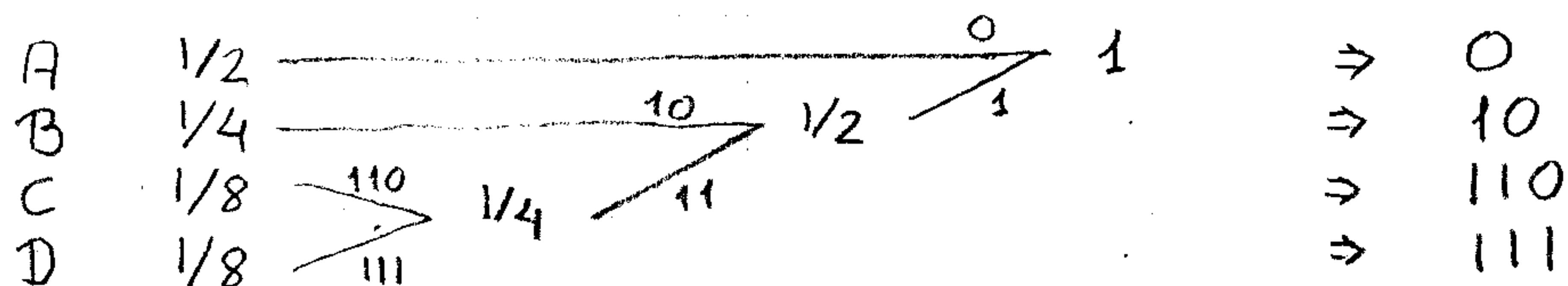
$$P_o(A/A) = P(A/A)(1-p_e) + P(B/A)p_e$$

$$H_o(F) = H_o(F/A)P(A) + H_o(F/B)P(B)$$

$$H_o(F/A) = \sum_{i=1}^F P_o(s_i/A) \log_2 \frac{1}{P_o(s_i/A)}$$

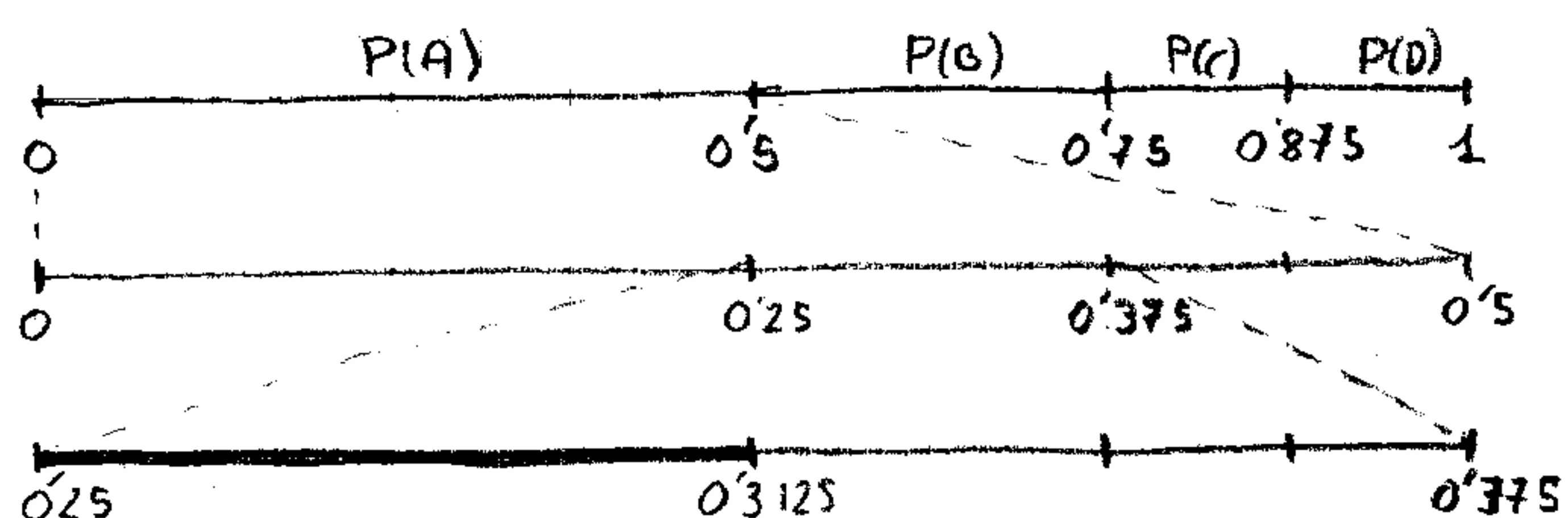
o HUFFMAN

1. - Ordenar símbolos fuente en orden decreciente probabilidad
2. - Unir dos símbolos de menor probabilidad
3. - Se construye una fuente reducida de $F-1$ elementos.
4. - Repetir hasta que queden 2 símbolos.



o CODIS ARITMÉTICS

Codificació: (Ex ABA)

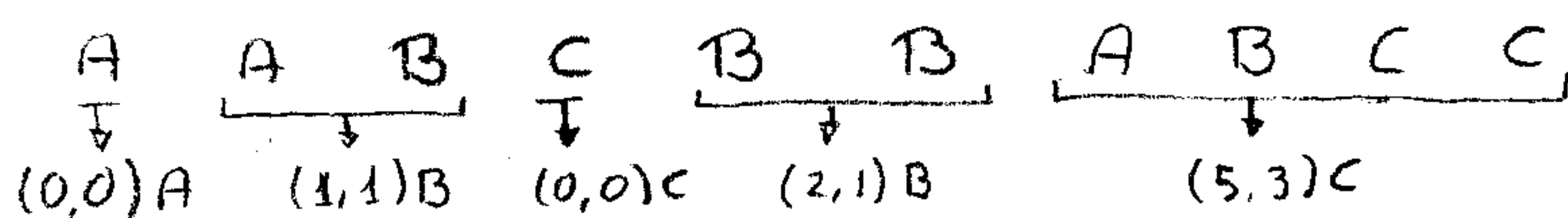


Escollim un número de l'interval $[0.25, 0.3125]$:

Descodificació

$$\begin{array}{l}
 0.3 \rightarrow \text{Interval A} \\
 \frac{0.3}{0.5} = 0.6 \rightarrow \text{Interval B} \\
 \frac{0.6 - 0.5}{0.25} = 0.4 \rightarrow \text{Interval A}
 \end{array}
 \left. \vphantom{\begin{array}{l} 0.3 \\ 0.3 \\ 0.6 - 0.5 \end{array}} \right\} \text{ABA}$$

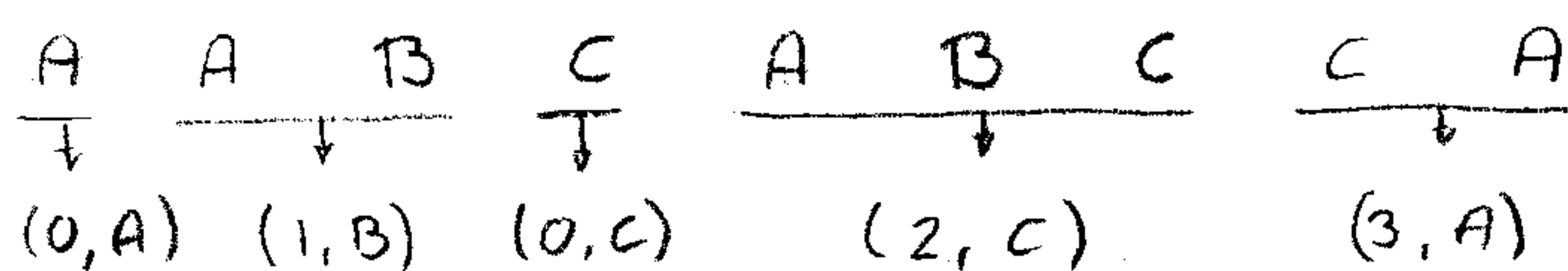
o LZ-77 (Mirem si una seqüència ja ha sortit)



(# pos anteriors, # long) nuevo

o LZ-SS (Idem però si no es eficient la codificació, s'envia el caràcter i no el punter \Rightarrow cA p(1,1)B cC p(2,1)B p(5,3)C)

o LZ-78 (Crea un diccionari amb les seq aparegudes)



Diccionari
 1: A 4: ABC
 2: AB 5: CA
 3: C 6:

o LZW (Idem amb el diccionari inicialitzat amb els caràcters, només enviem) index, no index + nou caràcter

1-3: CRIPTOGRAFIA

- Nivells de seguretat d'un algoritme criptogràfic

- Seguretat incondicional: El coneixement del criptoograma no aporta cap info sobre el missatge en clar.
- Seguretat computacional: El temps necessari per desxifrar el missatge sense tenir la clau és molt més gran que el seu temps de vida.
- Seguretat probable: No es pot demostrar que l'algoritme sigui totalment segur, però no s'ha pogut trencar.
- Seguretat condicional: L'atacant potencial no té prou medis o coneixements per trobar la clau.

- Serveis de seguretat

- Confidencialitat: La informació no és visible per a usuaris no autoritzats.
- Autenticitat: Tenim la certesa de la identitat origen.
- Integritat: Tenim la certesa que el missatge no ha sigut alterat.
- Control d'accés: Només el usuari amb els permisos corresponents podrà accedir a la informació.
- No repudi: Les entitats que participen a una comunicació no poden negar posteriorment la seva participació.

- Propietats d'un generador pseudoaleatori

- Long període seq. pseudoaleatoria $>$ long. missatge
- Estadística aleatoria.

- Postulats d'aleatorietat de Colom b

- En un període de una seq. pseudoaleatoria $|\#0 - \#1| \leq 1$
- Test de ràfegues \Rightarrow aprox. $1/2^k$ ràfegues de long k
- Autocorrelació bivaluada.

* XIFRAT SIMÈTRIC EN BLOC

- Es divideix el missatge de long. n i es xifra cada bloc.
- Dos blocs de memòria iguals generen criptogrames iguals.
- Algoritmes més emprats: DES, IDEA, AES.

Modes d'operació:

- o ECB: Electronic Code Block
- o CBC: Cipher Block Chaining
- o PBC: Plaintext Block Chaining
- o CFB: Cipher Feedback
- o OFB: Output Feedback

- DES (Data Encryption Standard)

Limitacions

- Clau 64 bits (56 útils + paritat).
amb xifrat triple 113 bits útils
- $E_{K_1}(M) = E_{\overline{K_1}}(\overline{M})$
- 4 claus febles $\Rightarrow E_K(E_K(M)) = M$
- 6 parelles de claus semifebles $\Rightarrow E_{K_1}(E_{K_2}(M)) = M$

* CRIPTOGRAFIA DE CLAU PÚBLICA

- Te Euler $a^{\phi(N)} \bmod N = 1$ si $\text{mcd}(a, N) = 1$

1. $\phi(N)$: nombre elements $i \in [1, N-1] / \text{mcd}(i, N) = 1$

2. Si N primer $\phi(N) = N-1$

- Procediment:

1.- p, q primers grans. $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

2.- Escollim una clau pública e , $\text{mcd}(e, \phi(N)) = 1$.

3.- Obtenim la clau privada $e \cdot d = 1 \bmod \phi(N)$

4.- Xifrat $\Rightarrow C = M^e \bmod N$ Desxifrat $\Rightarrow M = C^d \bmod N$

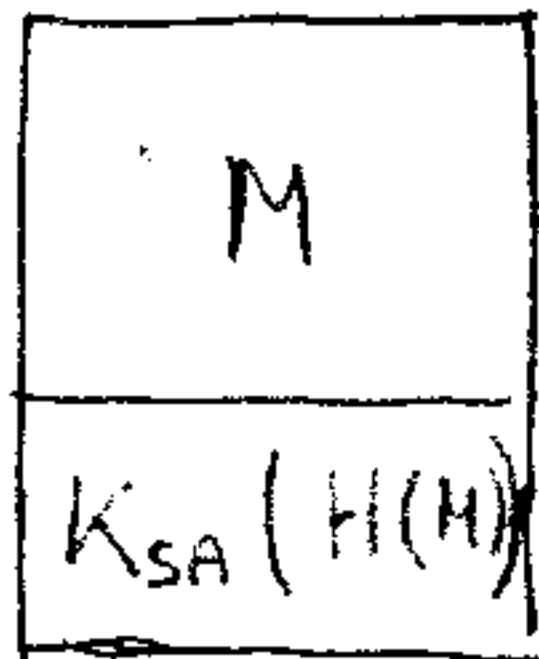
- Claus febles: # missatges que coincideixen amb el criptograma

$$\theta_{N,e} = [1 + \text{mcd}(e-1, p-1)][1 + \text{mcd}(e-1, q-1)]$$

- Mètode campesí rus \Rightarrow Ex.: $M^{25} \bmod N = M^{110016} \bmod N = M \left[\left[\left[\left[M \right]^2 \right]^2 \right]^2 \right]^2 \bmod N$
exp. dado la vuelta - 1 1 0 0 1 1

* FUNCIONS HASH

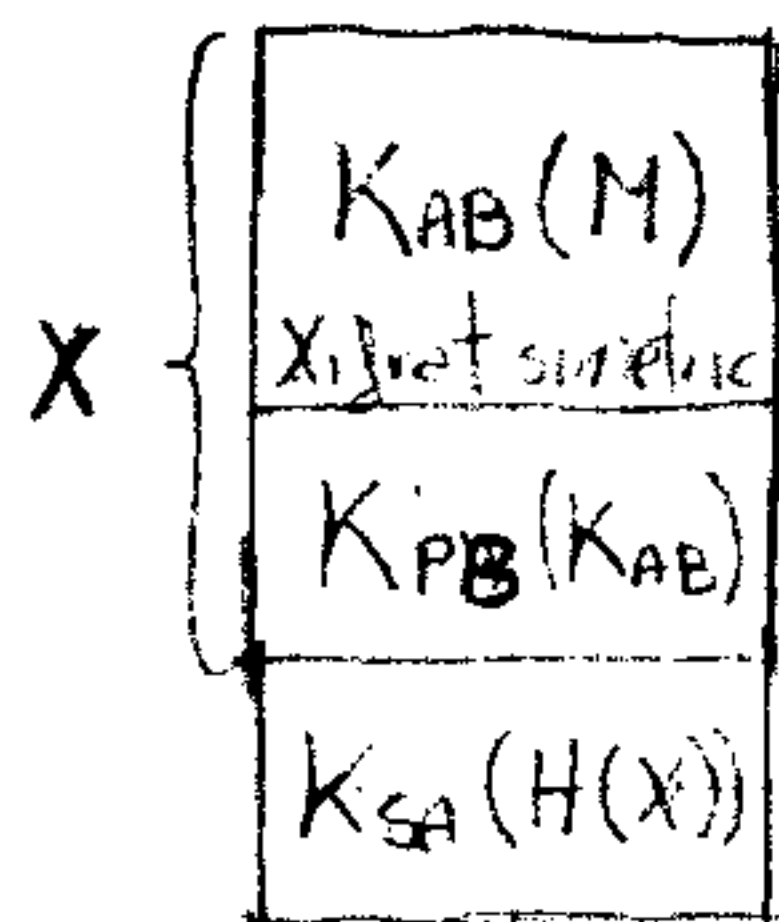
- Funcions unidireccionals que a partir d'un missatge de long. arbitrària generen una sortida de long. fixa.
- Lliure de col·lisions: es computacionalment impossible trobar dos missatges tals que $H(X) = H(Y)$
- Signature digital (de $A \rightarrow B$)



Objectius:

- Integritat
- Autenticitat d'origen

- Sobre digital (de $A \rightarrow B$)



- Confidencialitat
- Autenticitat

- Certificat digital

Nom: _____
Clau Pública: _____
Validessa desde: _____
" " fins a: _____
Algoritmes Claus: _____
Signature digital de l'autoritat certificadora

Servis per a donar a conèixer la clau pública d'un usuari de forma segura.

1-4: CODIFICACIÓ DE CANAL

* CODIFICACIÓ DE BLOC

X : missatge usuari (k simb.)
 Y : paraula codi (n simb.)
 Z : paraula rebuda (n simb.)

\hat{X} : estimació del msg (k simb.)
 r : redundància (r simb., $r = n - k$)

$$\underline{Y} = \underline{X} \cdot \underline{G}$$

\underline{G} : Matriu generadora.
Cada fila correspon a la codificació d'un vector de la base canònica del msg.

$$\underline{S} = \underline{Z} \cdot \underline{H}^T$$

\underline{H} : Matriu de comprovació

\underline{S} : Síndrome, si $\underline{S} = \underline{0} \Rightarrow \underline{Z}$ és paraula codi

- Com trobem H per codis sistemàtics?

$$\underline{G} = \left(\begin{array}{ccc|c} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{array} \right) = (\underline{I}_k | \underline{P})$$

$$\underline{H} = (-\underline{P}^T | \underline{I}_r)$$

- No pot tenir cap columna tot 0
- No pot haver dos columnes iguals

- Distància mínima d'un codi (lineal)

$$d_{\min} = \min_{\bar{Y}_k \neq \underline{0}} W_H(\bar{Y}_k)$$

$W_H(-)$: nombre components $\neq 0$

Capacitat detectora

$$\delta = d_{\min} - 1$$

Capacitat correctora

$$e = \frac{d_{\min} - 1}{2}$$

Si # errors $\leq \delta \Rightarrow$ detecto l'error

Si # errors $\leq e \Rightarrow$ puc corregir l'error

Cota de Singleton

$$r \geq \delta$$

$$r \geq 2e$$

- Prob. d'error de bloc

Prob. j errors, bloc n símbols \Rightarrow

$$P(j, n) = \binom{n}{j} p_{\text{simb}}^j (1 - p_{\text{simb}})^{n-j}$$

$$P_{\text{error bloc}} = \sum_{j=e+1}^n P(j, n)$$

- Codis perfectes

Si # errors $\leq e$ garanteix correcció.

Si # errors $> e$ sempre s'equivoca.

\Rightarrow Ha d'haver un síndrome diferent per a cada possible error.

Codis e-perfectes

$$q^r = 1 + \binom{n}{1}(q-1) + \dots + \binom{n}{e}(q-1)^e$$

q : símbols alfabet.

- Codis de Hamming

Codis binaris 1-perfectes \Rightarrow

$$2^r = 1 + n$$

$\Rightarrow k = n - r = 2^r - 1 - r$; amb $r \geq 2$

* REDUCCIÓ MODULAR POLINÒMICA

• Els elements els representem com a polinomis de coef. binaris

$$\{0, 1, \dots, 7\} \Rightarrow \{0, 1, D, D+1, D^2, D^2+1, D^2+D, D^2+D+1\}$$

$$\text{grau màxim} = \log_2(\text{tamany alfabet}) - 1$$

• Sumes de polinomis amb coef. binaris ($1+1=0$)

• Producte

Es fa multiplicar els polinomis i a continuació fent una reducció modular amb un polinomi irreduïble de grau $\log_2(\text{tamany alfabet}) \Rightarrow$ un grau superior al dels polinomis.

- Polinomis irreduïbles

• No son divisibles per cap polinomi de grau menor.

Provem si és divisible pels polinomis irreduïbles fins grau/2

• No pot tenir terme independent 0 \Rightarrow Divisible per D

• El nombre de coef. no pot ser parell \Rightarrow " " " $D+1$

• Els exponents no poden ser tots parells \Rightarrow Quadrat d'un polinomi

- Polinomis primitius

• Subconjunt dels polinomis irreduïbles

• Com a mínim hi ha un polinomi primitiu de grau m

• Si $p(D)$ primitiu el seu recíproc tb ho és

$$\text{ex } \Rightarrow p(D) = D^3 + D + 1 \rightarrow \left(\frac{1}{D^3} + \frac{1}{D} + \frac{1}{1}\right)D^3 = 1 + D^2 + D^3$$

- Propietat dels polinomis primitius ex. $p(D) = D^3 + D + 1$

D^l	1	D	D^2	D^3	D^4	D^5	D^6
$D^l \text{ mod } p(D)$	1	D	D^2	$D+1$	D^2+D	D^2+D+1	D^2+1

Apareixen tots els polinomis possibles de grau $[P(D)] - 1$

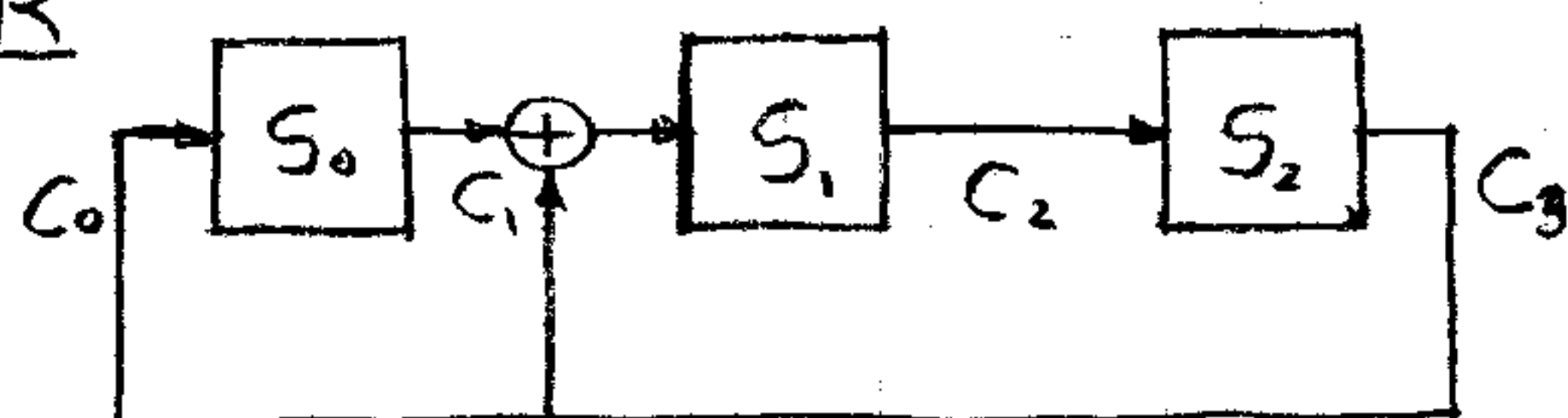
- Habitualment això s'empra per escollir \underline{H} en codis Hamming

Codi Hamming
(7,4)

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

$D^6 \quad D^5 \quad D^4 \quad D^3 \quad D^2 \quad D \quad 1$

* LSFR



$$C(D) = 1 + D + D^3$$

Pol. conexions : $C(D) = C_0 + C_1 D + C_2 D^2 + C_3 D^3$

Estat n : $S_n(D) = S_0 + S_1 D + S_2 D^2$

- Si el pol. conexions és primitiu, genera la \underline{H} d'un codi Hamming

$$S_{n+m}(D) = S_n(D) \cdot D^m \text{ mod } C(D)$$

- Periodicitat $K = 2^{\text{grau } C(D)} - 1$

- $C(D)$ divisor $D^K + 1$, No divisor $D^j + 1 \quad \forall j < K$

* CODIS POLINÒMICS I CODIS CÍCLICS

Codis cíclics :

$(y_{n-1}, y_{n-2}, \dots, y_1, y_0)$ és paraula codi
 $(y_0, y_{n-1}, y_{n-2}, \dots, y_1)$ tb ho és

Codis polinòmics = codis cíclics sistemàtics

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

$Y(D)$ múltiple pol. $g(D)$

$$R(D) = X(D)D^r \text{ mod } g(D)$$

$g(D)$ polinomi grau r

- Detecció d'errors:

△ No detectem l'error quan $e(D)$ sigui múltiple de $g(D)$

• 1 error $e(D) = 1 \cdot D^i$ (desplazament)

⇒ $g(D)$ no pot ser de la forma $p(D)D^i$ $i \geq 1$

• 2 errors $e(D) = (D^m + 1)D^i$

Si $g(D)$ primitiu, ~~no~~ garantim la detecció per $m \equiv k$ (grau $g(D)$)

• Ràjagues d'error $e(D) = (D^{m-1} + aD^{m-2} + \dots + bD + 1)D^i$

Si $m \geq r$ hi haurà situacions en que no es detecta l'error.

- Habitualment $g(D) = p(D)(D+1)$ $p(D)$ primitiu grau $r-1$

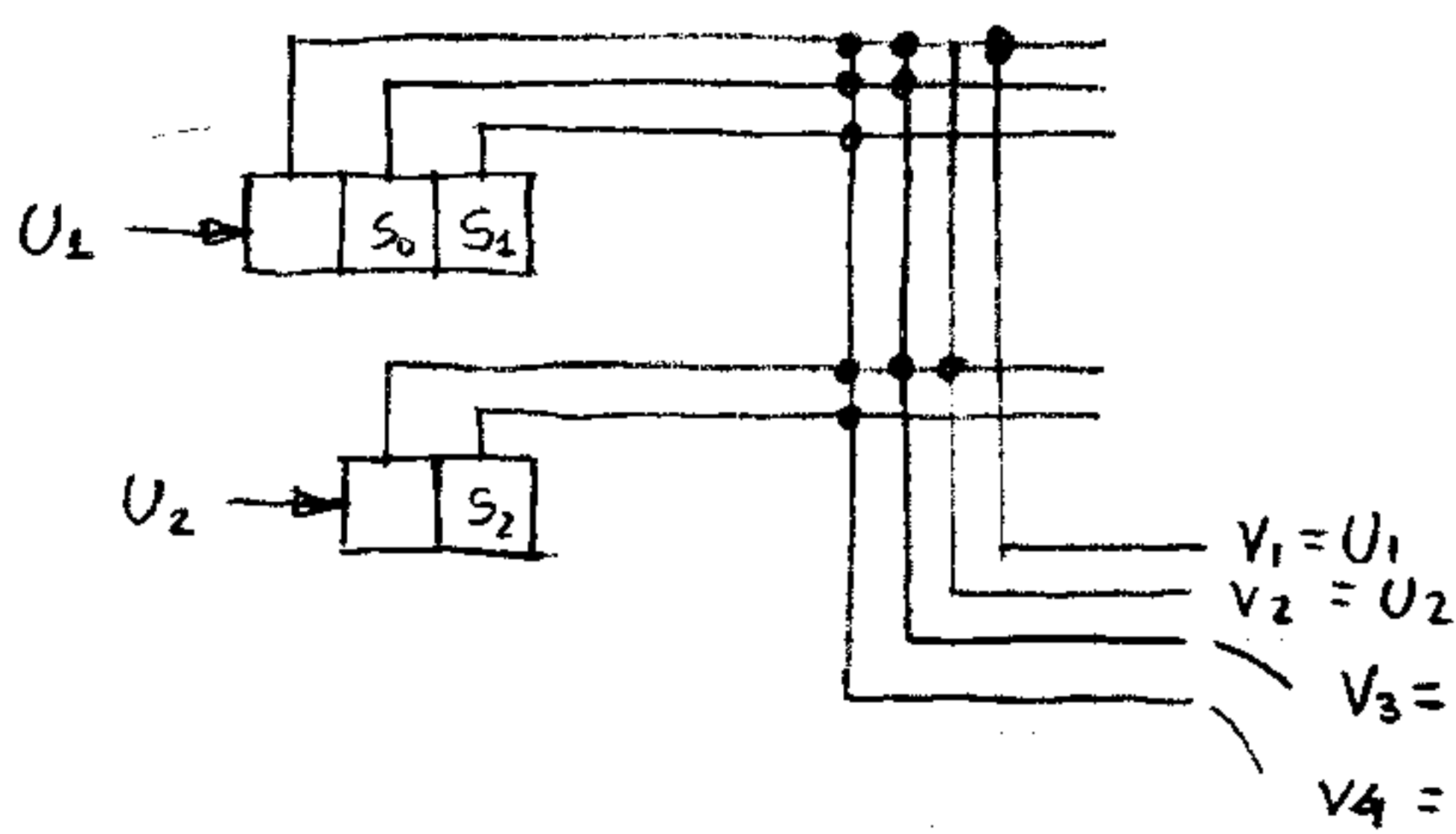
Sempre detecta un nombre senar d'errors.

* CODIS HAMMING RETALLATS

Hem de treure el mateix nombre de files i columnes d'un codi Hamming.

Ex.: $k=9 \Rightarrow H(15,11) \rightarrow H(13,9)$

* CODIS CONVOLUCIONALS



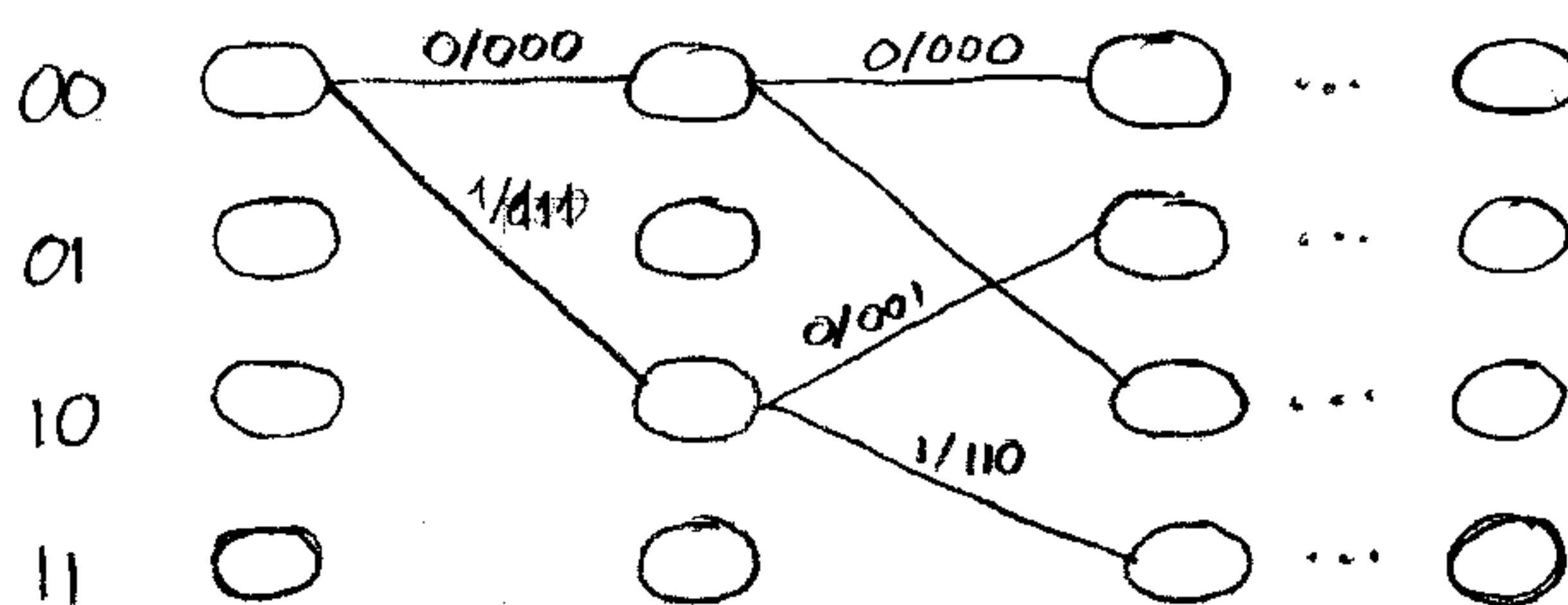
Memoria = 3

Memoria màxima = long. influència = 2

$k=2; n=4 \Rightarrow$ taxa = $1/2$

Nombre d'estats = $2^M = 8$

- Formes de representació: Diagrama d'estats, diagrama de Trellis



Distància lliure: nombre menor d'errors per tornar de nou a l'estat 00.

- Decodificació: suposem estat inicial 00, contem els error q hi hauria hagut en la transmissió per cada camí possible i seleccionem el camí amb menys errors acumulats.