TS226
-
Codes correcteur d'erreur

Romain Tajan

25 septembre 2019

Plan

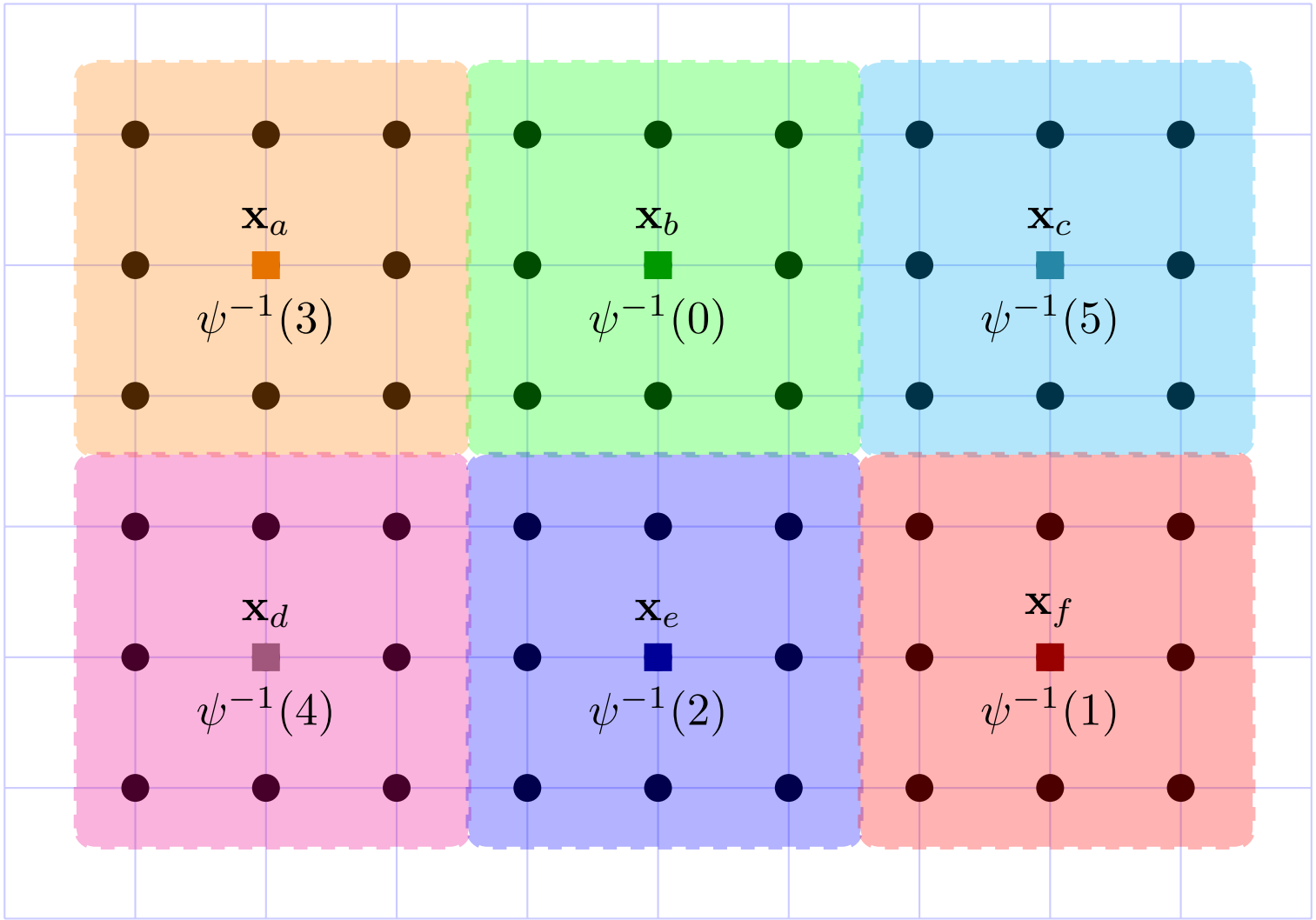
Dernier QCM

Comment avez-vous trouvé ce cours ?

A. Très difficile
B. Difficile
C. Moyen
D. Simple
E. Très simple

#QDLE#S#ABCDE#30#

Plan


$\mathbf{x}_a$
$\psi^{-1}(3)$
$\mathbf{x}_b$
$\psi^{-1}(0)$
$\mathbf{x}_c$
$\psi^{-1}(5)$
$\mathbf{x}_d$
$\psi^{-1}(4)$
$\mathbf{x}_e$
$\psi^{-1}(2)$
$\mathbf{x}_f$
$\psi^{-1}(1)$

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 :

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

Le décodeur MAP minimise P_e

Plan

Capacité

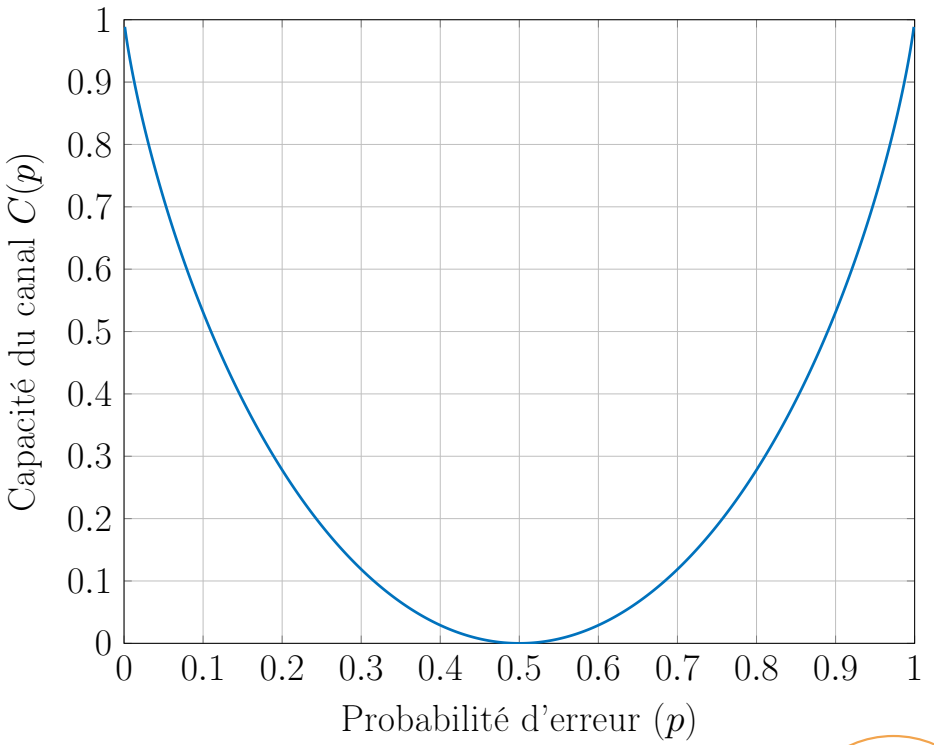
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

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

La **capacité** du canal BSC

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

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



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 $(\mathcal{C}_n)_{n\geq 1}$ où $\mathcal{C}_n$ est de longueur n, de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

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

2. Réciproquent, s'il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ telle que $\lambda^{(n)} \to 0$ alors

$$\limsup_n R_n \leq C$$

1. Quelque soit $\epsilon > 0$, il existe **toujours** un code $\mathcal{C}_n$ de longueur n et de rendement $R_n < C$ tel que $\lambda^{(n)} \leq \epsilon$.
2. La remarque précédente ne dit cependant rien sur la longueur n de ce code, qui **peut être éventuellement très grande**.
3. L'item (2) du théorème montre que C est une borne supérieure des rendements de codes **fiables**
4. La preuve de (1) (Cover & Thomas **Information theory**) repose sur une génération aléatoire des codes $\mathcal{C}_n$

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

Information mutuelle

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

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

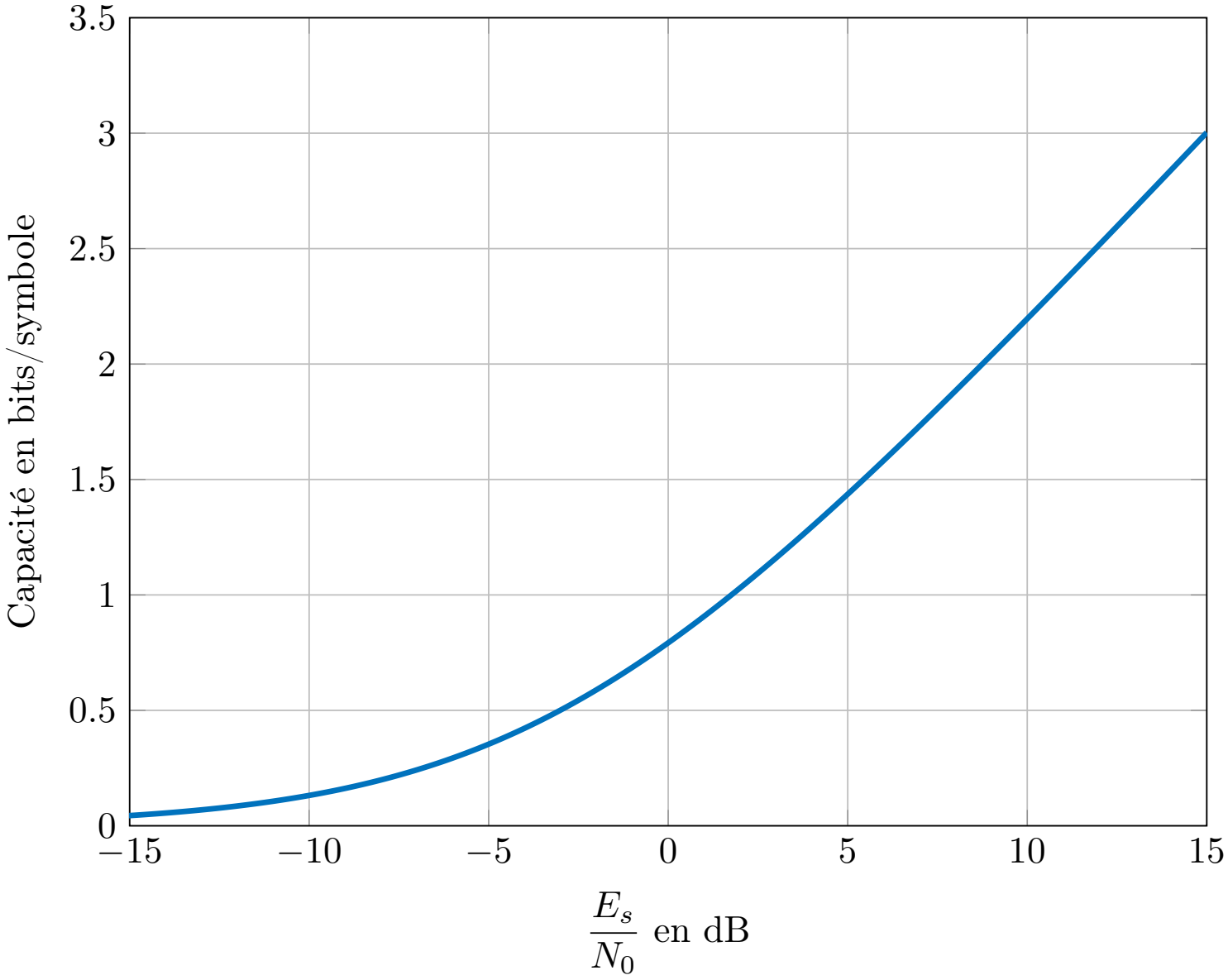
La **capacité d'un canal Gaussien sans mémoire** avec contrainte d'énergie E_s est

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

- 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)


3.5
3
2.5
2
1.5
1
0.5
0
Capacité en bits/symbole
−15
−10
−5
0
5
10
15
$\frac{E_s}{N_0}$ en dB

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

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

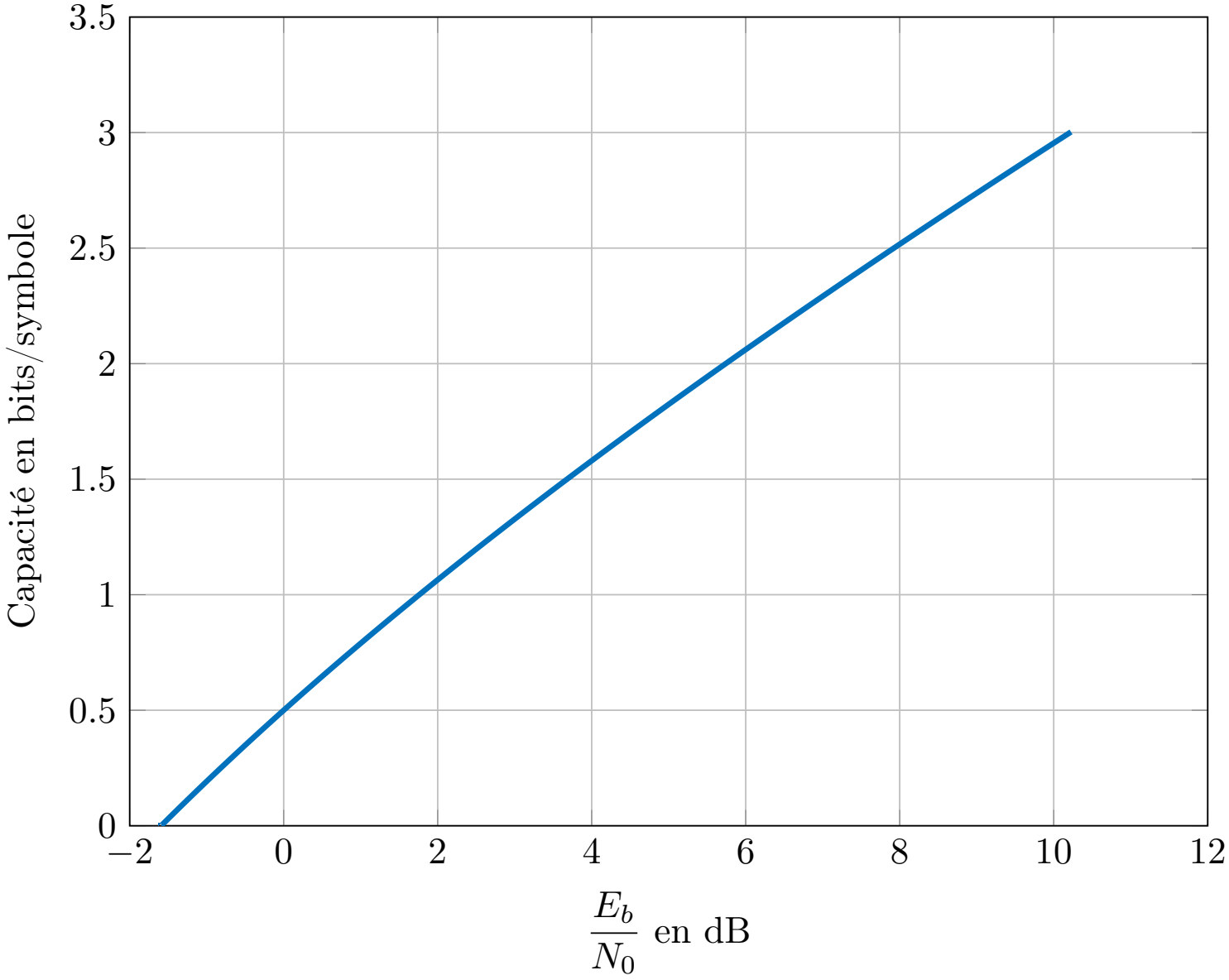
1. il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ où $\mathcal{C}_n$ est de longueur n, de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

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

2. Réciproquent, s'il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ telle que $\lambda^{(n)} \to 0$ alors

$$\limsup_n R_n \leq C$$

Retour sur l'efficacité énergétique



Débit maximal en bits/s | Bande passante

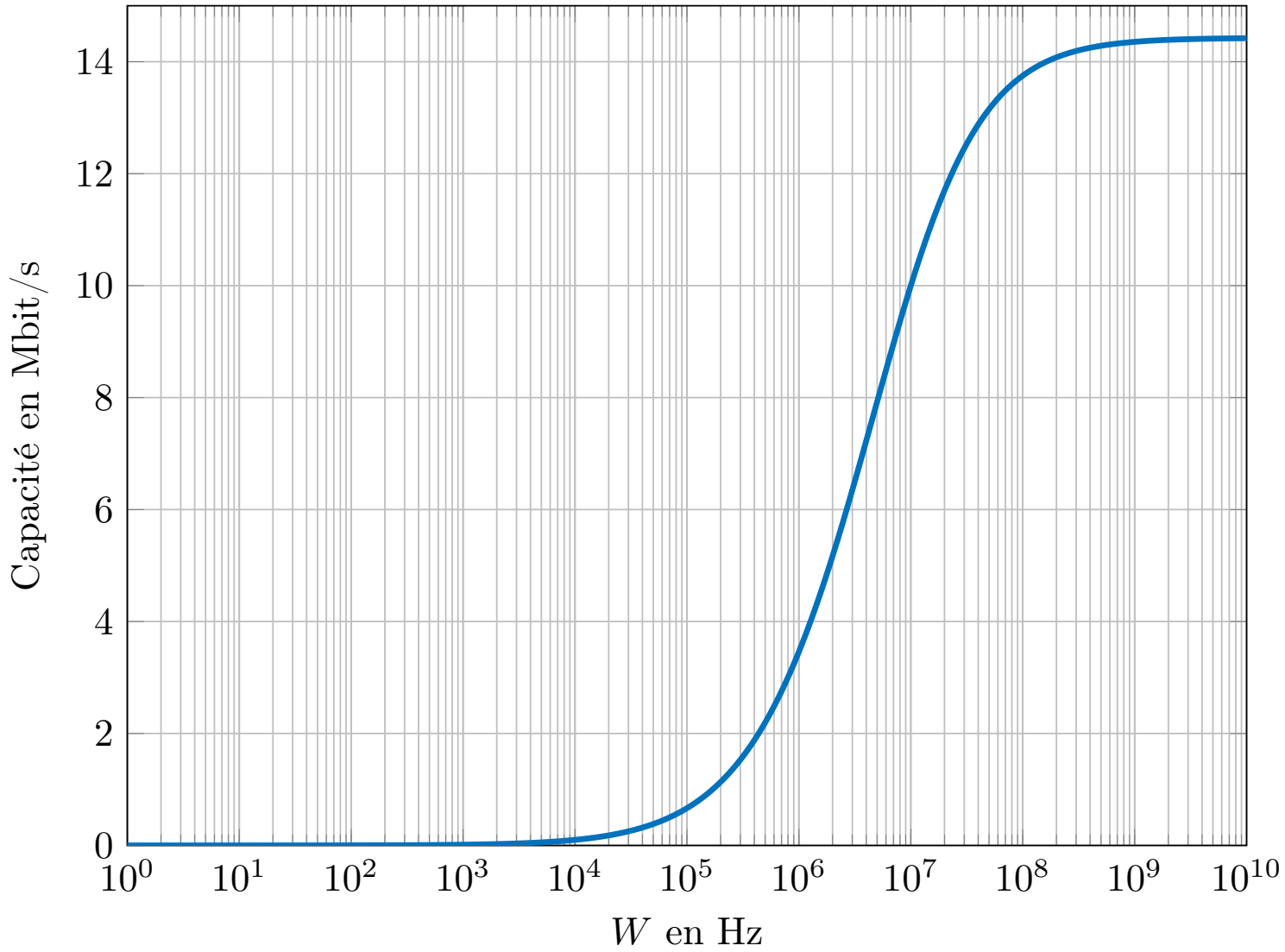
Supposons une transmission en **bande de base** telle que :

- 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



Plan

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)
3. $\mathbb{F}_2$ est un corps fini à deux éléments ($\mathbb{Z}/2\mathbb{Z}$)

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)
3. $\mathbb{F}_2$ est un corps fini à deux éléments ($\mathbb{Z}/2\mathbb{Z}$)
4. Par la suite on notera $\oplus \rightsquigarrow +$

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)
3. $\mathbb{F}_2$ est un corps fini à deux éléments ($\mathbb{Z}/2\mathbb{Z}$)
4. Par la suite on notera $\oplus \rightsquigarrow +$
5. $(\mathbb{F}_2^n, +, \cdot)$ est un **espace vectoriel** où
   - Pour $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, $\quad \mathbf{x} + \mathbf{y} = [x_0 + y_0, x_1 + y_1 \ldots, x_{n-1} + y_{n-1}]$
   - Pour $x \in \mathbb{F}_2$ et $\mathbf{y} \in \mathbb{F}_2^n$, $\quad x \cdot \mathbf{y} = [x \cdot y_0, x \cdot y_1, \ldots, x \cdot y_{n-1}]$

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)

Dans $\mathbb{F}_2$ que vaut $x + x$?

A. 0
B. 1
C. x
D. $\bar{x}$

#QDLE#Q#A*BCD#30#

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)

Dans $\mathbb{F}_2$ que vaut $x \cdot x$?

A. 0
B. 1
C. x
D. $\bar{x}$

#QDLE#Q#ABC*D#30#

Avant de commencer...

Dire si l'assertion suivante est vraie. "Si $\mathbf{x} \in \mathbb{F}_2^n$, alors $-\mathbf{x} = \mathbf{x}$."

A. Vrai

B. Faux

#QDLE#Q#A*B#30#

Code linéaire en bloc

Code linéaire

Un code binaire $\mathcal{C}$ possédant $M = 2^k$ mots de codes de longueur n est dit **linéaire** si et seulement si, il existe k vecteurs de $\mathbb{F}_2^n$ notés $\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}$ tels que tout mot de code $\mathbf{x}$ de c s'écrit comme une combinaison linéaire des vecteurs $\mathbf{g}_i$

$$\mathbf{c} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i$$

Remarques

1. L'ensemble $\mathcal{B}_\mathcal{C} = \{\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}\}$ est appelé **base** de $\mathcal{C}$.
2. $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k (si $\mathcal{B}_\mathcal{C}$ est une base libre)

Dernier QCM

Comment avez-vous trouvé ce cours ?

A. Très difficile
B. Difficile
C. Moyen
D. Simple
E. Très simple

#QDLE#S#ABCDE#30#