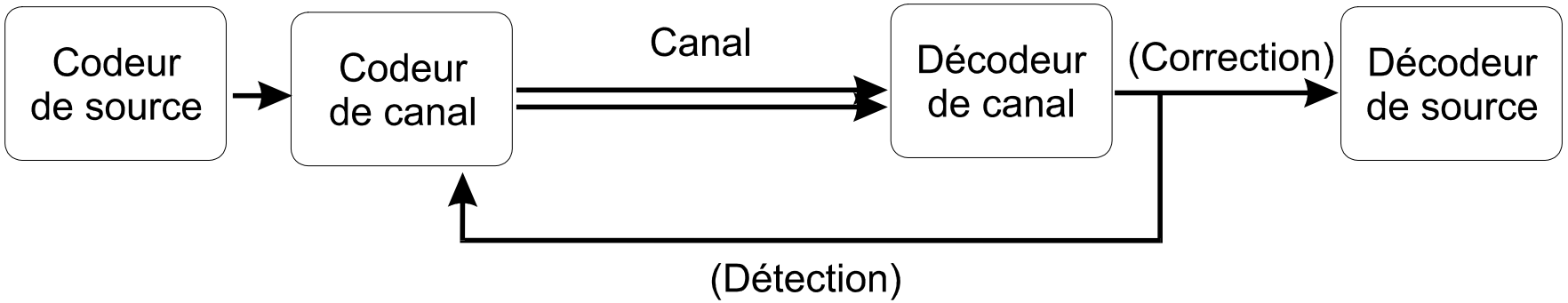
Plan

- 1. Introduction
- 2. Sources discrètes & Entropie
- 3. Canaux discrets & Capacité
- 4. Codage de source
- 5. Codage de canal
- 6. Cryptographie
- 7. Conclusion

5. Codage de canal

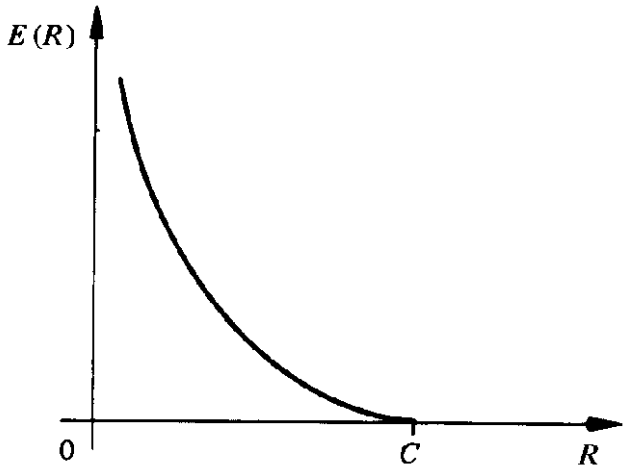
✓**Détecter** et/ou **corriger** les erreurs de transmission



Codeur de canal ⇨ **introduire** une **redondance** utilisable

- **Théorème des canaux à perturbation (codage de canal)**

" Pour une source à débit d'information de R bit/s et un canal de capacité C bit/s, si R<C, il existe un code ayant des mots de longueur n, de sorte que la probabilité d'erreur de décodage p_E vérifie : $p_E \leq 2^{-n.E(R)}$ "



Rq1 : un résultat inattendu !

Rq2 : existance ss méthode ...

Rq3 : à p_E constant, n augmente si R tend vers C.

Rq4 : en pratique, si R<0.5 C, des codes existent avec p_E faible.

- **Taux d'erreur**

$$T_e = \frac{Nombre\ de\ bits\ erronés}{Nombre\ de\ bits\ transmis}$$

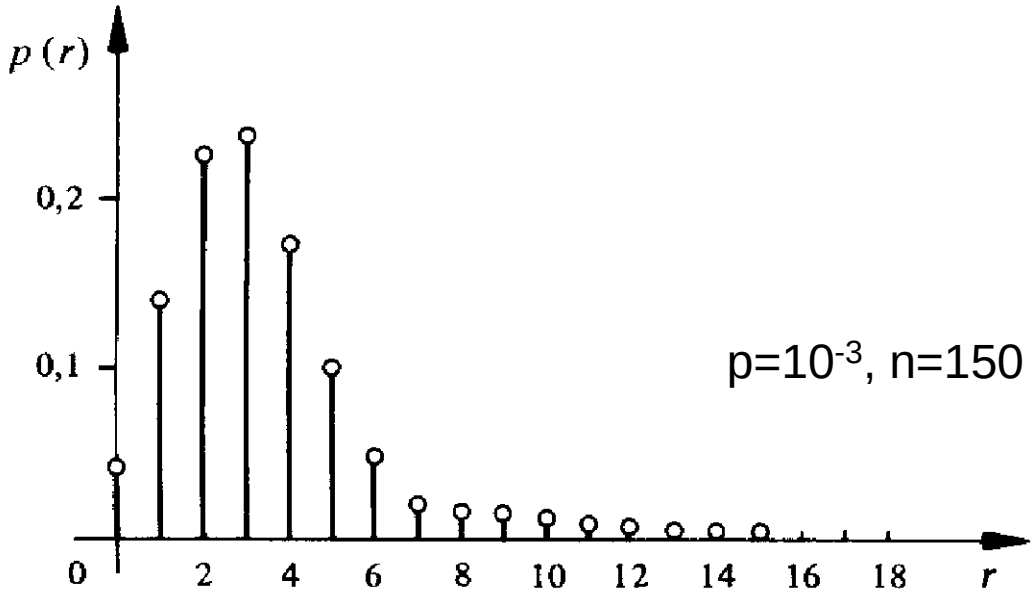
01100100100110010010100 1010 ⇨ 01100110110010110100 0010

↳ $T_e = 3/24 = 0.125$

- **Probabilité d'erreur**

$$P_{n\,bits\,corrects} = (1-p)^n$$

$$P_{r\,erreurs/n} = C_n^r . p^r . (1-p)^{n-r}$$



p=10^{-3}, n=150

- **Taux de codage**

$$R = \frac{k}{n}$$

- k taille du mot d ’information (avant codage)
- n taille du mot-code (après codage)

- **Détection et correction d'erreurs**

✓**Détection par écho**

✓**Détection par répétition**

✓**Détection par bit de parité**

✓**Détection par code**

✓**Détection et correction par code**

• Détection d'erreurs par bit de parité (caractère)

✓**VRC (**Vertical Redundancy Check)

⇨ Asynchrone

Caractère	O	S	I
Bit 0	1	1	1
Bit 1	0	0	0
Bit 2	0	1	0
Bit 3	1	0	1
Bit 4	1	0	0
Bit 5	1	1	0
Bit 6	1	1	1
Bit de parité	1	0	1
Bit d'imparité	0	1	0

✓**LRC (**Longitudinal Redundancy Check)

⇨ Synchrone

Caractère à envoyer	Bit de VRC	Caractère à envoyer	Bit de VRC	. . .	Caractère LRC	Bit de VRC

	H	E	L	L	O	LRC →
bit 1	0	1	0	0	1	0
bit 2	0	0	0	0	1	1
bit 3	0	1	1	1	1	0
bit 4	1	0	1	1	1	0
bit 5	0	0	0	0	0	0
bit 6	0	0	0	0	0	0
bit 7	1	1	1	1	1	1
VRC ↓	0	1	1	1	1	0

0001001	0	1010001	1	0011001	1	0011001	1	1111100	1	0100001	0
H		E		L		L		O		LRC	

- **Codes détecteur et/ou correcteur**

  ✓ **Codes linéaires**
  - **Codes groupes**

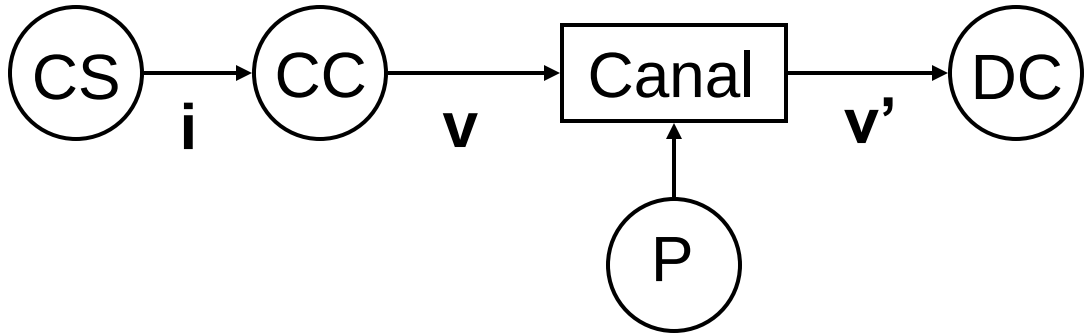
    Parité, Code de Hamming
  - **Codes cycliques**

    CRC/FCS, code BCH, Golay

  ✓ **Codes convolutifs**

    Algorithme de Viterbi

✓ Codes linéaires



- **Notations**

  - Mot-code : v

$$v = [a_1\ a_2\ ....\ a_m\ a_{m+1}\ a_{m+2}\ ....\ a_n] = [c \quad i]$$

[c] : *m* symboles de contrôle
[i] : *k* =*n*-*m* symboles d'information

  - Mot-erreur : ε

$$\varepsilon = [\varepsilon_1 \ \ \varepsilon_2\ .....\ \varepsilon_n] \qquad v_i = v_i' + \varepsilon \quad \Leftrightarrow \quad v_i' = v_i + \varepsilon$$

$$\varepsilon_i = \begin{bmatrix} 1 \text{ si erreur à la ième position} \\ 0 \text{ sinon} \end{bmatrix}$$

- **Propriétés des codes linéaires**

  Les symboles de contrôle sont obtenus par une combinaison linéaire des symboles d ’information.

  → un code linéaire contient v=[0 0 …0]

- **Code systématique**

  Les symboles d ’information et de contrôle sont séparés.

- **Distance de Hamming**

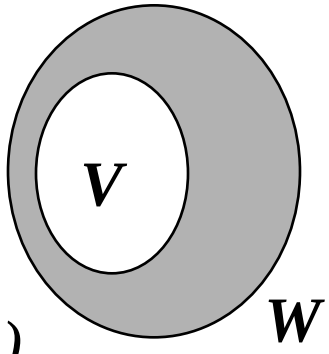
$$D(v_i, v_j) = (a_{i1} \oplus a_{j1}) + (a_{i2} \oplus a_{j2}) + ... + (a_{in} \oplus a_{jn})$$

  ↳ Le nombre de coordonnées par lesquelles les 2 mots diffèrent

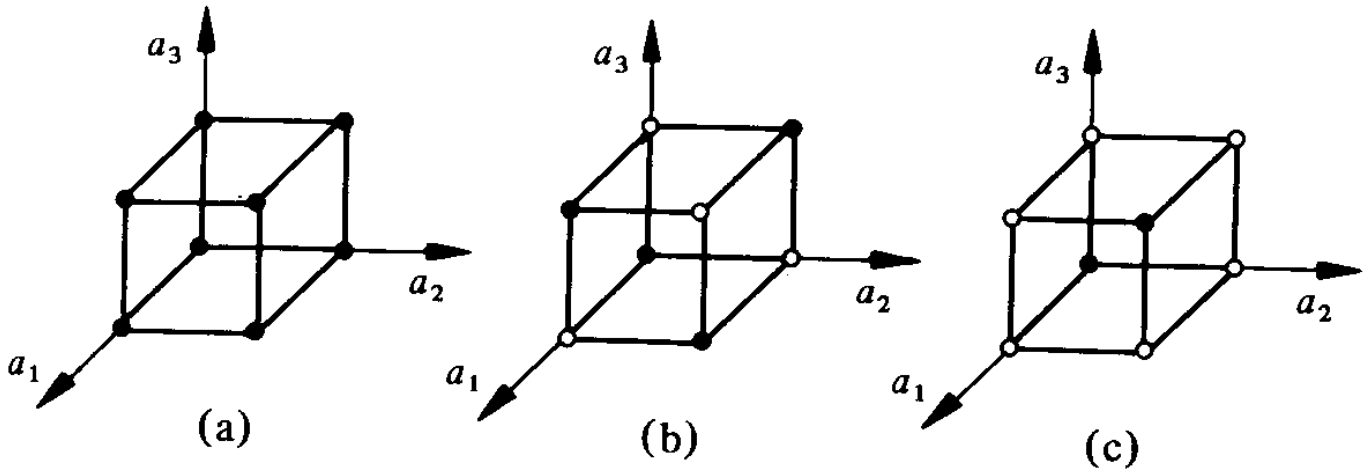
- **Illustration spatiale :** modèle code groupe

  - Un mot = un vecteur dans un espace à n dimensions !

    $w=[a_1\ a_2\ \ldots\ a_n]$



  - *W = ensemble des $N = 2^n$ mots*
  - *V = ensemble des $S = 2^k$ mots ayant un sens (mot-code)*



- **Capacité de détection et région de décision**

$v_i \rightarrow$ Région W_i Région $W_0 \rightarrow$ équidistant

→ Détection et correction ⇨ si W_i grand

Théorème de Hamming

✓ Détecter *d* erreurs → $D_{min} = d+1$

✓Corriger *e* erreurs → $D_{min} = 2e+1$

✓Corriger *e* & détecter *d* erreurs → $D_{min} = 2e + d + 1$

Ex → Hamming(S^4)

- **Principe de détection et correction**

Deux opérateurs : $H \quad D$

$$H(v_i) = 0 \text{ pour tout } i = 1 \text{ à } S = 2^k$$

✓ Si $H(v'_i) = 0$ alors $v'_i = v_i \rightarrow$ pas d'erreur

✓ Si $H(v'_i) = z \neq 0 \rightarrow$ détection d'erreur

Si z est connu $\rightarrow D(z) = \varepsilon$

$v'_i + \varepsilon = v_i \rightarrow$ correction d'erreur

- **Décodage et matrice de contrôle**

$$v = \begin{bmatrix} a_1 & a_2 & \dots & a_n \end{bmatrix}$$

Soit $H_{(m,n)}$ la matrice de contrôle, $$[H] = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & & h_{2n} \\ \dots & & & \dots \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{bmatrix}$$

Soit z le syndrome (ou correcteur), $$z = H.v'^{T} = \begin{bmatrix} z_1 \\ : \\ z_m \end{bmatrix}$$

Si z=[0] pas d ’erreur, sinon erreur et +- correction

- **Codage et matrice génératrice**

$$i = [i_1 \quad i_2 \quad \dots \quad i_k]$$

Soit $G_{(k,n)}$ la matrice génératrice, $[G] = \begin{bmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ g_{21} & g_{22} & & g_{2n} \\ \dots & & & \dots \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{bmatrix}$

$$\boxed{v = i.G}$$

Les matrices H et G sont liées par : $G.H^t = 0$

et peuvent se mettre sous la forme systématique

$$G = \begin{bmatrix} & : & \\ I_k & : & A_{k,m} \\ & : & \end{bmatrix} \qquad H = \begin{bmatrix} & : & \\ A^t_{k,m} & : & I_m \\ & : & \end{bmatrix}$$

- **Exemple** k=2, m=1, n=3

$$[G_1]=\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix} \qquad [H]=\begin{bmatrix}1 & 1 & 1\end{bmatrix} \qquad [G_2]=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}$$

$$\begin{bmatrix}0 & 0\end{bmatrix}\times\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0\end{bmatrix} \qquad \begin{bmatrix}0 & 0\end{bmatrix}\times\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1\end{bmatrix}\times\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0 & 1\end{bmatrix} \qquad \begin{bmatrix}0 & 1\end{bmatrix}\times\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}=\begin{bmatrix}0 & 1 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0\end{bmatrix}\times\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}=\begin{bmatrix}0 & 1 & 1\end{bmatrix} \qquad \begin{bmatrix}1 & 0\end{bmatrix}\times\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 1\end{bmatrix}\times\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 1 & 0\end{bmatrix} \qquad \begin{bmatrix}1 & 1\end{bmatrix}\times\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 1 & 0\end{bmatrix}$$

- **Code de Hamming groupe**

⇨ Correction d'une erreur

↳ $\boxed{2^m \geq n+1 \Leftrightarrow 2^m \geq k+m+1}$

✓ $[H] = [h_1 \quad h_2 \quad \ldots \quad h_n] = \begin{bmatrix} 0 & 0 & \ldots & \\ : & : & : & \ldots \\ 0 & 1 & 1 & \ldots \\ 1 & 0 & 1 & \ldots \end{bmatrix}$ avec $h_i = bin(i)$

✓ Mot-erreur : $\varepsilon = [\ldots. \ \alpha_i \ \ldots.]$

$$v'_j = v_j + \varepsilon \Leftrightarrow z = H.v'_j = H.\varepsilon^T \Leftrightarrow z = h_i$$

↳ L'erreur est à la position $dec(h_i)$

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

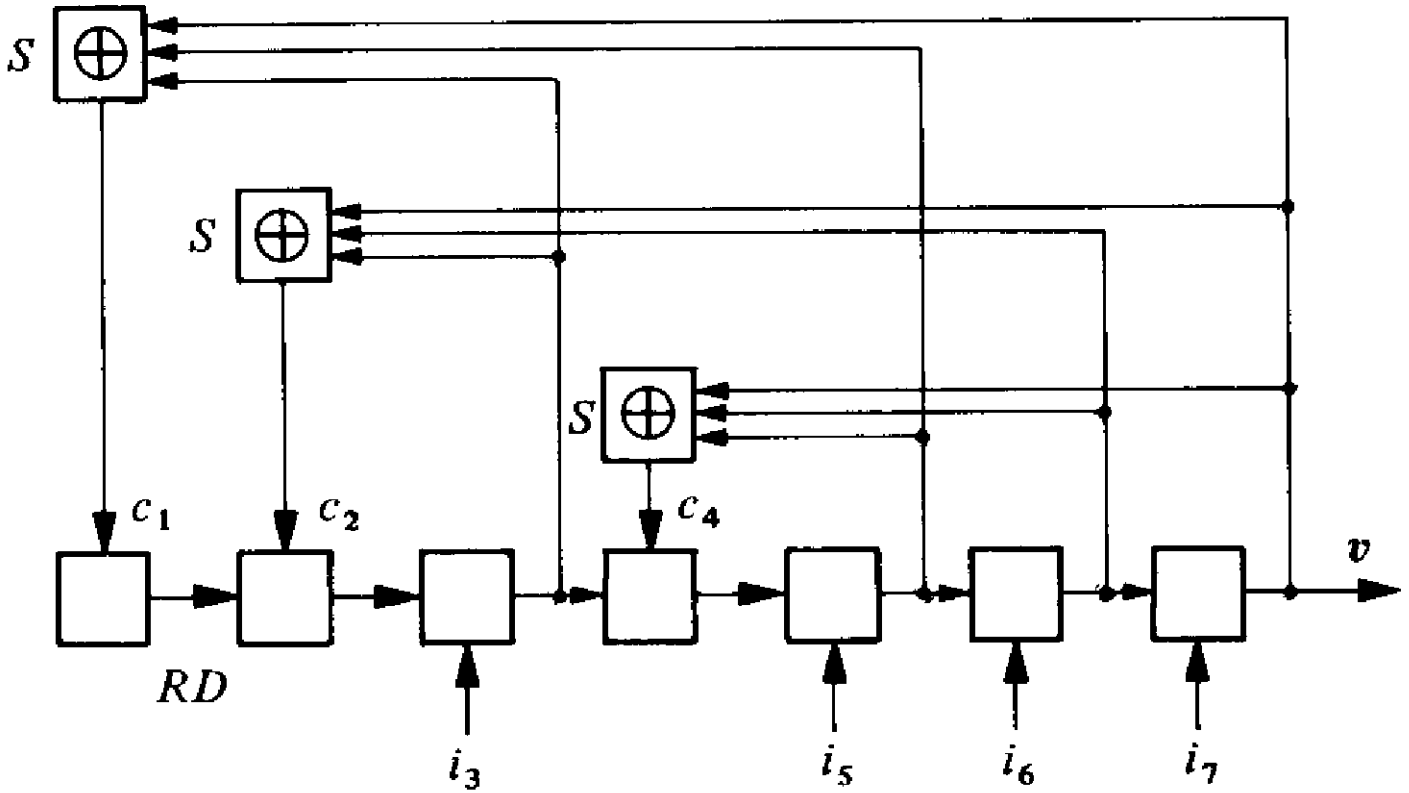
$$v = \begin{bmatrix} c_1 & c_2 & i_3 & c_4 & i_5 & i_6 & i_7 \end{bmatrix}$$

$$H.v^T = 0$$

$$\Downarrow$$

$$\begin{cases} c_1 = i_3 + i_5 + i_7 \\ c_2 = i_3 + i_6 + i_7 \\ c_4 = i_5 + i_6 + i_7 \end{cases}$$

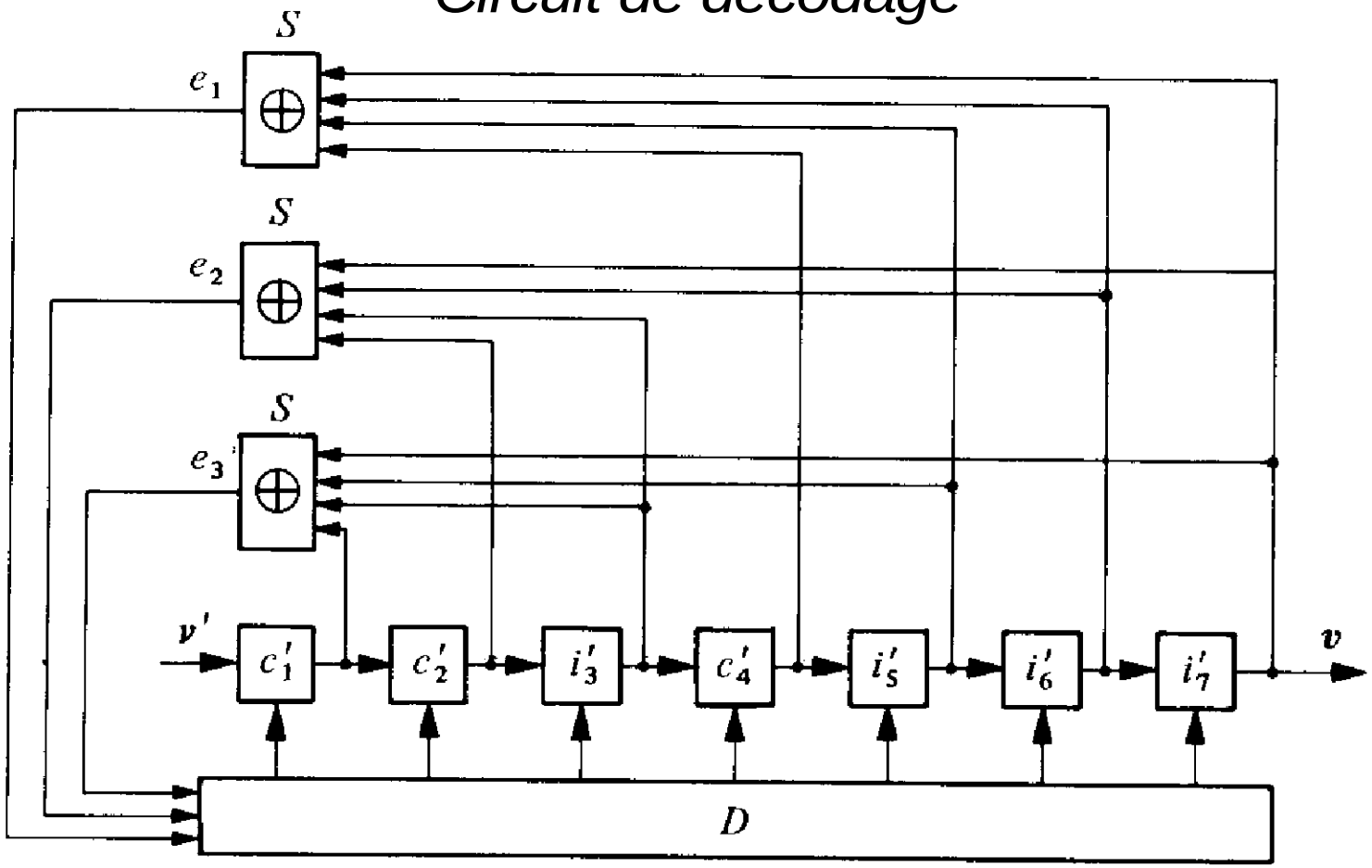
Circuit de codage



$$\begin{cases} e_3 = c'_1 + i'_3 + i'_5 + i'_7 \\ e_2 = c'_2 + i'_3 + i'_6 + i'_7 \\ e_1 = c'_4 + i'_5 + i'_6 + i'_7 \end{cases}$$

$$\varepsilon_i = 1 \quad \text{pour} \quad i = e_3.2^0 + e_2.2^1 + e_1.2^2$$

Circuit de décodage



✓ **Codes cycliques** (Cyclic Redundancy Check / Frame Check Sequence)

- Code cyclique = code linéaire + propriété de permutation
- Bloc de n symboles → **polynôme** de degré n-1 ! :

- Mot-code : $v = [a_0\ a_1\ ....\ a_{n-1}]$ $\quad v(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1}$
- Information : $i = [i_0\ i_1\ ....i_{k-1}]$ $\quad i(x) = i_0 + i_1 x + i_2 x^2 + ... + i_{k-1} x^{k-1}$

$$[1 \quad 0 \quad 1 \quad 1] \leftrightarrow 1 + x^2 + x^3$$

- **Polynôme générateur : *g(x)***

  - g(x) définit le codeur (n,k)

  - g(x) est de degré m=n-k

  - Il vérifie : $1+x^n = g(x) \times p(x)$

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k}$$

avec $g_{n-k} = g_m = 1$

et souvent $g_0 = 1$

Exemple : code cyclique (n=7, k=4)

$$1+x^7 = (1+x) \times (1+x^2+x^3) \times (1+x+x^3)$$

g(x) est de degré 3 soit :

$$g(x) = (1+x^2+x^3) \quad \text{ou} \quad g(x) = (1+x+x^3)$$

- **Matrice génératrice et polynôme générateur**

$$G_{(k,n)} = \begin{bmatrix} g(x) \\ x.g(x) \\ \dots \\ x^{k-1}.g(x) \end{bmatrix}$$

Exemple : $g(x)=(1+x^2+x^3)$

$$G_{(4,7)} = \begin{bmatrix} 1 & 0 & 1 & 1 & . & . & . \\ . & 1 & 0 & 1 & 1 & . & . \\ . & . & 1 & 0 & 1 & 1 & . \\ . & . & . & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$G^s_{(4,7)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$H^s_{(3,7)} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

- **Codage par multiplication** $\boxed{v(x) = i(x) \times g(x)}$

$$g(x) = 1 + x + x^3 \quad \text{et} \quad i(x) = x + x^2 + x^3 \quad \rightarrow \quad v(x) = x + x^5 + x^6$$

$$[0 \quad 1 \quad 1 \quad 1] \times [1 \quad 1 \quad 0 \quad 1] = [0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1]$$

\# convolution discrète !

- **Codage par division**

$$v(x) = c(x) + x^m . i(x)$$

Systématique !

$$\boxed{c(x) = Reste\left(\frac{x^m . i(x)}{g(x)}\right)}$$

- **Décodage par division**

$$\boxed{z(x) = Reste\left(\frac{v'(x)}{g(x)}\right)}$$

Si *z(x)=0* → Transmission OK
Sinon → Détection ou correction

Ex →

- **Exemple de polynômes générateurs**

✓ATM

- $x^8 + x^2 + x + 1$ → Cellule ATM
- $x^{10} + x^9 + x^5 + x^4 + x + 1$ → Couche AAL type 3/4

✓CCITT N°41 → X25 (HDLC)

- $x^{16} + x^{12} + x^5 + 1$

✓IEEE 802 → Réseaux locaux

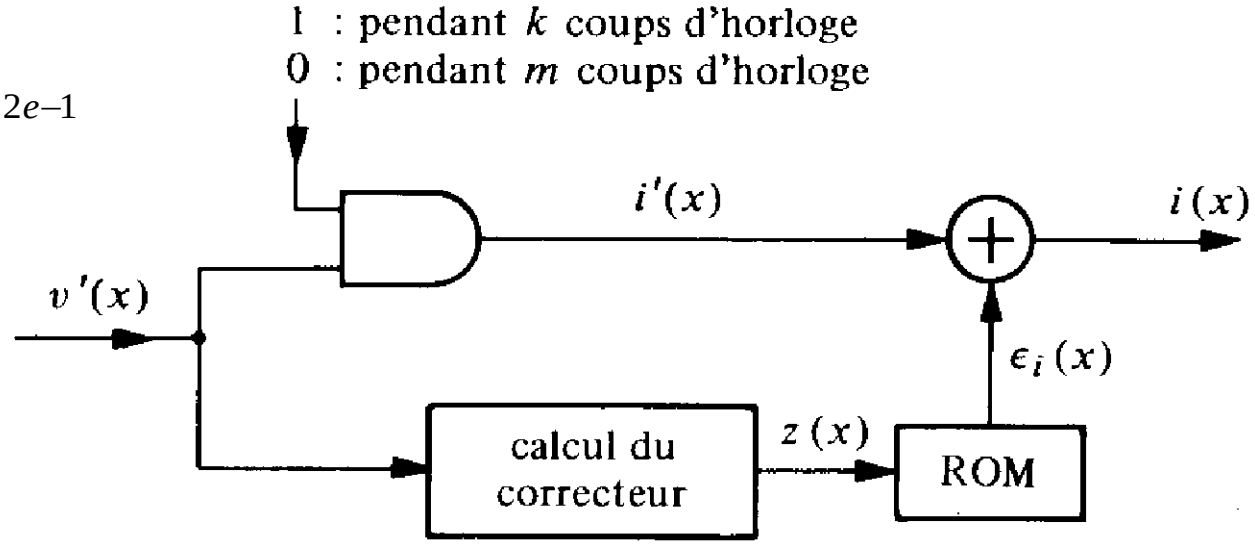
- $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$

- **Code BCH** (Bose-Chaudhuri - Hocquenghem)

  ⇨ Correction de e erreurs

$$g(x) = \prod_{i=1}^{r} m_i(x)$$

$$\beta_1 = \alpha, \beta_2 = \alpha^3, ..., \beta_r = \alpha^{2e-1}$$



- Exemple

  n=15 et e=3

  ↳ $g(x) = (1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)$

  ↳ m=10

- **Code Golay**

⇨ Correction de *e* erreurs parfait

⇨ Nb correcteurs = Nb mots-erreur

e → Nombre d'erreurs à corriger = $2^m - 1$

⇩

$g(x)$ polynôme minimal de degré m

- Exemple

n=23 et e=3

↳ m=11 , k=12

↳ $g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$

✓Codes convolutifs

- **Généralités**

  ⇨ Les symboles d'information sont traités en flux continu

- Rque :Blocs de n_0 symboles, mais dont les m_0 contrôleurs ne dépendent pas que des k_0 symboles d'information !

- Contrainte : m = nb de blocs contrôlés par un bloc donné
- Longueur de contrainte : $n=m.n_0$

- Taux d'émission : $R = \frac{k_0}{n_0}$

- **Codes convolutifs systématiques**

  - Mot-code : $V = \left[X_1 Y_1 X_2 Y_2 ..... X_j Y_j ..... _1 \right]$

    avec $X_j = \left[X_j^1 ..... X_j^{k_0} \right]$ Information

    $Y_j = \left[Y_j^1 ..... Y_j^{m_0} \right]$ Contrôle

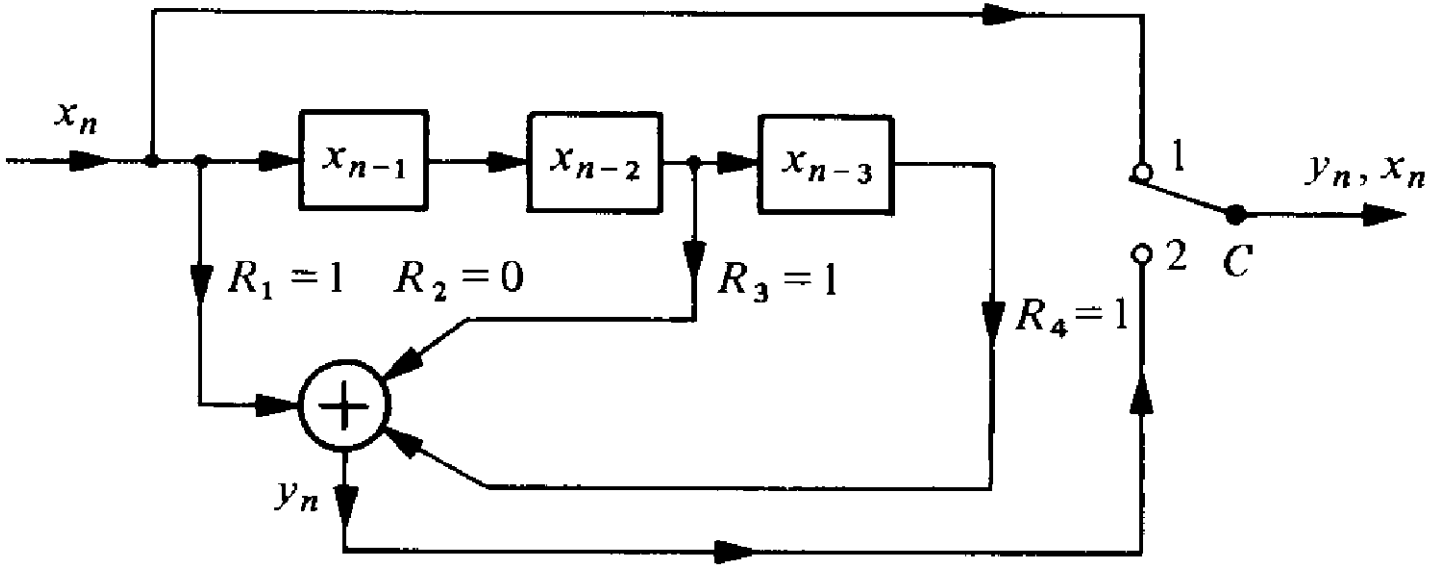
- **Codes convolutifs non systématiques**

  ⇨ Contrôle et information sont mélangés

  - Mot-code : $V = \left[U_1 U_2 ..... U_j ..... \right]$

- Exemple : m=4, k_0=1, m_0=1, n_0=2

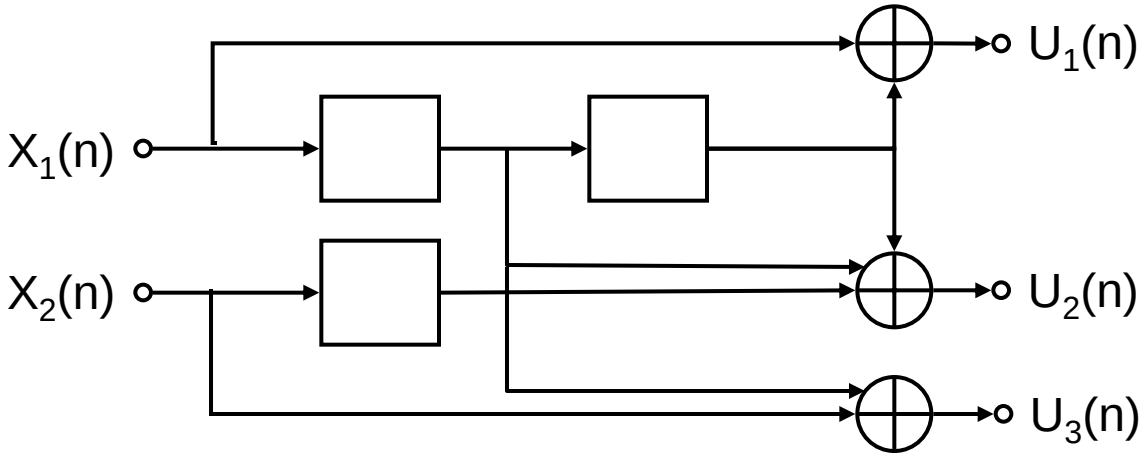
$$y_n = R_4.x_{n-3} + R_3.x_{n-2} + R_2.x_{n-1} + R_1.x_n$$



⇨ *R*=[1011]

- **Représentation des codes convolutifs**

- Par le codeur



- Par une matrice de transfert

$$G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 0 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} \qquad G_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$$

$$G = \begin{bmatrix} 5 & 3 & 2 \\ 0 & 2 & 4 \end{bmatrix}$$

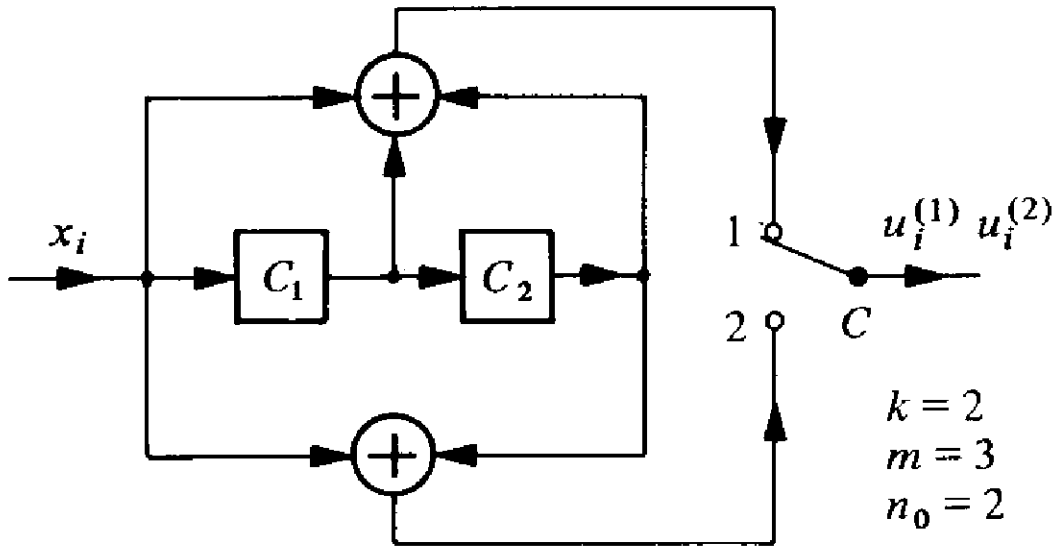
- Un diagramme d'état

- Un treillis → chemin → décodage par chemin le + probable

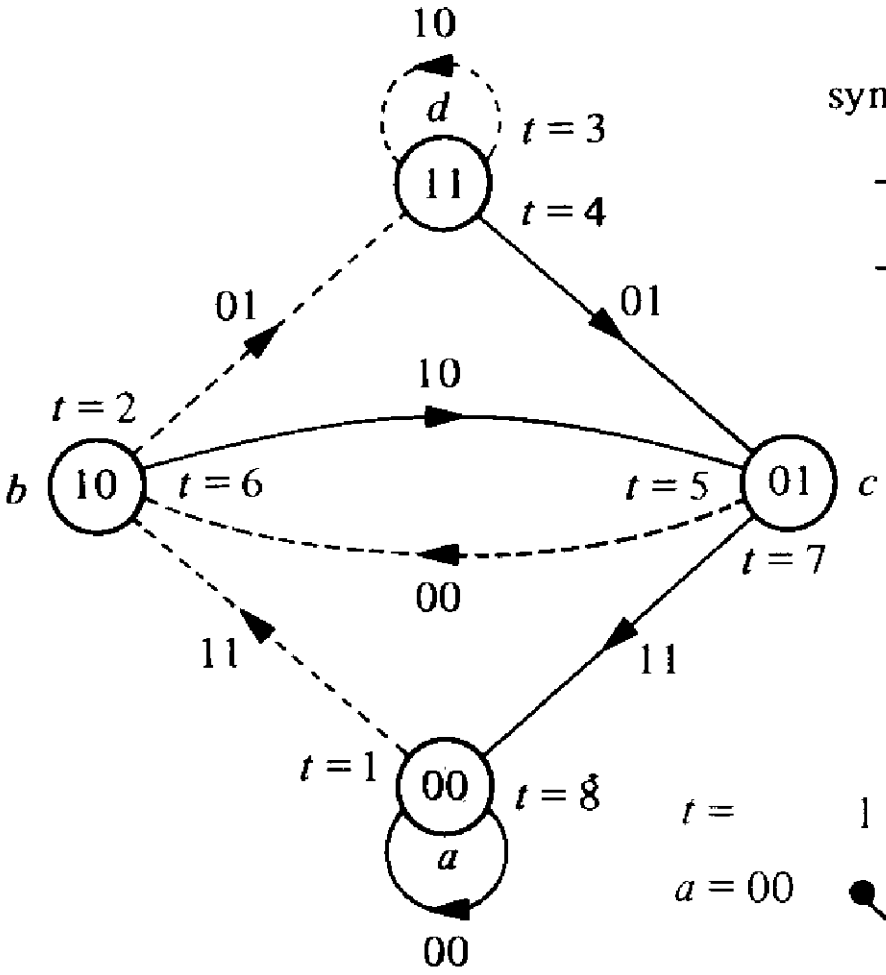
- Exemple : n_0=2, R=0.5 , m=3

$$U_n^{(1)} = x_n + x_{n-1} + x_{n-2}$$

$$U_n^{(2)} = x_n + x_{n-2}$$



t_i	1	2	3	4	5	6	7	8
x_i	1	1	1	0	1	0	0	0
$C_1 C_2$	00	10	11	11	01	10	01	00
$u_i^{(1)} u_i^{(2)}$	11	01	10	01	00	10	11	00



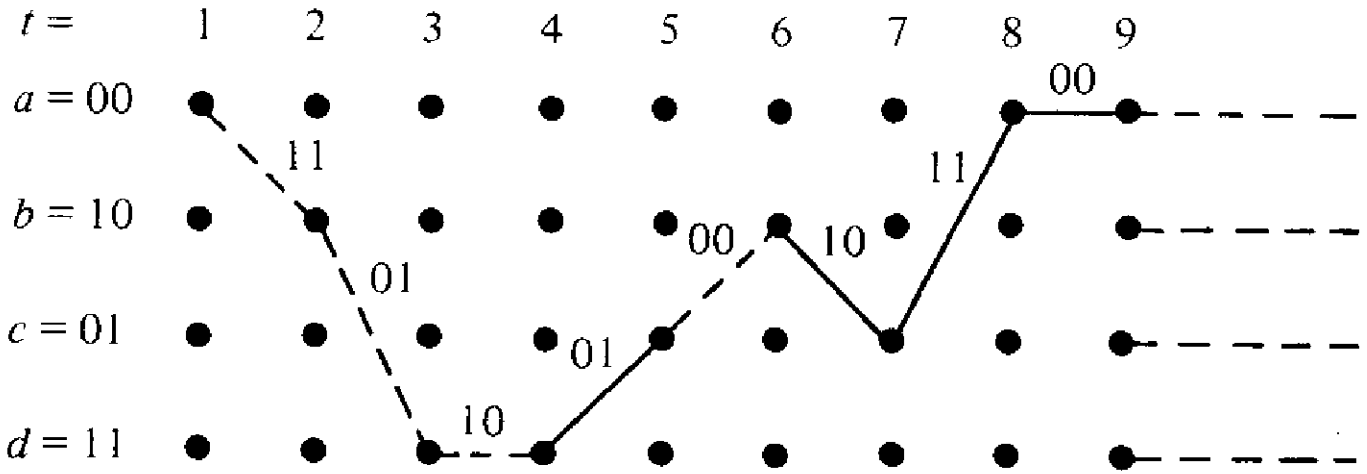
symbole entrant :

——— 0 :

– – – – 1 :

✓Recherche d'erreur à la fréquence N

→ Dmin = 2e+1



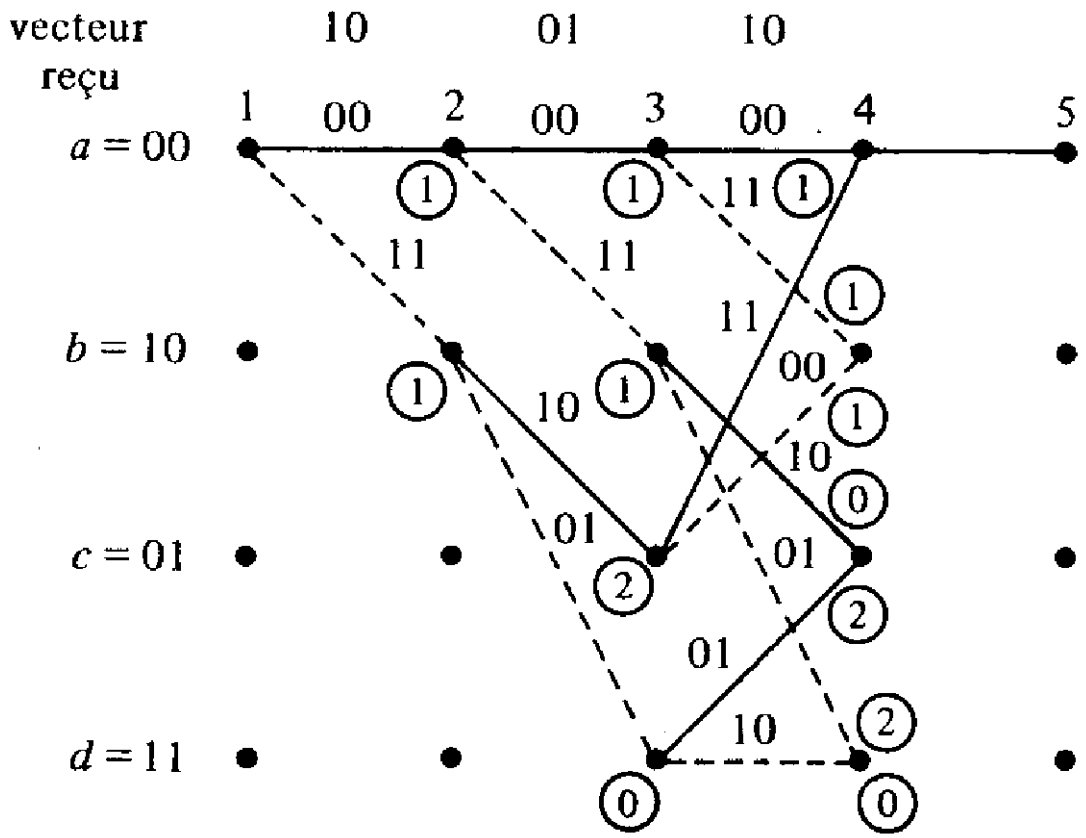
- **Décodage : algorithme de Viterbi**

⇨ Stratégie de recherche de D_{min}

✓Exemple pour N=3

10 01 10 → $Min\left(\sum_{i=1}^{3} d_i\right) = ?$

→ 1<u>1</u> 01 10



• Conclusion sur le codage de canal

✓ Indispensable

✓ Théories mathématiques complexes → des solutions concrètes

- Reed-Salomon (1984) : BCH Qaire → DVB(204,188,8)
- Turbo-Codes (1993) : Code convolutif + brassage

✓ Recherche de codeurs conjoint source / canal

- complexité --
- robustesse ++
- flexibilité ++