TS226
-
Codes correcteur d’erreur

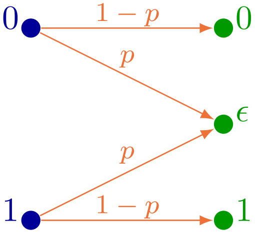
Romain Tajan

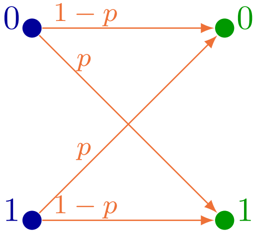
18 octobre 2023

Plan

Plan

Canaux BEC / BSC





Code (M, n)

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

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

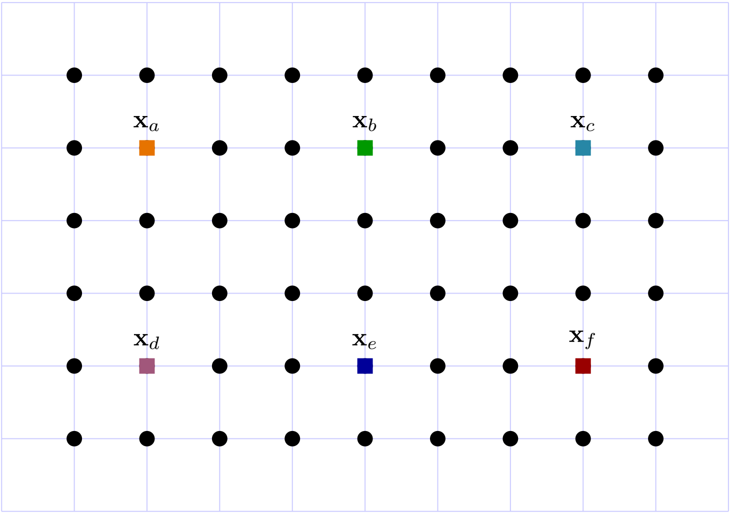
$$\begin{array}{rcl} \phi : \mathcal{M} & \rightarrow & \mathcal{X}^n \\ W & \mapsto & \mathbf{X} = \phi(W) \end{array}$$

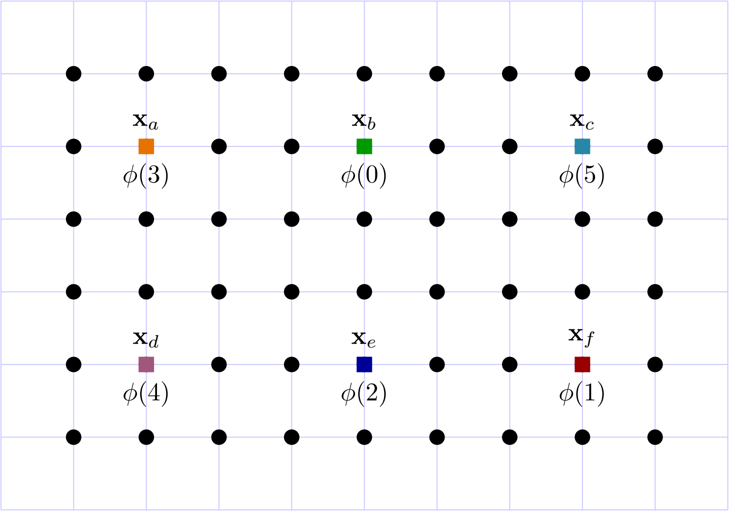
$$\boxed{\phi(\cdot) \text{ doit être } \textbf{injective}}$$

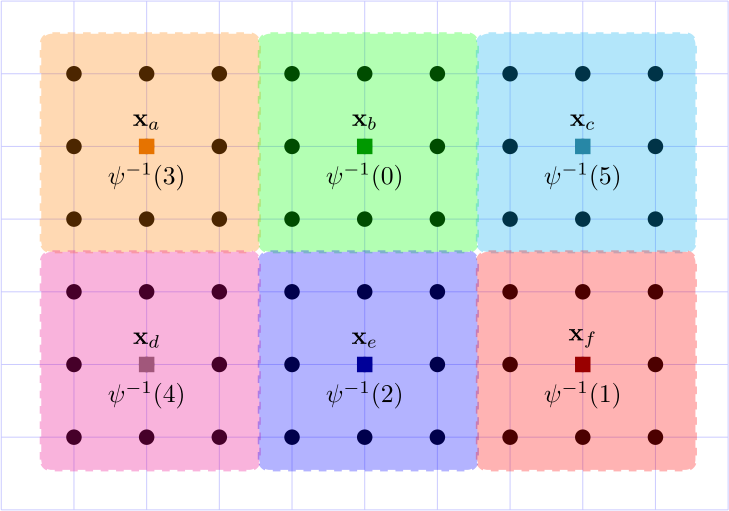
- Une fonction de **décodage** (ou décodeur) notée ψ :

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

$$\boxed{\psi(\cdot) \text{ doit être } \textbf{surjective}}$$


$\mathbf{x}_a$
$\mathbf{x}_b$
$\mathbf{x}_c$
$\mathbf{x}_d$
$\mathbf{x}_e$
$\mathbf{x}_f$


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



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

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

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

Définitions

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

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 :

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

Le décodeur MAP minimise P_e

Plan

Capacité

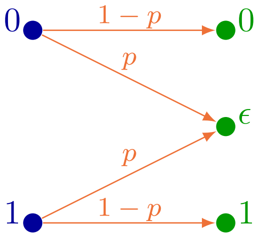
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

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

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



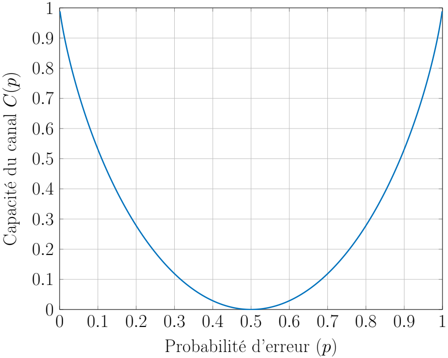
1. Montrer que la capacité du canal BEC vaut $C(p) = 1 - p$
2. Trouver la distribution $p(x)$ permettant d'atteindre cette capacité
3. Pour quelle(s) valeur(s) de p cette capacité est-elle nulle ?

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

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

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

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

2. Réciproquent, s'il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ 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** : $\mathbb{H}(X) = -\displaystyle\int_{\mathcal{X}} p(x)\log(p(x))dx$
- **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

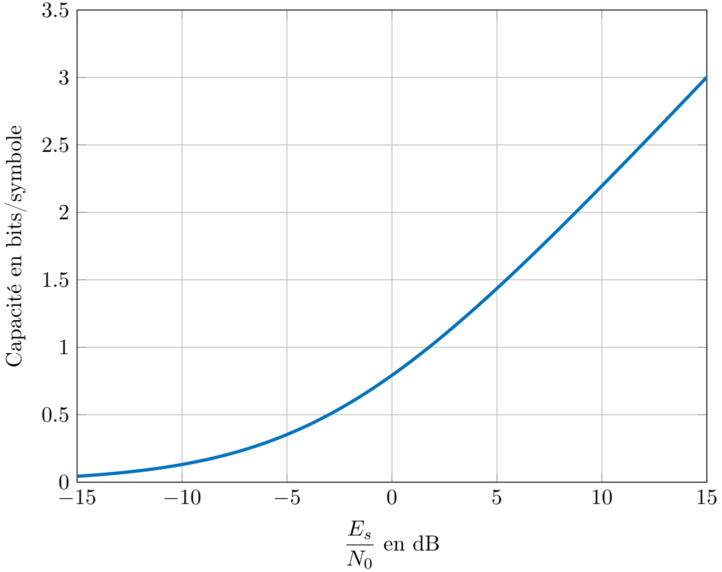
La **capacité d'un canal Gaussien sans mémoire** avec contrainte d'énergie E_s est

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

- 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 $\dfrac{E_s}{N_0}$
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

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

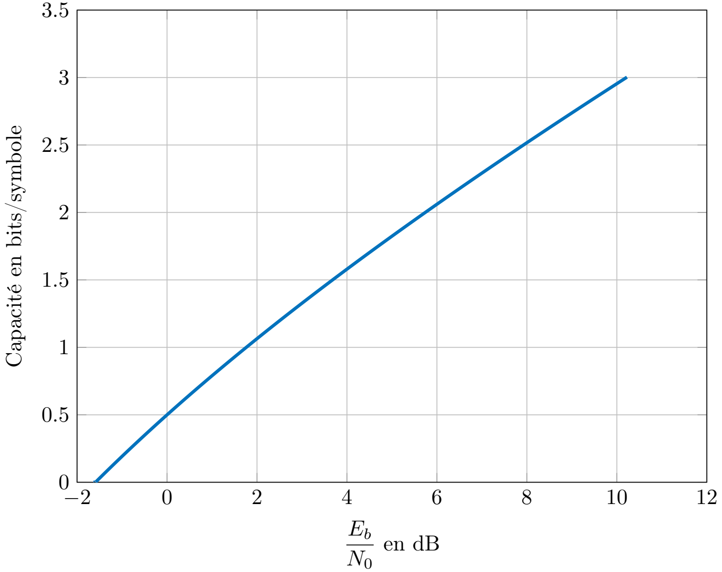
1. il existe une suite de codes $(\mathcal{C}_n)_{n \geq 1}$ où $\mathcal{C}_n$ est de longueur n, de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

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

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