

Com Nome - TD3.

exo 1 Code cyclique

1)  $\rightarrow$  Code cyclique  $C(7,4)$  par  $g(x) = x^3 + x + 1$ .

$\begin{cases} C(n, m) & k = \text{degré de } g(x) \\ m = n - k & m = \text{longueur du message.} \end{cases}$

$n=7$ ;  $m=4$   
↳ codé sur 4 bits

$$\rightarrow \underline{z^k m(x) = g(x) q(x) + r(x)}, \text{ as } \deg r(x) < \deg g(x)$$

- Base canonique

|                             | $m(x)$ | $x^k m(x)$ |
|-----------------------------|--------|------------|
| 0001                        | 1      | $x^3$      |
| 0010                        | $x$    | $x^4$      |
| 0100                        | $x^2$  | $x^5$      |
| 1000                        | $x^3$  | $x^6$      |
| $  \quad   \quad   \quad  $ |        |            |
| $x^3 \ x^2 \ x^1 \ x^0$     |        |            |

↓

- On divise  $x^k m(x)$  par  $g(x)$  :  $\frac{x^k m(x)}{g(x) \cdot q(x)} \rightarrow r(x) = \text{reste CRC}$   
avec  $k = 3, 4, 5$  et  $6$

$x^k \rightarrow x^3$   
 $-(x^3 + x + 1)$   
 $= x^2 \oplus x \oplus 1$   
 $= x+1 \rightarrow r(x)$

$x^3 \oplus x \oplus 1 \rightarrow g(x)$   
 $1 \rightarrow q(x)$   
 $x^k \cdot 1 = (x^2 + x + 1) \times 1 + (x + 1)$   
 $x^k \quad m(x) \quad g'(x) \quad q'(x) \rightarrow r(x) : \text{reste CRC}$

$$\begin{array}{r|l} x^4 & x^3 + x + 1 \\ -(x^4 + x^2 + x) & \\ \hline & x^2 + x \end{array}$$

$$\Rightarrow x^4 \cdot x = (x^3 + x + 1) \times x + (x^2 + x)$$

$$\begin{array}{r|l} x^5 & x^3 \oplus x \oplus 1 \\ & x^2 + 1 \\ \hline \end{array} \Rightarrow x^5 \cdot x^2 = (x^3 + x + 1) \times (x^2 + 1) + (x^2 + x + 1)$$

(si available  $q(x) = x^2$ , alors  $r(x) = x^3 + x^2$   
or  $\deg r(x) < \deg q(x)$  !

$$\begin{array}{l} x^6 \\ -(x^5 + x^4 + x^3 \\ + x^2 + x + 1) \\ \hline x^2 + 1 \end{array} \quad \begin{array}{l} x^3 + x + 1 \\ x^3 + x + 1 \\ \hline 0 \end{array}$$

Conclus°

$$0001 \rightarrow m = 1 \rightarrow r = (n+1) = \underbrace{0}_x x^2 + \underbrace{1}_x x^1 + \underbrace{1}_x x^0$$

dc

$$\begin{cases} 0001 \rightarrow 011 \\ 0010 \rightarrow 110 \\ 0100 \rightarrow 111 \\ 1000 \rightarrow 101 \end{cases}$$

2) +3)

a) Message : 1110 011  
info CRC  
      ↳ m       ↳ r

⚠ sens inverse

$$p(x) = g(x) \cdot q(x)$$

$$\hookrightarrow p(x) = 1 + x + x^4 + x^5 + x^6$$

$$p(x) / g(x)$$

$$\begin{array}{l} \hookrightarrow x^6 \oplus x^5 \oplus x^4 \oplus x \oplus 1 \quad | \quad x^3 \oplus x \oplus 1 \\ \underline{-(x^6 \oplus x^5 \oplus x^4 \oplus x \oplus 1)} \\ \phantom{\hookrightarrow} r(x) \rightarrow 111 \end{array}$$

$$\hookrightarrow 0100 \quad 111$$

↑  
erreur sur le 3<sup>e</sup> bit de l'info

dc erreur sur le 3<sup>e</sup> bit du message:

$$\begin{array}{c} 1 \oplus 10 \quad 011 \\ \downarrow \\ x^5 : \text{bit erroné} \end{array}$$

Donc l'erreur estimée est:

$$E(x) = 0100 \quad 000$$

$$\oplus$$

message reçu = 1110 011

Message restitué: 1010 011

| A | B | ⊕ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

b) Message : 1010 111  
info CRC

$$g(x) = x^3 + x + 1$$

$$p(x) = 1 + x + x^2 + x^4 + x^6$$

$$\begin{array}{l} x^6 \oplus x^4 \oplus x^2 \oplus x \oplus 1 \quad | \quad x^3 \oplus x \oplus 1 \\ \underline{-(x^6 \oplus x^4 \oplus x^2)} \\ x^3 \oplus x^2 \oplus x \oplus 1 \\ \underline{-(x^3 \oplus x + 1)} \\ x^2 \end{array}$$

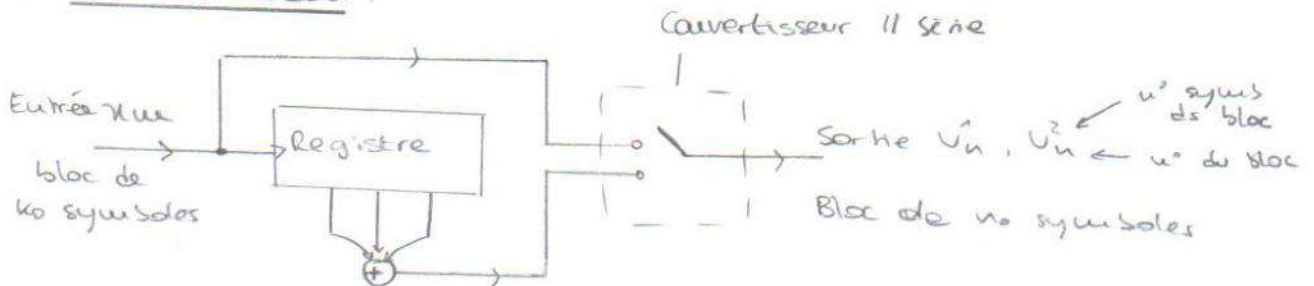
↳  $r(x) = 100 \rightarrow$  Erreur sur le bit de contrôle (CRC)  
donc inutile de corriger

4)  
condition réalisée  
si  $g(x)$  primitif

## Exo 2 Codes convolutifs

- 1) code convolutif de rendement  $1/2$  déf par poly générateurs:  
 $g^{(1)}(x) = x^2 + x + 1$        $g^{(2)}(x) = x^2 + 1$

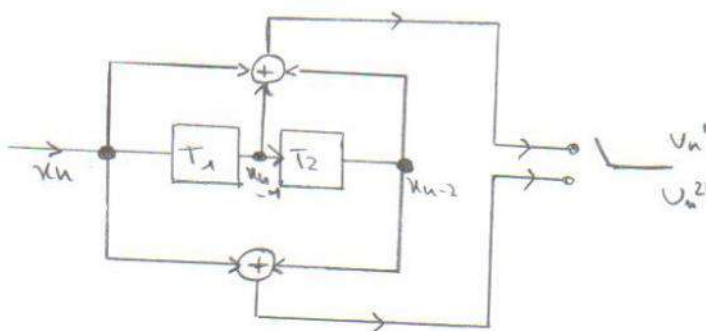
• schéma du codeur:



• Taux d'émission - Rendement

$$R = \frac{n_0}{n_0 + n_1} = \frac{1}{2} \quad \text{car} \quad \begin{array}{l} n_0 = \text{symbole d'info} \\ n_1 = \text{longueur de bloc} \end{array}$$

• Contrainte  $\ell = 3$  car  $R = \frac{1}{2}$  de  $n_0 = 1$  et  $n_1 = 2$   
 $\ell = n_0 + n_1$



$\ell = 3$ .  $x_n$  apparaîtra dans  
 $u_n^1, u_n^2, u_{n+1}^1, u_{n+1}^2, u_{n+2}^1, u_{n+2}^2$

$$\Rightarrow \begin{cases} u_n^1 = x_n \oplus x_{n-1} \oplus x_{n-2} \\ u_n^2 = x_n \oplus x_{n-2} \end{cases}$$

TD n°3

$$n-k=m \quad m=4$$

exo 1. Codes cycliques cf (2) p13

1)  $c(7,4)$   
 $n$  bits message  
 $m$  bits message  
 $k$  bits message  
 $m$  bits message  
 $k$  bits message  
 $m$  bits message  
 $k$  bits message

$$m=4 \quad k=3$$

$$g(x) = x^3 + x + 1$$

$$x^k m(x) = g(x) q(x) + r(x)$$

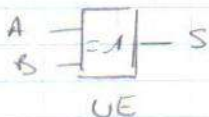
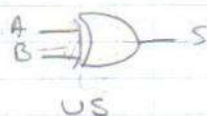
Base canonique:

$$ax^3 + bx^2 + cx + d$$

| a b c d | $m(x)$ | $x^k m(x)$ |
|---------|--------|------------|
| 0001    | 1      | $x^3$      |
| 0010    | $x$    | $x^4$      |
| 0100    | $x^2$  | $x^5$      |
| 1000    | $x^3$  | $x^6$      |

Rappel

ou EXCLUSIF



| A | B | S |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

$$A \oplus A = 0$$

CRC: Code à Redance Cyclique.

$$\begin{aligned}
 & x^5 \overline{) x^5 + x^3 + x^2} \\
 & \underline{-(x^5 + x^3 + x^2)} \\
 & = x^4 + x^2 + 1 \\
 & \underline{-(x^4 + x^2 + 1)} \\
 & = 0
 \end{aligned}$$

$x^2 + x + 1 \rightarrow r(x)$

# Recherche du CRC associé au message :

$$6 \div 3 \quad 6 = 3 \times 2 + 0$$

$$\begin{array}{r|l} x^3 & x^3+x+1 \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \end{array}$$

$\textcircled{1} \rightarrow q(x)$

$$\begin{array}{r|l} x^4 & x^3+x+1 \\ - (x^4+x^3+x) & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \end{array}$$

$$\hookrightarrow x^3 \cdot 1 = (x^3+x+1) \cdot 1 + x^3+x+1$$

$\Downarrow$

$$x^3 = q(x) g(x) \quad x^3-1 \times (x^3+x+1) = x^3+x^3+x+1$$

$$\begin{array}{r|l} x^3 & x^3+x+1 \\ x^3+x+1 & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \end{array}$$

$\textcircled{1} \rightarrow q(x)$

$$x^3 \cdot 1 = (x^3+x+1) \cdot 1 + (x+1) \quad \text{reste (CRC)}$$

$$\begin{array}{r|l} x^4 & x^3+x+1 \\ x^4+x^3+x & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \end{array}$$

$$x^4 \cdot (x) = (x^3+x+1) \cdot x + (x^2+x) \quad \text{CRC}$$

$$\begin{array}{r|l} x^5 & x^3+x+1 \\ x^5+x^4+x^3+x^2+x & \\ \hline x^3+x+1 & \\ - (x^3+x+1) & \\ \hline x^3+x+1 & \end{array}$$

$$x^5 \cdot x^2 = (x^3+x+1) (x^2+1) + (x^3+x+1) \quad \text{CRC}$$

$$\begin{array}{r|l}
 x^6 & x^3 \oplus x \oplus 1 \\
 \hline
 x^4 \oplus x^3 & x^3 \oplus x \oplus 1 \\
 \oplus x^3 \oplus & \\
 x^2 \oplus x \oplus & \\
 x^2 \oplus 1 & 
 \end{array}$$

$$x^k m(x) = q(x) g(x) + r(x)$$

$$x^6 x^3 = (x^3 + x + 1) \cdot (x^3 + x + 1) + (x^2 + 1) \quad \text{CRC}$$

Conclusion

CRC

|      |   |     |
|------|---|-----|
| 0001 | → | 011 |
| 0010 | → | 110 |
| 0100 | → | 111 |
| 1000 | → | 101 |

1.2) + 1.3)

Exemple 1. Message reçu 1110 011  
info CRC.

⚠ Sens

0 → 1100 111  
Le 1<sup>er</sup> qui arrive est le 1<sup>er</sup>  
de poids faible.

$$1110011 \Rightarrow P(x) = 1 + x + x^4 + x^5 + x^6$$

$$\begin{array}{r|l}
 x^6 \oplus x^5 \oplus x^4 \oplus x \oplus 1 & x^3 \oplus x \oplus 1 \\
 \hline
 x^5 \oplus x^3 \oplus x \oplus 1 & x^3 \oplus x^2 \\
 x^2 \oplus x \oplus 1 & 
 \end{array}$$

Reste non nul  
égal à 111

↳ Il y a erreur en  $x^5$

1110011  
car 111 → 0100  
bit erroné

L'Erreur  $E(x)$ : 0100 0000

message reçu : 1110011

erreur estimée : 0100 0000

⇒ Message restitué : 1010011

## Exemple 2:

$$1010111 \rightarrow P(x) = x^6 + x^4 + x^2 + x + 1$$

$$x^6 \oplus x^4 \oplus x^2 + x + 1$$

|                                               |                                           |
|-----------------------------------------------|-------------------------------------------|
| $x^6 \oplus x^4 \oplus x^2 \oplus x \oplus 1$ | <u><math>x^3 \oplus x \oplus 1</math></u> |
| $x^3 \oplus x^2 \oplus x \oplus 1$            | $x^3 \oplus 1$                            |
| $x^2$                                         |                                           |

erreur sur 100  $\leftarrow$  (Erreur sur le bit de contrôle)

L'erreur se trouve sur le CRC de inutile de corriger.

(On a 99% de chance si un bit varie entre le message transmis et le message reçu).

1.4). Condition réalisée si  $g(x)$  primitif.

$$1010111$$

$$r(x) = 101 \rightarrow \begin{array}{c} \downarrow \\ 1000 \\ \downarrow \\ \textcircled{1010} \end{array}$$

erreur sur  $x^6$  1000 000

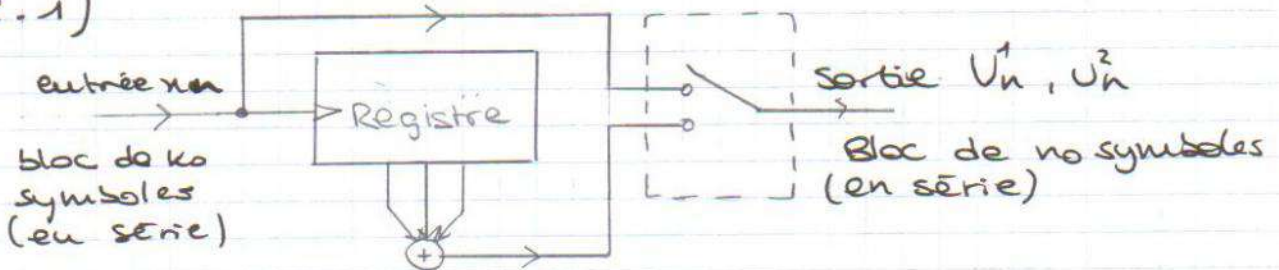
$$\begin{array}{r} 1000000 \\ \oplus \\ 1010111 \\ \hline 0010111 \end{array}$$

23/01

# TD3 (2)

## II. Codes convolutif.

2.1)



1  $\leftarrow$  n° symbole de la bloc  
NB:  $U_n^1 \leftarrow$  n° du bloc.

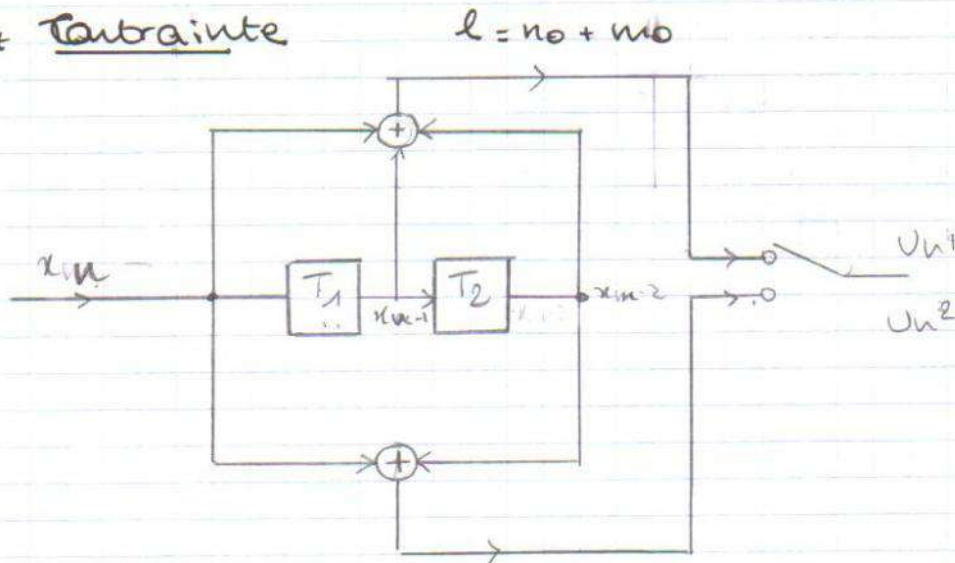
\* Taux d'émission (= rendement)

$$R = \frac{m_0}{n_0} \cdot \frac{1}{2}$$

$m_0$  = symbole d'information

$n_0$  = longueur de bloc

\* Contrainte



$$n_0 = 2, m_0 = 1 \rightarrow l = 3 \text{ et } R = \frac{1}{2}$$

$l = 3 \rightarrow x_m$  apparaît ds

$$U_n^1, U_n^2, U_{n+1}^1, U_{n+1}^2; U_{n+2}^1, U_{n+2}^2$$

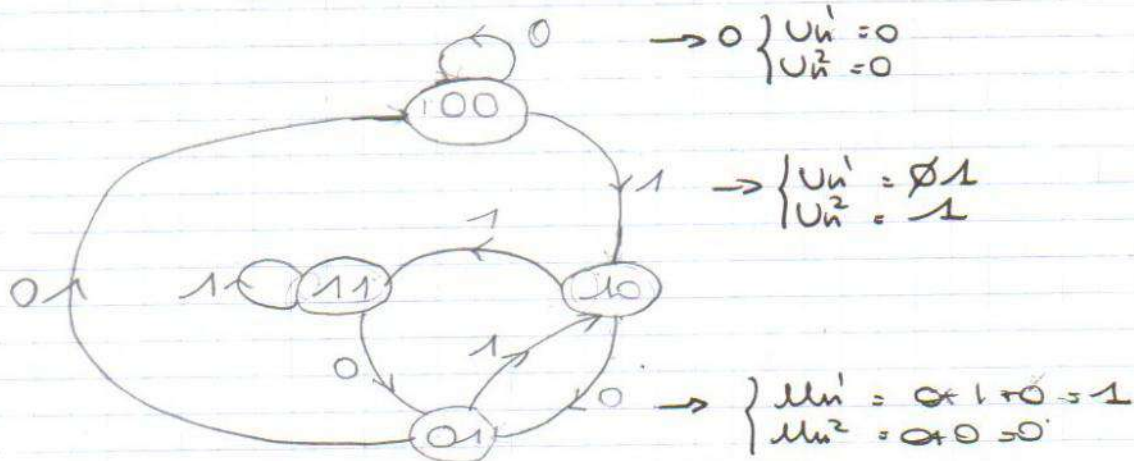
$$\Rightarrow \begin{cases} U_n^1 = x_m \oplus x_{m-1} \oplus x_{m-2} \\ U_n^2 = x_m \oplus x_{m-2} \end{cases}$$

$$\text{si } x_m = 0, U_n^1 \text{ et } U_n^2 = 0$$

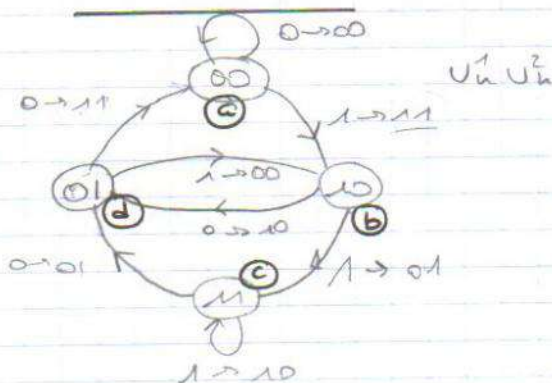
→ polynômes générateurs:

$$\Rightarrow \begin{cases} g^{u1}(x) = x^2 + x + 1 (M_1^1) \\ g^{u2}(x) = x^2 + 1 (M_1^2) \end{cases}$$

• Diagramme de transition  $T_1 T_2$



3010107



code cyclique: data + CRC (code de contrôle)

code caudatif: code entrelacé → faire calcul par désentrelacer data et CRC

2.2)

information: 01011 - 6 bits.

Ajout d'une queue : 00 (par ex) Pour contrôler l'état initial et correct  
(au envoi ou recepi)

code = résultat d'une transition. Ps avec le 1er bit  
 Avec cette queue, on indique de son point de départ

⇒ message: 01011100 - 8 bits.

Puis on envoie la séquence associée à ce message, ce qui compte, ce sont les transitions.

| Message          | 0   | 1   | 0   | 1   | 1   | 1   | 0   | 0   |
|------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Etat du registre | (a) | (b) | (d) | (b) | (c) | (c) | (d) | (a) |
| Codage           | 00  | 11  | 10  | 00  | 01  | 10  | 01  | 11  |

!!!  
 ↓  
 Etat de départ

Séquence d'envoi: 00111000110111 - 16 bits

Par rapport au code à redondance cyclique, le code associé à la data est + important.

$$\text{rendement} = \frac{8}{16} = 50\%$$

2.3)

Par rendement, on diminue le séquence d'envoi  
 ↳ code poinçonné

Poinçonnage bits n: 3, 6, 9, 12, 15

nouveau code: 00110011011 - 11 bits.

$$\text{Rendement} = \frac{8}{11} = 76\%$$

Lorsqu'il recevra la data, le récepteur sait que c'est un code poinçonné, et il va rajouter des 0 et 1 aléatoirement

↳ faire 1 algo pour savoir si ce que l'on a reçu est bon ou pas

↳ Algo de Viterbi (distance de Hamming)

Avg code poinçonné : économie de bande passante + rapide.

Ce qui est important, c'est q ce qui a été poinçonné à l'entrée, soit connu à la sortie (un format de poinçonnage)

Donc contrôle à l'entrée et contrôle à la sortie  
→ Émetteur et récepteur savent {  
- même diagramme de transition  
- même état de départ (def toutes les 13ms)  
- même format de message. 11 bits  
- même code de poinçonnage

## 2.4) Algo de Viterbi

Message reçu: 001101111010

- Etape 1 : remplissage des positions poinçonnées par des 0, des 1, ou un tirage aléatoires de 0 à 1.

Ici, on prend par ex des 0.

→ Séquence reconstituée: 0000000000000000 - 16 bits

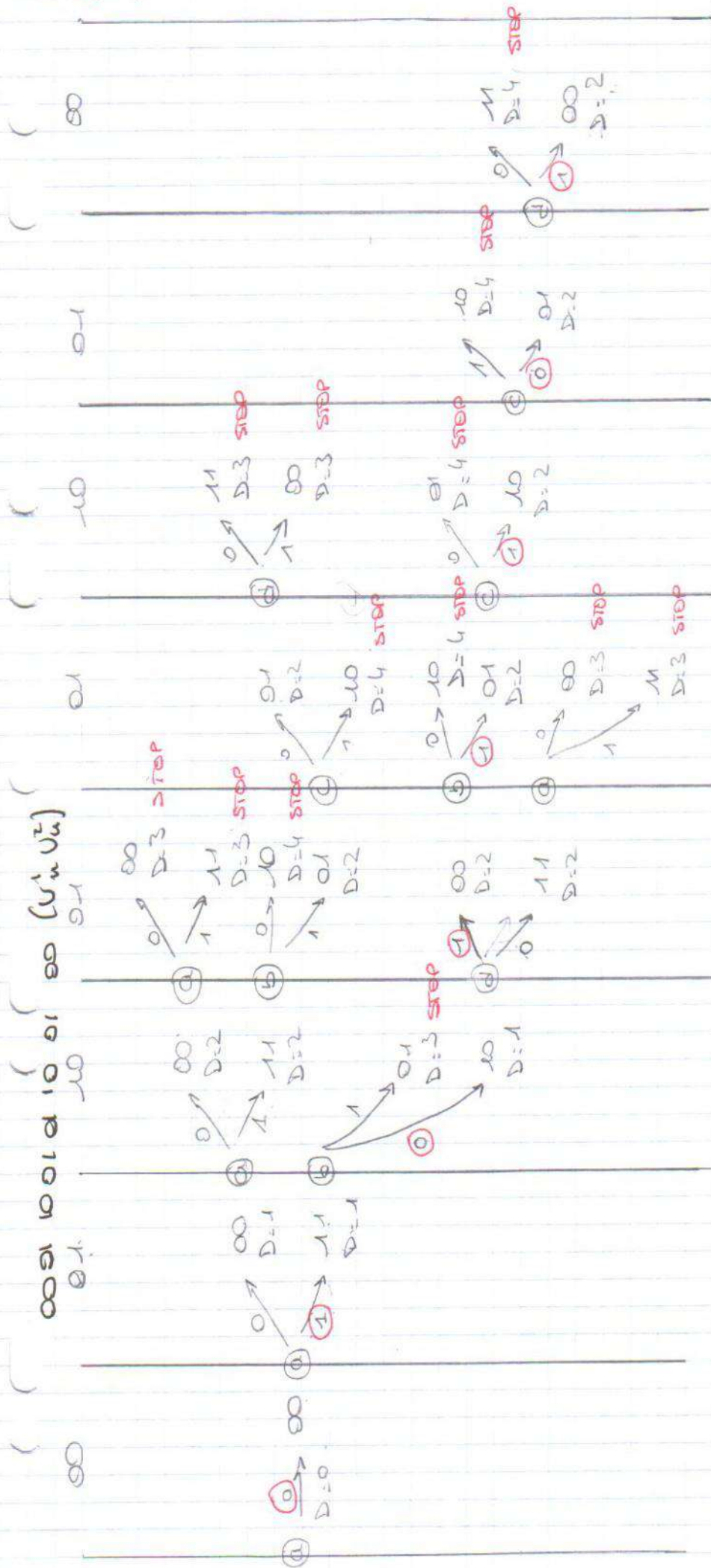
- Etape 2: algorithme de Viterbi en utilisant le diagramme de transition, en partant du même état initial @ (≠ protocole)

Choix de survie par des distances de Hamming  $D < 3$  (= modif de l'algo de Viterbi)

↳ écart entre message restitué et msg reçu.  
On arrête à partir du moment où on a 3 erreurs ou arrêté.  
Il faut un minimum d'erreur.

D : Distance de Hamming ⇒ écart entre message reçu et message reconstitué

valeur D : différences (annulées) entre entrée et ce qu'on trouve.



$D_{min} = 2$  à la fin  $\Rightarrow$  on remonte l'arbre par decoder le message  
(écriture de droite à gauche)  
 $\hookrightarrow$  lecture de gauche à droite.

Message corrigé: 010111 01 queue  
Message initial: 010111.