

TS226

-

Codes correcteur d'erreur

Romain Tajan

11 septembre 2019

Plan

- 1 Introduction au codage / définitions
 - ▷ Sur la modélisation du canal
 - ▷ Code correcteur d'erreur
 - ▷ Probabilité d'erreur

- 2 Théorie de l'information / Capacité d'un canal
 - ▷ Capacité d'un canal
 - ▷ Théorème de Shannon
 - ▷ Rappels de théorie de l'information (VA continues)
 - ▷ Capacité d'un canal à entrées continues

Dernier QCM

Comment avez-vous trouvé ce cours ?

- ☐ A Très difficile
- ☐ B Difficile
- ☐ C Moyen
- ☐ D Simple
- ☐ E Très simple

#QDLE#S#ABCDE#30#

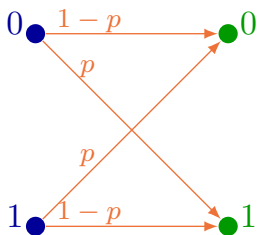
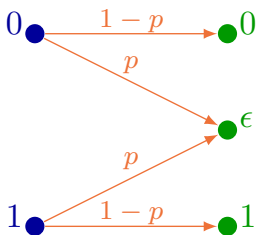
Plan

1 Introduction au codage / définitions

- ▷ Sur la modélisation du canal
- ▷ Code correcteur d'erreur
- ▷ Probabilité d'erreur

2 Théorie de l'information / Capacité d'un canal

Canaux BEC / BSC



Exemple de QCM

J'ai compris la définition d'un code correcteur d'erreurs

- ☐ A Très bien
- ☐ B Bien
- ☐ C Mal
- ☐ D Très mal

#QDLE#S#ABCD#30#

Code (M, n)

Un code (M, n) pour le canal $(\mathcal{X}^n, \mathcal{Y}^n, p(\mathbf{y}|\mathbf{x}))$ est composé de 3 éléments

- Un ensemble de M **messages**. On notera cet ensemble $\mathcal{M} = \{0, 1, \dots, M-1\}$
- Une fonction d'**encodage** (ou encodeur) notée ϕ :

$$\begin{aligned}\phi : \mathcal{M} &\rightarrow \mathcal{X}^n \\ W &\mapsto \mathbf{X} = \phi(W)\end{aligned}$$

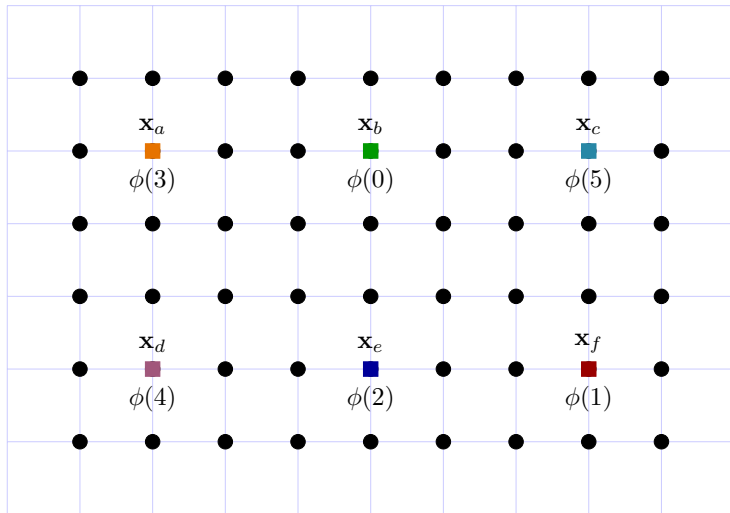
$\phi(\cdot)$ doit être **injective**

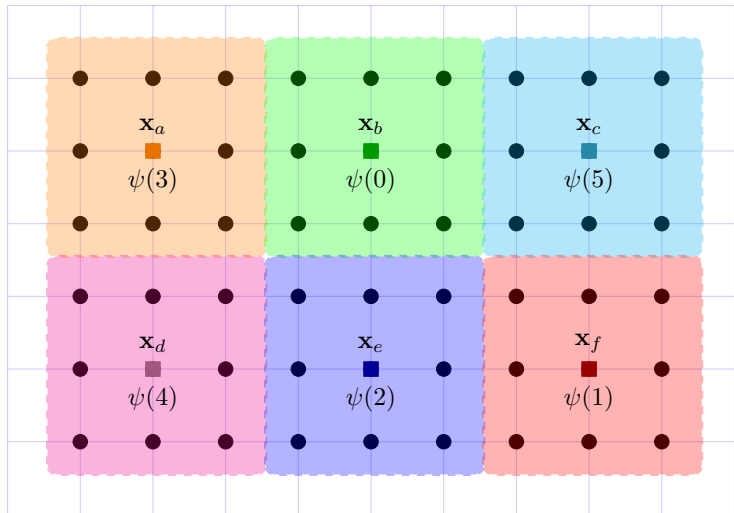
- Une fonction de **décodage** (ou décodeur) notée ψ :

$$\begin{aligned}\psi : \mathcal{Y}^n &\rightarrow \mathcal{M} \\ \mathbf{Y} &\mapsto \hat{W} = \psi(\mathbf{Y})\end{aligned}$$

$\psi(\cdot)$ doit être **surjective**







Exemple de QCM

Soit un code à 3 répétitions, travaillant sur des blocs de messages de 4 bits. Ce code est un code

- A (4, 12)
- B (16, 12)
- C (2, 16)
- D (4, 16)

#QDLE#S#AB*CD#60#

Probabilité d'erreur

Si le mot de code $W = w$ est envoyé, une erreur se produit ssi $\hat{W} \neq w$.

La probabilité associée à cet événement est notée

$$\begin{aligned}\lambda_w &= \mathbb{P}(\hat{W} \neq w | W = w) \\ &= \mathbb{P}(\psi(\mathbf{Y}) \neq w | W = w)\end{aligned}$$

Définitions

- **Probabilité d'erreur maximale** : $P_m^{(n)} = \max_w \lambda_w$
- **Probabilité d'erreur moyenne** : $P_e^{(n)} = \mathbb{P}(\hat{W} \neq W) = \frac{1}{M} \sum_{w=0}^{M-1} \lambda_w$

Décodage du Maximum a Posteriori

Définition

- Soit \mathcal{C} un code (M, n) donné.
- Le **décodeur** du **Maximum A Posteriori (MAP)** est la fonction de \mathbf{y} définie par :

$$\Psi_{MAP}(\mathbf{y}) = \operatorname{argmax}_{w \in \mathcal{M}} \mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})$$

Le décodeur MAP minimise P_e

Plan

1 Introduction au codage / définitions

2 Théorie de l'information / Capacité d'un canal

- ▷ Capacité d'un canal
- ▷ Théorème de Shannon
- ▷ Rappels de théorie de l'information (VA continues)
- ▷ Capacité d'un canal à entrées continues

Capacité

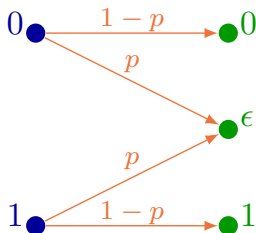
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

$$C = \sup_{p(x)} \mathbb{I}(X, Y)$$

Remarque

- 1 Le canal ($p(y|x)$) étant **fixé**, $\mathbb{I}(X, Y)$ ne "dépend" que de $p(x)$.
- 2 La capacité est atteinte pour au moins une distribution ($\mathbb{I}(X, Y)$ est une fonction continue concave de $p(x)$)
- 3 $C \geq 0$
- 4 $C \leq \log |\mathcal{X}|$
- 5 $C \leq \log |\mathcal{Y}|$

Capacité du canal BEC



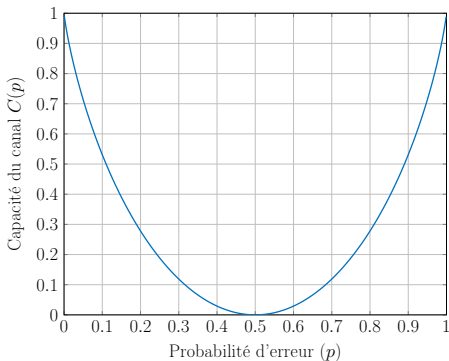
- 1 Montrer que la capacité du canal BEC vaut $C(p) = 1 - p$
- 2 Trouver la distribution $p(x)$ d'atteindre cette capacité
- 3 Pour quelle(s) valeur(s) de p cette capacité est-elle nulle ?

Capacité du canal BSC

La **capacité** en bits par symbole d'entrée du canal BSC vaut

$$C(p) = 1 + p \log_2(p) + (1 - p) \log_2(1 - p)$$

est atteinte ssi $X \sim \mathcal{B}(0.5)$



Remarques

- 1 Si $p = 0.5$, $C(0.5) = 0$
i.e. la connaissance de Y ne permet pas de diminuer l'incertitude sur X .
- 2 Si $p = 0$ ou $p = 1$ capacité maximale

Théorème du codage canal de Shannon

Soit $(\mathcal{X}, \mathcal{Y}, p(y|x))$ un **canal discret sans mémoire** de capacité $C \geq 0$ et soit $R < C$

- 1 il existe une suite de codes $(C_n)_{n \geq 1}$ où C_n est de longueur n , de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

$$\lambda^{(n)} \rightarrow 0, \text{ et } R_n \rightarrow R$$

Théorème du codage canal de Shannon

Soit $(\mathcal{X}, \mathcal{Y}, p(y|x))$ un **canal discret sans mémoire** de capacité $C \geq 0$ et soit $R < C$

- 1 il existe une suite de codes $(C_n)_{n \geq 1}$ où C_n est de longueur n , de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

$$\lambda^{(n)} \rightarrow 0, \text{ et } R_n \rightarrow R$$

- 2 Réciproquement, s'il existe une suite de codes $(C_n)_{n \geq 1}$ telle que $\lambda^{(n)} \rightarrow 0$ alors

$$\limsup_n R_n \leq C$$

Soient X et Y deux variables aléatoires continues dans les alphabets $\mathcal{X} \subset \mathbb{R}$ et $\mathcal{Y} \subset \mathbb{R}$

Entropies

- **Entropie de X** : $\mathbb{H}(X) = - \int_{\mathcal{X}} p(x) \log(p(x)) dx$
- **Entropie jointe de X et Y** : $\mathbb{H}(X, Y) = - \int_{\mathcal{X} \times \mathcal{Y}} p(x, y) \log(p(x, y)) dx dy$
- **Entropie conditionnelle de Y sachant X** : $\mathbb{H}(Y|X) = - \int_{\mathcal{X} \times \mathcal{Y}} p(x, y) \log(p(y|x)) dx dy$

Information mutuelle

$$\begin{aligned} \mathbb{I}(X, Y) &= \mathbb{H}(X) - \mathbb{H}(X|Y) \\ &= \mathbb{H}(Y) - \mathbb{H}(Y|X) \\ &= \int_{\mathcal{X} \times \mathcal{Y}} p(x, y) \log \left(\frac{p(x, y)}{p(x)p(y)} \right) dx dy \end{aligned}$$

Propriétés

- 1 Si $\mathbb{V}(X) \leq \sigma^2$ alors $\mathbb{H}(X) \leq \log(2\pi e\sigma^2)$ avec égalité ssi $X \sim \mathcal{N}(0, \sigma^2)$.

Propriétés

- 1 Si $\mathbb{V}(X) \leq \sigma^2$ alors $\mathbb{H}(X) \leq \log(2\pi e\sigma^2)$ avec égalité ssi $X \sim \mathcal{N}(0, \sigma^2)$.
- 2 Pour $\beta \in \mathbb{R}$ et $\alpha > 0$, $\mathbb{H}(\alpha X + \beta) = \mathbb{H}(X) + \log(\alpha)$

Propriétés

- 1 Si $\mathbb{V}(X) \leq \sigma^2$ alors $\mathbb{H}(X) \leq \log(2\pi e\sigma^2)$ avec égalité ssi $X \sim \mathcal{N}(0, \sigma^2)$.
- 2 Pour $\beta \in \mathbb{R}$ et $\alpha > 0$, $\mathbb{H}(\alpha X + \beta) = \mathbb{H}(X) + \log(\alpha)$
- 3 $\mathbb{H}(X, Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
- 4 $\mathbb{H}(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- 5 $\mathbb{H}(Y|X) \leq \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes

Propriétés

- 1 Si $\mathbb{V}(X) \leq \sigma^2$ alors $\mathbb{H}(X) \leq \log(2\pi e\sigma^2)$ avec égalité ssi $X \sim \mathcal{N}(0, \sigma^2)$.
- 2 Pour $\beta \in \mathbb{R}$ et $\alpha > 0$, $\mathbb{H}(\alpha X + \beta) = \mathbb{H}(X) + \log(\alpha)$
- 3 $\mathbb{H}(X, Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
- 4 $\mathbb{H}(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- 5 $\mathbb{H}(Y|X) \leq \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
- 6 L'entropie (jointe, conditionnelle) dans le cas continu peut prendre des valeurs négatives.

Propriétés

- 1 Si $\mathbb{V}(X) \leq \sigma^2$ alors $\mathbb{H}(X) \leq \log(2\pi e\sigma^2)$ avec égalité ssi $X \sim \mathcal{N}(0, \sigma^2)$.
- 2 Pour $\beta \in \mathbb{R}$ et $\alpha > 0$, $\mathbb{H}(\alpha X + \beta) = \mathbb{H}(X) + \log(\alpha)$
- 3 $\mathbb{H}(X, Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
- 4 $\mathbb{H}(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- 5 $\mathbb{H}(Y|X) \leq \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
- 6 L'entropie (jointe, conditionnelle) dans le cas continu peut prendre des valeurs négatives.
- 7 $\mathbb{I}(X, Y) \geq 0$ avec égalité ssi X et Y sont indépendantes.

Capacité

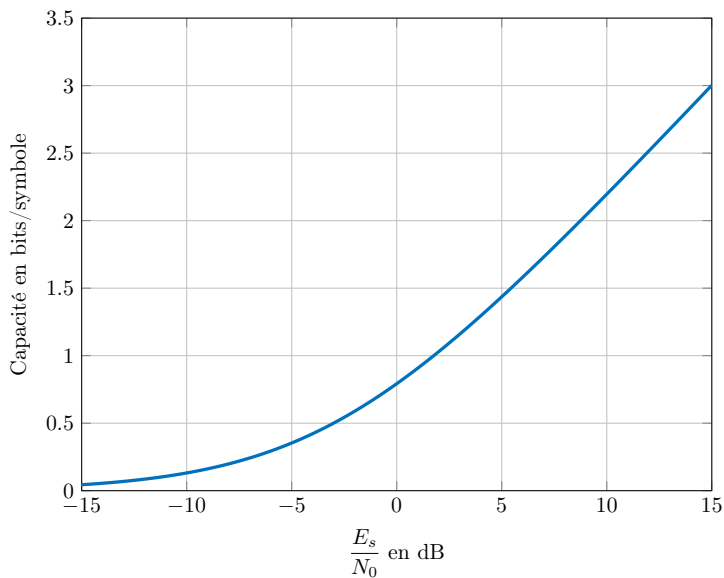
La **capacité d'un canal Gaussien sans mémoire** avec contrainte d'énergie E_s est

$$\begin{aligned} C &= \sup_{p(x): \mathbb{V}(X) \leq E_s} \mathbb{I}(X, Y) \\ &= \frac{1}{2} \log \left(1 + 2 \frac{E_s}{N_0} \right) \end{aligned}$$

- Le supremum est ici pris sur les densités de probabilités $p(x)$ telles que $\mathbb{V}(X)$.
- Le supremum est atteint par $p(x) = \mathcal{N}(0, E_s)$
- Capacité en nats/accès canal (nats/symbole)

Remarque

- 1 Cette expression fait apparaître de rapport signal à bruit $\frac{E_s}{N_0}$
- 2 La capacité croît lentement en fonction du RSB (log)



Théorème du codage canal de Shannon

Soient $(\mathcal{X}, \mathcal{Y}, p(y|x))$ un **canal gaussien de variance** $\frac{N_0}{2}$, une contrainte de puissance E_s et R tel que

$$0 < R < \frac{1}{2} \log_2 \left(1 + 2 \frac{E_s}{N_0} \right)$$

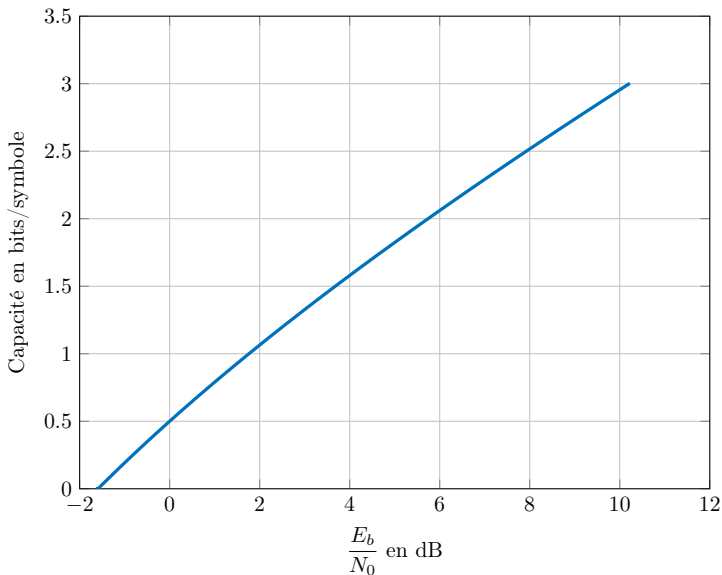
- 1 il existe une suite de codes $(C_n)_{n \geq 1}$ où C_n est de longueur n , de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

$$\lambda^{(n)} \rightarrow 0, \text{ et } R_n \rightarrow R$$

- 2 Réciproquement, s'il existe une suite de codes $(C_n)_{n \geq 1}$ telle que $\lambda^{(n)} \rightarrow 0$ alors

$$\limsup_n R_n \leq C$$

Retour sur l'efficacité énergétique



Débit maximal en bits/s | Bande passante

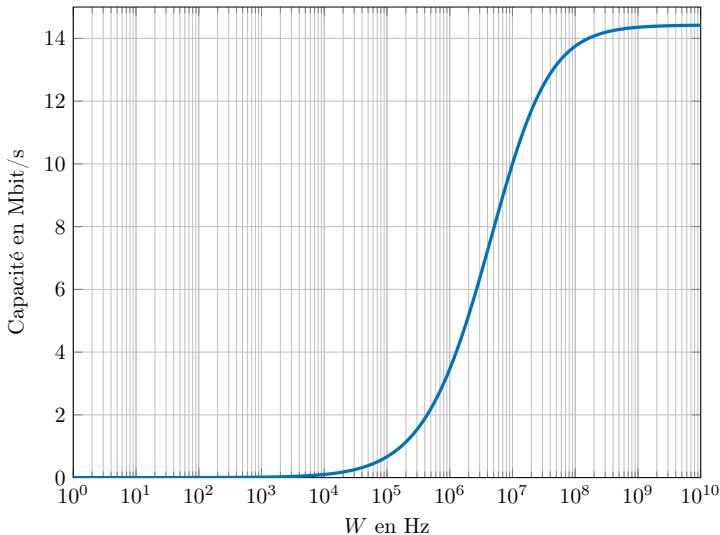
Supposons une transmission en **bande de base** telle que :

- le signal occupe une bande passante W
- le signal analogique possède une puissance P
- le canal est additif gaussien de DSP $\frac{N_0}{2}$

alors le débit binaire maximal atteignable vaut

$$D_b = W \log_2 \left(1 + \frac{P}{N_0 W} \right)$$

Débit maximal en bits/s | Bande passante



Dernier QCM

Comment avez-vous trouvé ce cours ?

- ☐ A Très difficile
- ☐ B Difficile
- ☐ C Moyen
- ☐ D Simple
- ☐ E Très simple

#QDLE#S#ABCDE#30#