TS226

_

Codes convolutifs et codes concaténés associés

Romain Tajan

1er octobre 2020

Plan

- Previously on TS226 . . .
- ▶ Rappels sur l'encodeur
- ▶ Rappels sur le diagramme d'état
- ▶ Rappels sur le treillis
- Rappels sur les décodeurs
- ▶ Rappels sur l'algorithme de Viterbi
- 2 Décodage MAP-Bit des Codes Convolutifs
 - Introduction
 - Décodage MAP-Bit : algorithme BCJR
- 3 Codes concatenés Turbocodes
- Turbo-Codes

QCM

Comment avez-vous trouvé le cours précédent?

- Très difficile
- Difficile
- Moyen
- Simple
- Très simple

Plan

- Previously on TS226 . . .
- ▶ Rappels sur l'encodeur
- Rappels sur le diagramme d'état
- Rappels sur le treillis
- Rappels sur les décodeurs
- ▶ Rappels sur l'algorithme de Viterbi
- Décodage MAP-Bit des Codes Convolutifs
- 3 Codes concatenés Turbocodes
- 4 Turbo-Codes

Rappels / définitions

• Entrée :
$$U(z) = [U^{(0)}(z), U^{(1)}(z) \dots U^{(n_b-1)}(z)]$$

 \to dans ce cours $n_b = 1 \Rightarrow U(z) \to U(z)$

• État :
$$S(z) = [S^{(0)}(z), S^{(1)}(z) \dots S^{(m-1)}(z)]$$

→ m est appelé "mémoire du code"



$$ightarrow$$
 2 m : nombre d'états

• Sortie :
$$C(z) = [C^{(0)}(z), C^{(1)}(z) \dots C^{(m-1)}(z)]$$

$$\rightarrow n_s$$
 nombre de sorties

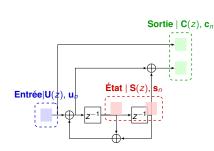
$$\rightarrow$$
 dans l'exemple $n_s = 2$

$$\rightarrow$$
 De façon générale : $\mathbf{C}(z) = U(z)\mathbf{G}(z)$

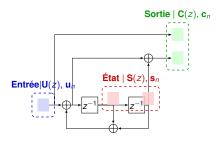
$$\rightarrow$$
 où $\mathbf{G}(z) = \left[\frac{A^{(1)}(z)}{B^{(1)}(z)} \dots \frac{A^{(n_s)}(z)}{B^{(n_s)}(z)} \right]$

• Rendement du code : $R = \frac{\text{\#bits d'info. en entrée}}{\text{\#bits codés en sortie}}$

$$\rightarrow$$
 Ici : $R = \frac{n_b}{n_s} = \frac{1}{2}$

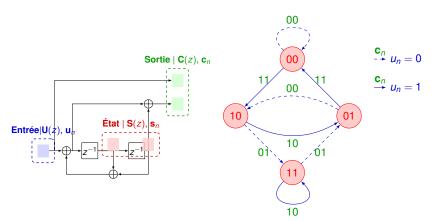


Rappels / définitions

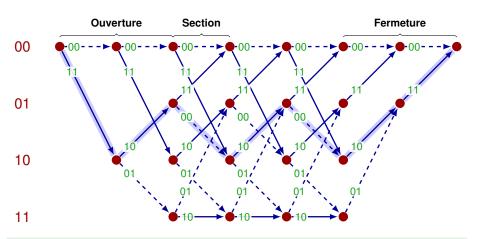


- Code linéaire
- Encodeur récursif / non récursif
- Encodeur systématique / non systématique
- Notation octale

Rappels / définitions



- Message ⇔ chemin dans le graphe
- Mot de code ⇔ étiquettes le long du chemin dans le graphe
- Nécessité de définir (au moins) un état initial



- On souhaite envoyer le message : $\mathbf{u} = [1, 1, 0, 1, 0]$
- On calcule le mot de code : **c** = [1 1, 1 0, 0 0, 1 0, 0 0, 1 0, 1 1]
- On envoie le signal : $\mathbf{x} = [-1, -1, -1, 1, 1, -1, 1, -1, -1, -1]$

Décodage des Codes convolutifs

$$\mathbf{u} \in \{0,1\}^K \\ \underline{\text{Message}} \quad \text{Encodeur} \quad \mathbf{c} \in \mathcal{C} \subset \{0,1\}^L \\ \underline{\text{Mot de code}} \quad 1-2\mathbf{c} \quad \mathbf{Signal} \\ \underline{\text{Transmis}} \quad p(\mathbf{y}|\mathbf{x}) \quad \mathbf{Signal} \\ \underline{\text{Observ\'e}} \quad \mathbf{D\'ecodeur} \quad \mathbf{u} \in \{0,1\}^K \\ \underline{\text{Message}} \quad \mathbf{u} \in \{0,1\}^K \\ \underline{\text{Message}} \quad \mathbf{u} \in \{0,1\}^K \\ \underline{\text{Signal}} \quad \mathbf{u} \in \{0,1\}^K \\ \underline{\text{Signal}} \quad \mathbf{u} \in \{0,1\}^K \\ \underline{\text{Message}} \quad \mathbf{u} \in \{0$$

- Le Max. A Posteriori (MAP) : $\hat{\mathbf{u}} = \underset{\mathbf{u} \in \{0,1\}^K}{\operatorname{argmax}} \mathbb{P}(\mathbf{U} = \mathbf{u} | \mathbf{y})$
 - → Minimise la probabilité d'erreur trame

- Le Max. de vraisemblance (ML) : $\hat{\mathbf{u}} = \underset{\mathbf{u} \in \{0,1\}^K}{\operatorname{argmax}} p(\mathbf{y}|\mathbf{u}) = \underset{\mathbf{c} \in \mathcal{C}}{\operatorname{argmin}} \sum_{\ell=0}^{L-1} \mathbf{c}_{\ell} \mathbf{y}_{\ell}^T$
 - → CC : Équivalent moins complexe du MAP, algorithme de Viterbi

- Le Max. A Posteriori Bit (MAP-Bit) : $\hat{u}_i = \operatorname*{argmax}_{u_i \in \{0,1\}} \mathbb{P}(U_i = u_i | \mathbf{y})$
 - → Minimise la probabilité d'erreur binaire

TS226 CC et Turbo-Codes

Romain Tajan

K Nombre de bits dans le message :

• Taille message + fermeture :
$$L = K + m$$

• Le message envoyé :
$$\mathbf{u} = [u_0, u_1, \dots, u_{K-1}]$$

$$oldsymbol{c}$$
 Le mot de code émis : $oldsymbol{c} = [oldsymbol{c}_0, \ oldsymbol{c}_1, \ \dots, \ oldsymbol{c}_{L-1}],$ où $oldsymbol{c}_\ell = [c_\ell^{(0)}, c_\ell^{(1)}]$

$$ullet$$
 Le signal observé : $ullet y = [ullet y_0, \ ullet y_1, \ \dots, \ ullet y_{L-1}],$ où $ullet y_\ell = [y_\ell^{(0)}, y_\ell^{(1)}]$

• Le message reçu :
$$\hat{\mathbf{u}} = [\hat{u}_0, \ \hat{u}_1, \ \dots, \ \hat{u}_{K-1}] = \phi^{-1}(\hat{\mathbf{c}})$$

Solution 1 : explorer tous les messages (eq. tous les mots de codes)

K Nombre de bits dans le message :

I = K + mTaille message + fermeture :

 $\mathbf{u} = [u_0, u_1, \dots, u_{K-1}]$ Le message envoyé :

 $\mathbf{c} = [\mathbf{c}_0, \ \mathbf{c}_1, \ \dots, \ \mathbf{c}_{L-1}], \text{ où } \mathbf{c}_{\ell} = [c_{\ell}^{(0)}, c_{\ell}^{(1)}]$ Le mot de code émis :

 $\mathbf{y} = [\mathbf{y}_0, \ \mathbf{y}_1, \ \dots, \ \mathbf{y}_{L-1}], \text{ où } \mathbf{y}_{\ell} = [y_{\ell}^{(0)}, y_{\ell}^{(1)}]$ Le signal observé :

$$\begin{split} \hat{\mathbf{c}} &= \underset{\mathbf{c} \in \mathcal{C}}{\operatorname{argmin}} \sum_{\ell=0}^{L-1} \mathbf{c}_{\ell} \mathbf{y}_{\ell}^T \\ \hat{\mathbf{u}} &= [\hat{u}_0, \ \hat{u}_1, \ \dots, \ \hat{u}_{K-1}] = \phi^{-1}(\hat{\mathbf{c}}) \end{split}$$
Décodeur ML :

• Le message reçu :

• Solution 1 : explorer tous les messages (eq. tous les mots de codes) \rightarrow il y en a 2^K ...

 Nombre de bits dans le message : K

I = K + mTaille message + fermeture :

 $\mathbf{u} = [u_0, u_1, \dots, u_{K-1}]$ Le message envoyé :

 $\mathbf{c} = [\mathbf{c}_0, \ \mathbf{c}_1, \ \dots, \ \mathbf{c}_{L-1}], \text{ où } \mathbf{c}_{\ell} = [c_{\ell}^{(0)}, c_{\ell}^{(1)}]$ Le mot de code émis :

 $\mathbf{y} = [\mathbf{y}_0, \ \mathbf{y}_1, \ \dots, \ \mathbf{y}_{L-1}], \text{ où } \mathbf{y}_{\ell} = [y_{\ell}^{(0)}, y_{\ell}^{(1)}]$ Le signal observé :

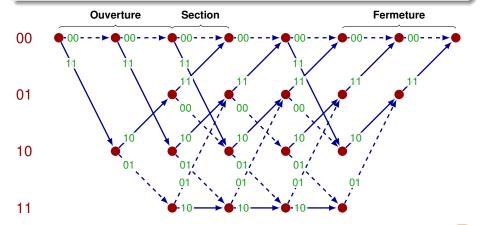
 $\hat{\boldsymbol{c}} = \mathop{\mathsf{argmin}}_{\boldsymbol{c} \in \mathcal{C}} \sum_{\ell=0}^{L-1} \boldsymbol{c}_{\ell} \boldsymbol{y}_{\ell}^T$ Décodeur ML :

 $\hat{\mathbf{u}} = [\hat{u}_0, \hat{u}_1, \dots, \hat{u}_{K-1}] = \phi^{-1}(\hat{\mathbf{c}})$ • Le message reçu :

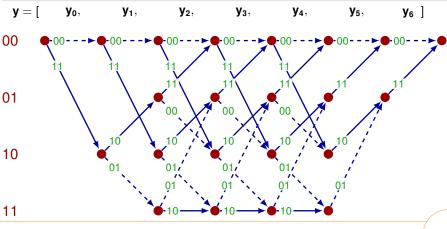
- Solution 1 : explorer tous les messages (eq. tous les mots de codes) \rightarrow il y en a 2^K ...
- Solution 2 : utiliser le treillis + la forme de la fonction de coût → algorithme de Viterbi

$$\bullet \; \mathsf{Soit} \; J_n(s_n) = \min_{\mathbf{c} \in \mathcal{C}(s_0 \to s_n)} \sum_{\ell=0}^{n-1} \mathbf{c}_\ell \mathbf{y}_\ell^T$$

• Le décodage ML est équivalent à trouver l'antécédent de $J_L(s_L)$ où $s_0 = s_L = 0$



- $\mathcal{P}(s_n)$: parents de l'état s_n , i.e. ensemble des s_{n-1} tels que $s_{n-1} \to s_n$ existe
- Algotithme de Viterbi : pour chaque $n \in [0, L-1]$ et chaque $s_n \in \mathcal{S}_n$ calculer $J_n(s_n) = \min_{s_{n-1} \in \mathcal{P}(s_n)} \left[J_{n-1}(s_{n-1}) + \mathbf{c}_{n-1}(s_{n-1} \to s_n) \mathbf{y}_{n-1}^{\mathsf{T}} \right]$
- $\hat{\mathbf{u}}$: chemin survivant minimisant $J_L(s_L)$



- $\mathcal{P}(s_n)$: parents de l'état s_n , i.e. ensemble des s_{n-1} tels que $s_{n-1} \to s_n$ existe
- **Algotithme de Viterbi** : pour chaque $n \in [0, L-1]$ et chaque $s_n \in \mathcal{S}_n$ calculer $J_n(s_n) = \min_{s_{n-1} \in \mathcal{P}(s_n)} \left[J_{n-1}(s_{n-1}) + \mathbf{c}_{n-1}(s_{n-1} \to s_n) \mathbf{y}_{n-1}^T \right]$
- $\hat{\mathbf{u}}$: chemin survivant minimisant $J_l(s_l)$

 $\mathbf{y} = [$ **y**₀, y_1 , **y**₂, **y**₃, **y**₄, y_5 **y**₆]

01

00

10

11

- $\mathcal{P}(s_n)$: parents de l'état s_n , i.e. ensemble des s_{n-1} tels que $s_{n-1} \to s_n$ existe
- **Algotithme de Viterbi** : pour chaque $n \in [0, L-1]$ et chaque $s_n \in S_n$ calculer $J_n(s_n) = \min_{s_{n-1} \in \mathcal{P}(s_n)} \left[J_{n-1}(s_{n-1}) + \mathbf{c}_{n-1}(s_{n-1} \to s_n) \mathbf{y}_{n-1}^T \right]$
- $\hat{\mathbf{u}}$: chemin survivant minimisant $J_l(s_l)$

 $\mathbf{y} = [$ **y**₀, y_1 , **y**₂, **y**₃, **y**₄,

 $J_{2}(2)$

01

00

10

11

 y_5

y₆]

- **Algotithme de Viterbi** : pour chaque $n \in [0, L-1]$ et chaque $s_n \in S_n$ calculer $J_n(s_n) = \min_{s_{n-1} \in \mathcal{P}(s_n)} \left[J_{n-1}(s_{n-1}) + \mathbf{c}_{n-1}(s_{n-1} \to s_n) \mathbf{y}_{n-1}^{\mathsf{T}} \right]$
- $\hat{\mathbf{u}}$: chemin survivant minimisant $J_L(s_L)$

y₀,

y₁,

y₂,

у3,

y₄,

y₅,

y6]

01

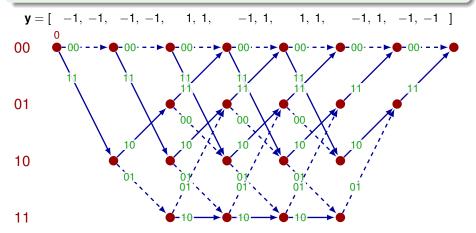
00

10

 $J_{2}(2)$

Sommer chaque $J_2(s_2)$ avec sa métrique de branche. Ne conserver que le chemin minimisant $J_3(3)$.

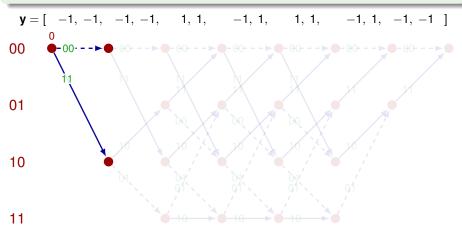
11

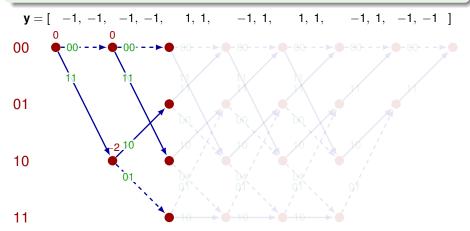


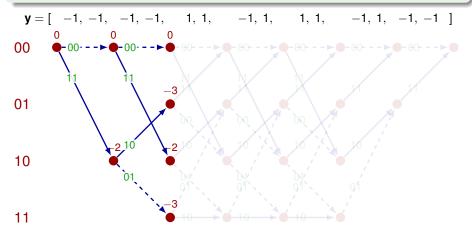
 $\mathbf{u} = [1, 1, 0, 1, 0]$, reçoit-on le message sans erreur?

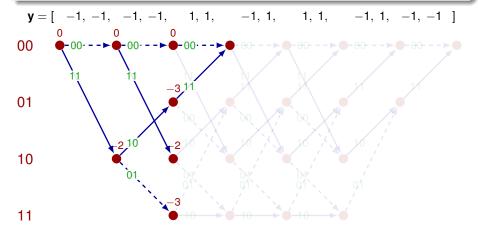
01

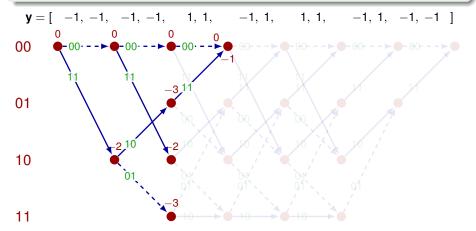


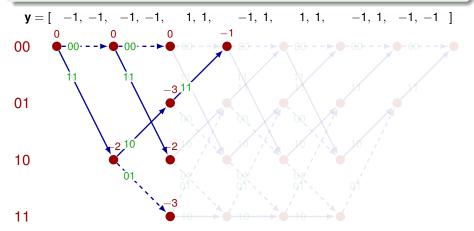


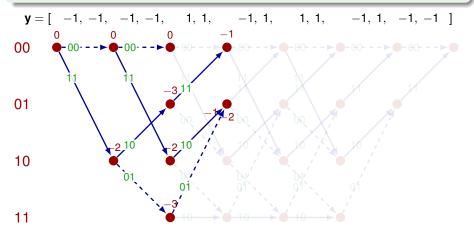


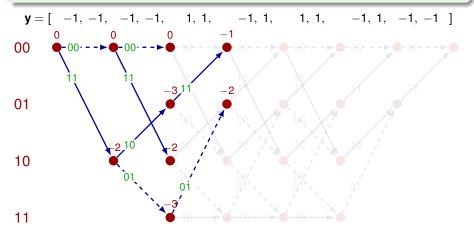


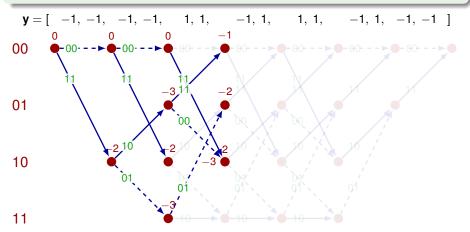


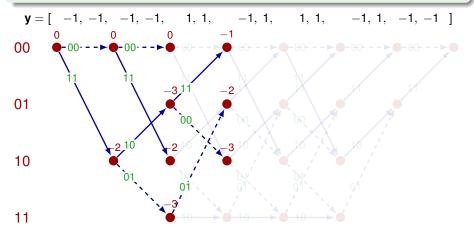


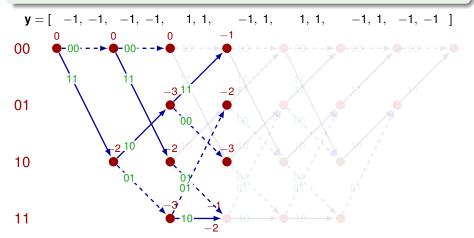


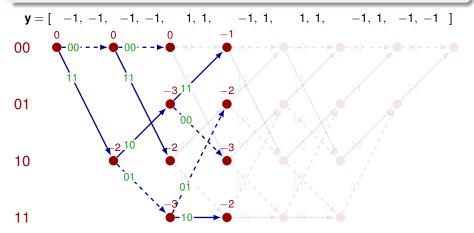


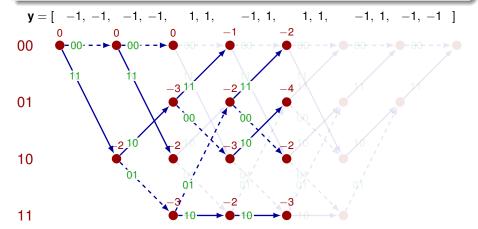


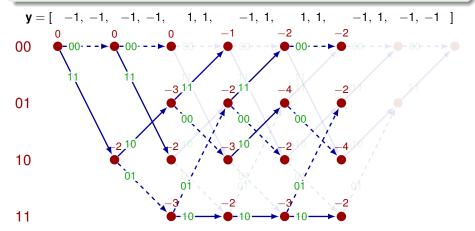


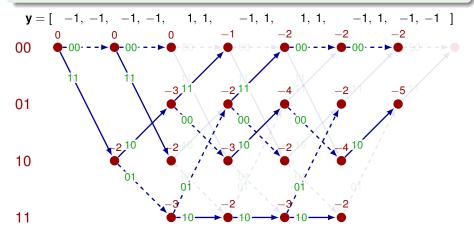


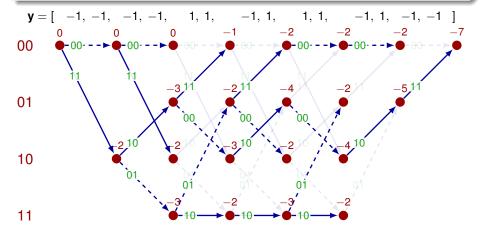


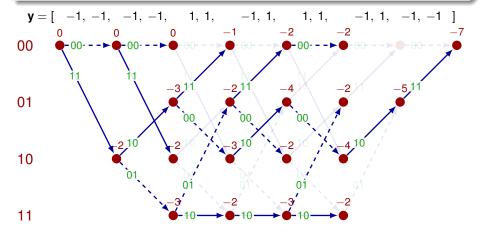


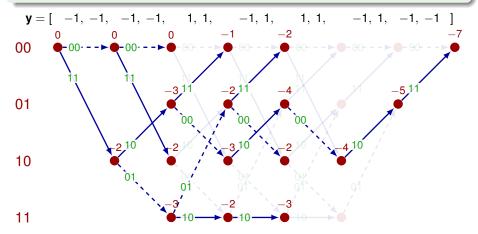


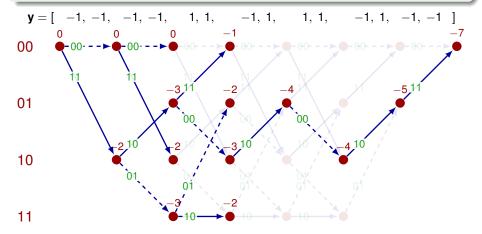


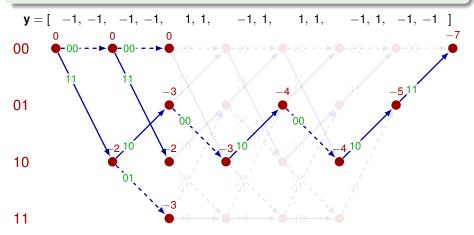


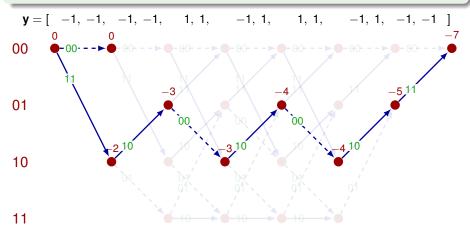


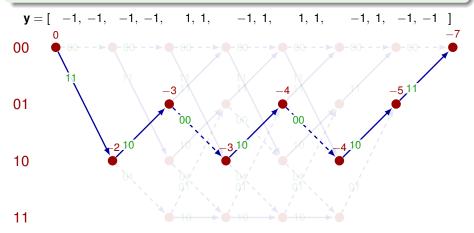












Plan

- 1 Previously on TS226 . . .
- Décodage MAP-Bit des Codes Convolutifs
 - Introduction
- Décodage MAP-Bit : algorithme BCJR
- 3 Codes concatenés Turbocodes
- 4 Turbo-Codes

Introduction

$$\mathbf{u} \in \{0,1\}^K \\ \underline{\text{Message}} \quad \text{Encodeur} \quad \mathbf{c} \in \mathcal{C} \subset \{0,1\}^L \\ \underline{\text{Mot de code}} \quad 1-2\mathbf{c} \quad \underbrace{\text{Signal}}_{\text{transmis}} \quad \underbrace{p(\mathbf{y}|\mathbf{x})}_{p(\mathbf{y}|\mathbf{x})} \quad \underbrace{\mathbf{y} \in \mathbb{R}^L}_{\text{Signal}} \\ \underline{\text{Décodeur}} \quad \underbrace{\hat{\mathbf{u}} \in \{0,1\}^K}_{\text{Message}} \\ \underline{\text{estimé}}$$

Le décodeur du Maximum A Posteriori - Bit (MAP-Bit) est la fonction de y définie par

$$\hat{u}_\ell = rg\max_{u_\ell \in \{0,1\}} \mathbb{P}(U_\ell = u_\ell | \mathbf{y})$$

- Le décodeur MAP-Bit minimise la probabilité d'erreur binaire.
- En pratique, on calcule le Logarithme du Rapport de Vraisemblance (LLR) suivant :

$$L(u_{\ell}) = \log \left(\frac{\mathbb{P}(U_{\ell} = 0|\mathbf{y})}{\mathbb{P}(U_{\ell} = 1|\mathbf{y})} \right)$$

- Le signe de $L(u_{\ell})$ représente la décision : $\hat{u}_{\ell} = \begin{cases} 0, \text{ si } L(u_{\ell}) \geq 0 \\ 1, \text{ sinon.} \end{cases}$
- Le **module** de $L(u_{\ell})$ i.e. $|L(u_{\ell})|$ représente la **fiabilité** de la décision.
- Un décodeur produisant de telles valeurs est dit **souple**.

15 / 27

Algorithme BCJR (Bahl Cocke Jelinek Raviv)

L'algorithme BCJR repose sur deux principes :

1 Les LLR $(L(u_\ell))$ peuvent êtres calculés sur le treillis :

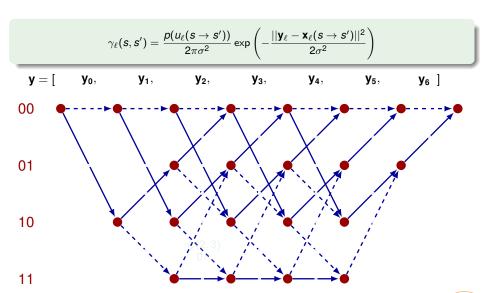
$$L(u_{\ell}) = \log \left(\frac{\sum_{(s \to s') \in \mathcal{U}_0} \alpha_{\ell}(s) \gamma_{\ell}(s, s') \beta_{\ell+1}(s')}{\sum_{(s \to s') \in \mathcal{U}_1} \alpha_{\ell}(s) \gamma_{\ell}(s, s') \beta_{\ell+1}(s')} \right)$$

où

- $\alpha_\ell(s) = p(s_\ell = s, \mathbf{y}_0^{\ell-1})$ est une **métrique de nœud** appelée **métrique aller**
- $\beta_{\ell}(s) = p(\mathbf{y}_{\ell}^{L-1}|s_{\ell}=s)$ est une métrique de nœud appelée métrique retour
- $\gamma_{\ell}(s,s') = p(s_{\ell+1} = s' | s_{\ell} = s, y_{\ell})$ est une métrique de branche
- 2 Les métriques de nœuds et de branches se calculent elles-mêmes sur le treillis :

$$\begin{array}{lcl} \alpha_{\ell+1}(s') & = & \displaystyle\sum_{s \in \mathcal{S}} \alpha_{\ell}(s) \gamma_{\ell}(s,s') \\ \\ \beta_{\ell}(s) & = & \displaystyle\sum_{s' \in \mathcal{S}} \beta_{\ell+1}(s') \gamma_{\ell}(s,s') \\ \\ \gamma_{\ell}(s,s') & = & \displaystyle\frac{p(u_{\ell}(s \to s'))}{2\pi\sigma^2} \exp\left(-\frac{||\mathbf{y}_{\ell} - \mathbf{x}_{\ell}(s \to s')||^2}{2\sigma^2}\right) \end{array}$$

Métrique de branche $\gamma_{\ell}(s, s')$



Métrique de branche $\gamma_{\ell}(s, s')$

$$\gamma_\ell(s,s') = rac{p(u_\ell(s o s'))}{2\pi\sigma^2} \exp\left(-rac{||\mathbf{y}_\ell - \mathbf{x}_\ell(s o s')||^2}{2\sigma^2}
ight)$$

$$y = [\qquad y_0, \qquad y_1, \qquad y_2, \qquad y_3, \qquad y_4, \qquad y_5, \qquad y_6 \]$$

00

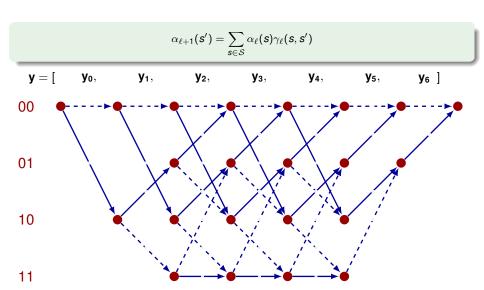
01

10

 $\gamma_2(2,3)$

11

Récursion "aller" : calcul des $\alpha_{\ell}(s)$



Récursion "aller" : calcul des $\alpha_{\ell}(s)$

$$\alpha_{\ell+1}(s') = \sum_{s \in \mathcal{S}} \alpha_{\ell}(s) \gamma_{\ell}(s, s')$$

$$\mathbf{y} = [\quad \mathbf{y_0}, \quad \mathbf{y_1}, \quad \mathbf{y_2}, \quad \mathbf{y_3}, \quad \mathbf{y_4}, \quad \mathbf{y_5}, \quad \mathbf{y_6} \]$$

$$00$$

$$11$$

$$\alpha_3(3) = \sum_{s \in \mathcal{S}} \alpha_2(s) \gamma_2(s, 3)$$

Récursion "aller" : calcul des $\alpha_{\ell}(s)$

$$\alpha_{\ell+1}(s') = \sum_{s \in \mathcal{S}} \alpha_{\ell}(s) \gamma_{\ell}(s, s')$$

$$\mathbf{y} = [\quad \mathbf{y_0}, \quad \mathbf{y_1}, \quad \mathbf{y_2}, \quad \mathbf{y_3}, \quad \mathbf{y_4}, \quad \mathbf{y_5}, \quad \mathbf{y_6} \]$$

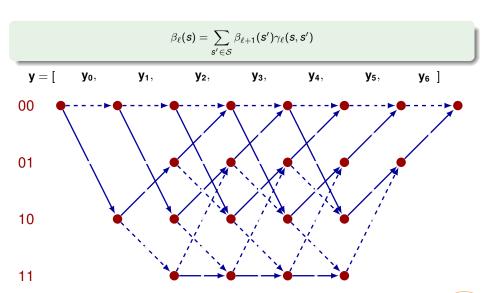
$$00 \qquad \qquad \gamma_2(0, 3) = 0$$

$$01 \qquad \qquad \alpha_2(1) \qquad \qquad \gamma_2(1, 3) = 0$$

$$10 \qquad \qquad \alpha_2(2) \qquad \qquad \qquad \gamma_2(2, 3)$$

$$11 \qquad \qquad \alpha_2(3) \qquad -\gamma_2(3, 3) \qquad \alpha_3(3) = \sum_{s \in \mathcal{S}} \alpha_2(s) \gamma_2(s, 3)$$

Récursion "retour" : calcul des $\beta_{\ell}(s)$



Récursion "retour" : calcul des $\beta_{\ell}(s)$

$$eta_\ell(s) = \sum_{s' \in \mathcal{S}} eta_{\ell+1}(s') \gamma_\ell(s,s')$$
 $\mathbf{y} = [\quad \mathbf{y}_0, \quad \mathbf{y}_1, \quad \mathbf{y}_2, \quad \mathbf{y}_3, \quad \mathbf{y}_4, \quad \mathbf{y}_5, \quad \mathbf{y}_6]$

01

00

10

11
$$\beta_3(3) = \sum_{s' \in S} \beta_4(s') \gamma_3(3, s') \bullet$$

TS226 CC et Turbo-Codes

Récursion "retour" : calcul des $\beta_{\ell}(s)$

$$\beta_{\ell}(s) = \sum_{s' \in S} \beta_{\ell+1}(s') \gamma_{\ell}(s, s')$$

$$\mathbf{y} = [\quad \mathbf{y_0}, \quad \mathbf{y_1}, \quad \mathbf{y_2}, \quad \mathbf{y_3}, \quad \mathbf{y_4}, \quad \mathbf{y_5}, \quad \mathbf{y_6}]$$

$$00$$

$$\gamma_3(3, 0) = 0$$

$$\beta_4(0)$$

$$01$$

$$\gamma_3(3, 1) \bullet \beta_4(2)$$

$$\gamma_3(3, 2) = 0$$

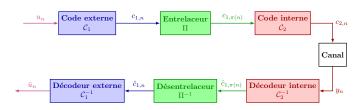
$$11$$

$$\beta_3(3) = \sum_{s' \in S} \beta_4(s') \gamma_3(3, s') \bullet \gamma_3(3, 3) \bullet \beta_4(3)$$

Plan

- 1 Previously on TS226 ...
- 2 Décodage MAP-Bit des Codes Convolutifs
- 3 Codes concatenés Turbocodes
- 4 Turbo-Codes

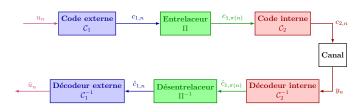
Concaténation série - Définition



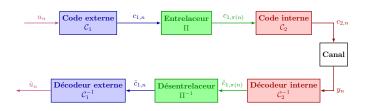
Remarques

- Jusqu'aux années 1980 :
 - $\rightarrow \mathcal{C}_1$: **code linéaire en bloc** corrigeant jusqu'à t erreurs (code RS, code BCH)
 - $ightarrow \ \mathcal{C}_2$: code convolutif
- Rendement : R = R₁R₂
- Entrelaceur : permute les éléments de c₁
- <u>Désentrelaceur</u> : remet les éléments à leur place avant décodage
 - ightarrow Permet de disperser les erreurs commises en **rafale** par \mathcal{C}_2^{-1} pour qu'elles apparaissent **isolées** et soient corrigées par \mathcal{C}_1^{-1}

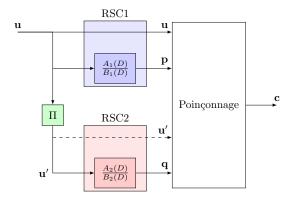
Concaténation série - Émetteur



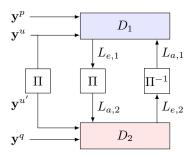
Concaténation série - Récepteur



Turbocode et concaténation parallèle



Turbocode et concaténation parallèle



TS226 CC et Turbo-Codes

Dernier QCM

Comment avez-vous trouvé ce cours?

- A Très difficile
- B Difficile
- Moyen
- Simple
- Très simple

#QDLE#S#ABCDE#30#