TS226
-
Codes correcteur d’erreur

Romain Tajan

11 septembre 2019

Plan

Exemple de QCM

Comment allez vous aujourd'hui ?

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

#QDLE#S#ABCD#30#

Plan

1. Introduction au codage / définitions
   - ▷ Sur la modélisation du canal
   - ▷ Code correcteur d'erreur
   - ▷ Probabilité d'erreur
   - ▷ Retour sur les enjeux

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

Redéfinissons le canal...

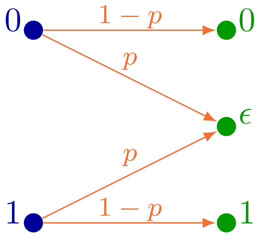
Un **canal** est défini par un triplet : $(\mathcal{X}, \mathcal{Y}, p(y|x))$ où

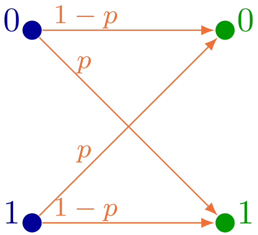
- $\mathcal{X}$ est l'**alphabet d'entrée**
- $\mathcal{Y}$ est l'**alphabet de sortie**
- $p(y|x)$ est la **probabilité de transition**

Soit $n \in \mathbb{N}$ et soit le canal $(\mathcal{X}^n, \mathcal{Y}^n, p(\mathbf{y}|\mathbf{x}))$, ce canal est dit "**sans mémoire**" si sa probabilité de transition vérifie

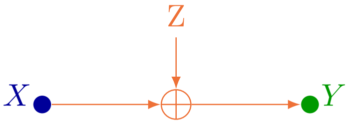
$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i)$$

Canaux BEC / BSC





Le canal additif gaussien



- $\mathcal{X} = \mathbb{R}$ ou $\mathcal{X} = \{-1, 1\}$
- $\mathcal{Y} = \mathbb{R}$
- $p(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(y-x)^2}$

Définition d'un code correcteur d'erreur

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 $\mathcal{M} = \{0, 1, \ldots, M-1\}$
- Une fonction d'**encodage** (ou encodeur) notée ϕ :

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

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

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

Le ratio $R = \frac{\log_2(M)}{n}$ est appelé **rendement** du code (M, n)

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 :

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

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

Enjeux du codage

Compromis entre

- La **taille** du code (n)
- Le **rendement de code** (le débit)
- La **probabilité d'erreur** (maximale ou moyenne)
- La **complexité** de l'encodage
- La **complexité** du décodage

Efficacité spectrale $\Longleftrightarrow$ Codage $\Longleftrightarrow$ Efficacité énergétique

Plan

Soient X et Y deux variables aléatoires discrètes dans les alphabets $\mathcal{X}$ et $\mathcal{Y}$

Entropie de X

$$\mathbb{H}(X) = -\sum_{x \in \mathcal{X}} p(x) \log(p(x))$$

Elle représente la quantité moyenne d'incertitude délivrée par la v.a. X

Soient X et Y deux variables aléatoires discrètes dans les alphabets $\mathcal{X}$ et $\mathcal{Y}$

Entropie de X

$$\mathbb{H}(X) = -\sum_{x\in\mathcal{X}} p(x)\log(p(x))$$

Elle représente la quantité moyenne d'incertitude délivrée par la v.a. X

Entropie jointe de X, Y

$$\mathbb{H}(X,Y) = -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} p(x,y)\log(p(x,y))$$

Elle représente la quantité moyenne d'incertitude délivrée par le couple (X,Y)

Soient X et Y deux variables aléatoires discrètes dans les alphabets $\mathcal{X}$ et $\mathcal{Y}$

Entropie de X

$$\mathbb{H}(X) = -\sum_{x\in\mathcal{X}} p(x)\log(p(x))$$

Elle représente la quantité moyenne d'incertitude délivrée par la v.a. X

Entropie jointe de X, Y

$$\mathbb{H}(X,Y) = -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} p(x,y)\log(p(x,y))$$

Elle représente la quantité moyenne d'incertitude délivrée par le couple (X,Y)

Entropie conditionnelle de Y sachant X

$$\mathbb{H}(Y|X) = -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} p(x,y)\log(p(y|x))$$

Elle représente la quantité moyenne d'incertitude restante sur Y une fois X connue

Propriétés

1. $\mathbb{H}(X) \leq log(|X|)$ avec égalité ssi $X \sim U(X)$ (loi uniforme sur $\mathcal{X}$).
2. $\mathbb{H}(X, Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes
3. $\mathbb{H}(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
4. $\mathbb{H}(Y|X) \leq \mathbb{H}(Y)$ avec égalité ssi X et Y sont indépendantes

Information mutuelle

$$\begin{aligned}\mathbb{I}(X, Y) &= \mathbb{H}(X) - \mathbb{H}(X|Y) \\ &= \mathbb{H}(Y) - \mathbb{H}(Y|X)\end{aligned}$$

Elle représente la quantité moyenne d'incertitude soustraite de X une fois Y connue

Propriétés

1. $\mathbb{I}(X, Y) = \mathbb{I}(Y, X)$
2. $\mathbb{I}(X, Y) \geq 0$ avec égalité ssi X et Y sont indépendantes.

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 $p(x)$.

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 $p(x)$)

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. $C \geq 0$

Capacité

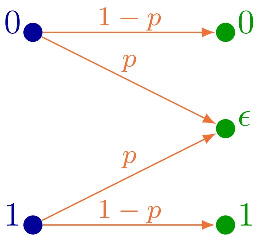
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

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

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



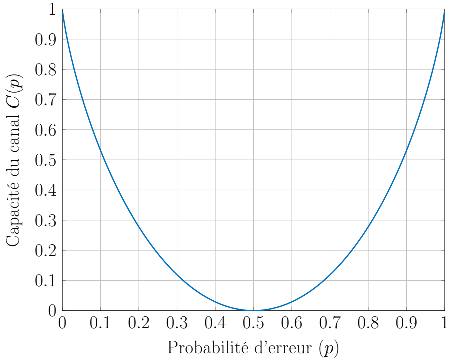
1. Montrer que la capacité du canal BEC vaut $C(p) = 1 - p$
2. Trouver la distribution $p(x)$ d'atteindre cette capacité
3. Pour quelle(s) valeur(s) de p cette capacité est-elle nulle ?

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 $(\mathcal{C}_n)_{n \geq 1}$ 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

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

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

$$\limsup_n R_n \leq C$$

Dernier QCM

Comment avez-vous trouvé ce cours ?

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

#QDLE#S#ABCDE#30#