Théorie de l'information

Thomas Grenier

Hugues Benoit-Cattin

Plan

1. Introduction

1948 : Shannon → Théorie de l'information

Réflexion sur les techniques de communication (XIX°)

- Mécanique, accoustique
- Ondes radio-électrique
- Télégraphe (code morse)
- Téléphone, ….

Système de communication = Σ fonctions physiques réalisables

↳ Mauvaise compréhension des perturbations, des débits …

Vue d'ensemble d'un système de communication indépendante des moyens techniques & physiques

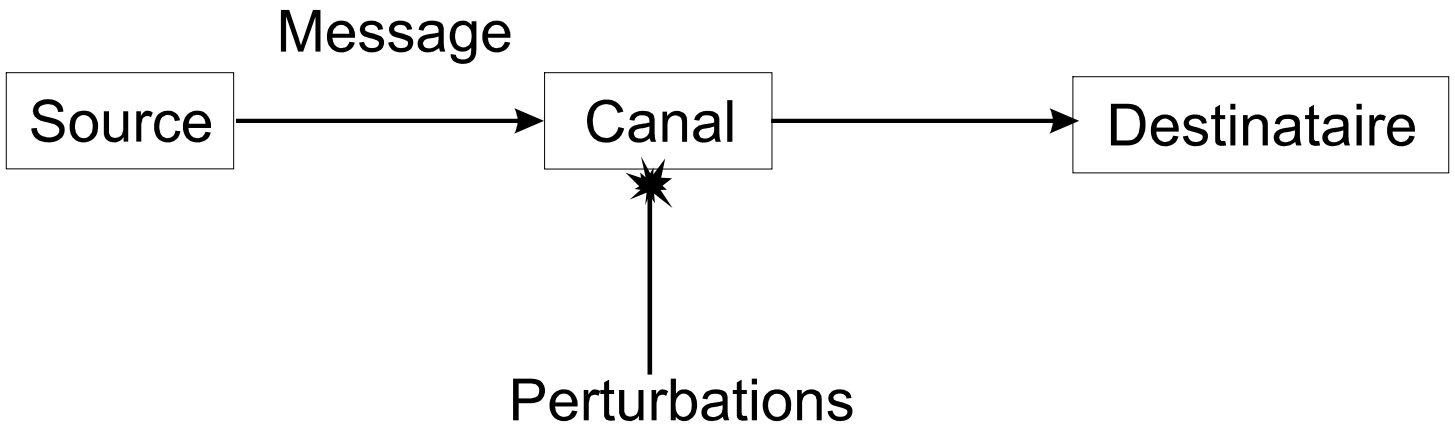
☹ Ca ne sert à rien !

☺ 1960 / conquête spatiale → codage de source

Aujourd'hui 

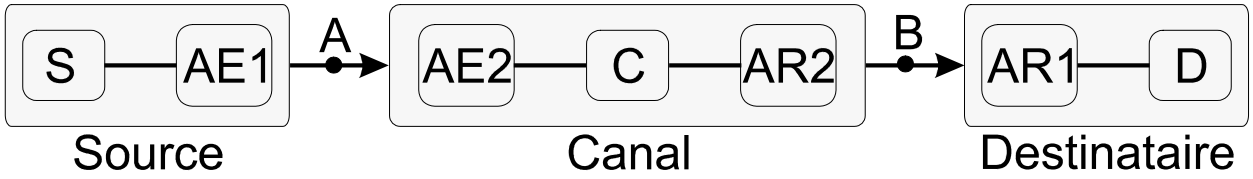
- ✓GSM ⇨ codage de source & canal
- ✓TV Num ⇨ codage de source & canal
- ✓Réseaux ⇨ codage de canal (erreurs)
- ✓@business ⇨ cryptage

- Paradigme de Shannon = modèle sys. com.



Source	=	je parle
Canal	=	l'air ambiant
Perturbations	=	bruit sonore
Destinataire	=	tu écoutes

- Modèle détaillé



✓Th. Signaux ⇨ décrit messages et perturbations

✓Modulation ⇨ modifie les signaux pour les propager

✓Electronique ⇨ réalise les fonctions

✓Th. Information ⇨ propose une mesure quantitative de l'**information** et étudie sa représentation, sa transmission, sa dégradation

✓**Source** : siège d'évènements aléatoires qui constituent le message émis ⇨ **Entropie**

✓**Canal** : transmet et dégrade le message ⇨ **Capacité**

Des messages différents portent la même information, le **codage** cherche le message avec les meilleures propriétés.

✓Codage de source ⇨ supprime la redondance, réduit le coût

✓Codage de canal ⇨ protège contre les perturbations

✓Cryptage/Authentification ⇨ protège des curieux

Deux théorèmes fondamentaux :

- Codage de source
- Codage de canal

2. Sources discrètes & Entropie

Sources débitant des messages sous forme discrète !

✓**Source discrète d'information** : suite de variables aléatoires discrètes X_1, X_2, … X_n

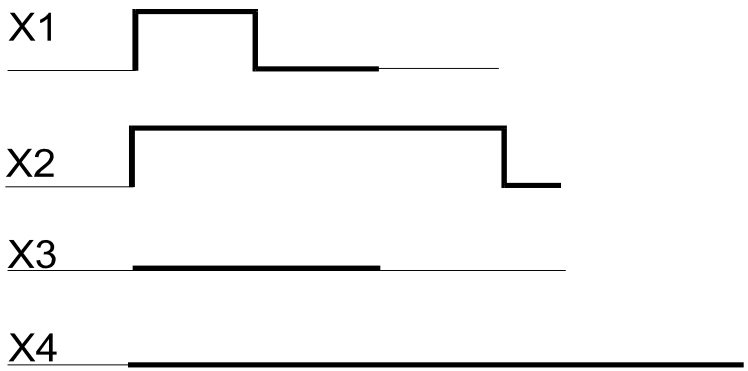
✓**Symbole** ou **lettre** : élément fondamental irréductible contenant une information, cad réalisation particulière de la source d'information.

✓**Mot** : succession finie de symboles

✓**Alphabet** : totalité des D lettres

$[X] = [x_1, x_2, \ldots, x_D]$

Ex : Code morse, 4 symboles



✓**Source discrète sans mémoire** : source pour laquelle la probabilité d'apparition d'un symbole ne dépend pas des symboles précédents

$$p(x_{i_n} / x_{i_{n-1}}, x_{i_{n-2}}, ...) = p(x_{i_n})$$

✓**Source discrète à mémoire** : source pour laquelle la probabilité d'apparition d'un symbole dépend du ou des symboles précédents

✓**Source sationnaire** : source pour laquelle les probabilités d'apparition des différents symboles ne dépendent pas de l'origine des temps

$$p(x_{i_n}) = p(x_{i_{n+k}}) \quad \forall k$$

✓**Source à débit contrôlable** : source pouvant générer des messages comme suite à une commande externe (Télégraphe, .)

✓**Source à débit non contrôlable** : source générant des messages avec un débit fixé, propriété de la source (CD audio)

✓**Source discrète à contraintes fixes** : source pour laquelle certains symboles ne peuvent être utilisés qu'en des conditions déterminées (Morse, …)

✓**Source discrète à contraintes probabilistes** : source à mémoire. Dans un état, la source peut générer n'importe lequel des symboles avec une probabilité qui dépend des symboles précédents (texte …)

✓**Source de Markov** : source pour laquelle la probabilité de générer un symbole ne dépend que du symbole à l'instant n-1

$$p(x_{i_n} / x_{i_{n-1}}, x_{i_{n-2}}, ...) = p(x_{i_n} / x_{i_{n-1}})$$

Quantité d'information & Entropie

- **Quantité d'information propre**

Propriété de l'information = **imprévisibilité**

Quantité d'information propre : $h(x) = f(1/p(x))$

Avec f croissante & f(1)=0

2 evt. indépendants apportent la somme de leur quantité d'info

$$h(x,y) = f(1/p(x,y)) = f(1/p(x).p(y)) = f(\frac{1}{p(x)}) + f(\frac{1}{p(y)}) = h(x) + h(y)$$

f → fonction **logarithme** (Base 2 >> bit)

$$h(x) = \log(1/p(x)) = -\log(p(x))$$

$$h(x,y) = \log(1/p(x,y))$$

$$h(x/y) = \log(1/p(x/y))$$

Règle de Bayes : $p(x,y) = p(x/y).p(y) = p(y/x).p(x) = p(y,x)$

$$h(x,y) = h(x/y) + h(y) = h(y/x) + h(x) = h(y,x)$$

$h(x/y) = h(x)$ si x et y indépendants

Ex → cartes

- **Entropie**

Hyp : source discrète finie stationnaire sans mémoire

Emission = variable aléatoire X

$$p_i = p(X = x_i) \qquad \text{pour} \quad i = 1,2,...,n$$

$$\sum_{i=1}^{n} p_i = 1$$

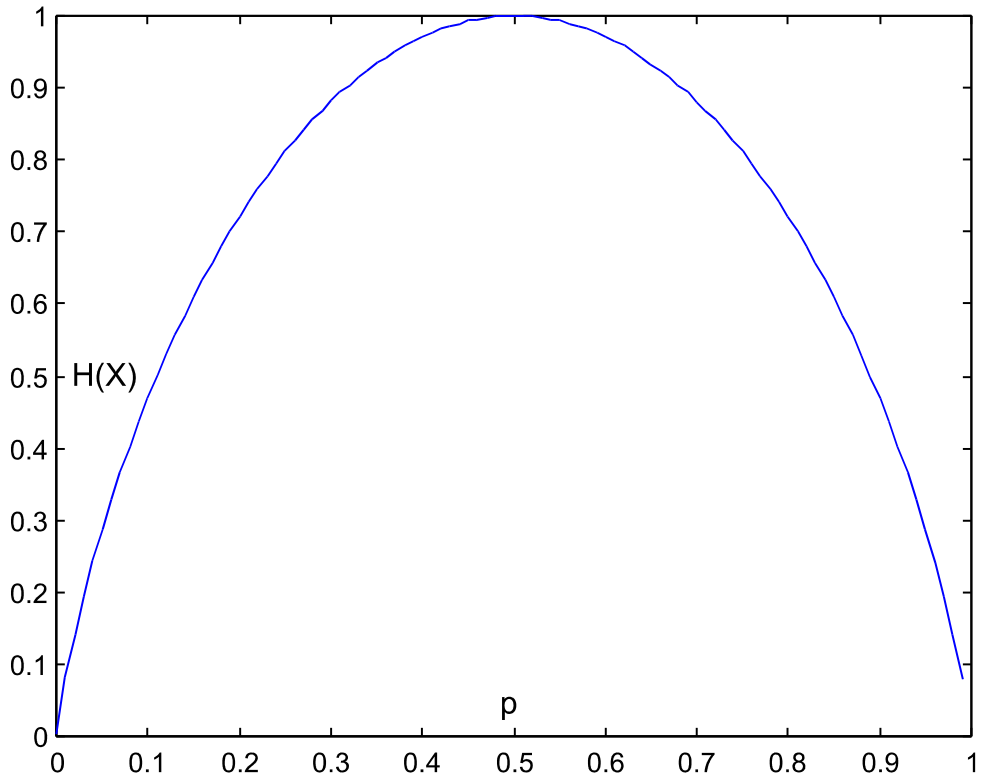
Quantité d'information moyenne associée à chaque symbole de la source = **entropie**

$$H(X) = E(h(X)) = \sum_{i=1}^{n} p_i . \log(1/p_i) = -\sum_{i=1}^{n} p_i . \log(p_i)$$

- Ex : Source binaire

$$p(1) = p$$
$$p(0) = 1 - p$$

$$H(X) = \begin{cases} -p.\log(p) - (1-p).\log(1-p) & \text{pour } 0 < p < 1 \\ 0 \quad \text{si} \quad p = 0 \text{ ou } 1 \end{cases}$$



- **Propriétés de l ’entropie**

  ✓**Continuité** : l'entropie est une fonction continue de chaque variable p_i.

  ✓**Additivité** : de part la définition de l'information propre.

  ✓**Positive** : $H(X) = H(p_1, p_2, ..., p_n) \geq 0$

  ✓**Bornée** : $$H(X) \leq H(\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n}) = \log(n)$$

- **Redondance**

$$R = H_{\max}(X) - H(X)$$

$$\rho = 1 - \frac{H(X)}{H_{\max}(X)}$$

- **Entropie & Débit d ’information**

  ✓Le débit d'information d'une source est donné par le produit de l'entropie de la source (valeur moyenne de l'info /symbole) par le nombre moyen de symboles par seconde soit :

$$D_X = \frac{H(X)}{\tau} \quad (bits.s^{-1}) \quad \text{avec } \tau \text{ durée moyenne d'un symbole}$$

- **Source Qaire**

  ✓**Source Q^{aire}** : source S dont l'alphabet possède Q éléments

  ✓**k^{ième} extension** : source S^{k} dont l'alphabet Q^{kaire} est obtenu en groupant par bloc de k celui de la source S

3. Canaux discrets & Capacité

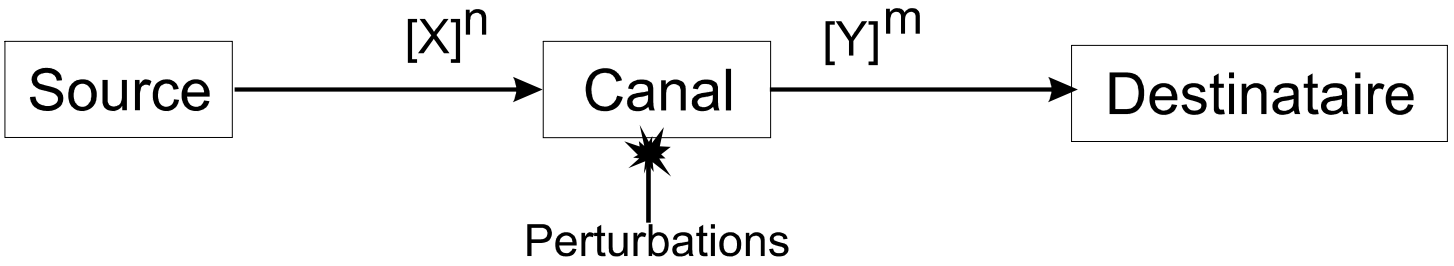
✓**Canal** : milieu de transmission de l'information situé entre la source et la destination. Le canal opère une transformation entre l'espace des symboles à l'entrée et celui de la sortie.

✓**Canal discret** : les espaces d'entrée et de sortie sont discrets

✓**Canal continu** : les espaces d'entrée et de sortie sont continus

✓**Canal sans mémoire** : si la transformation d'un symbole x à l'entrée en un symbole y en sortie ne dépend pas des transformations antérieures

✓**Canal stationnaire** : si les transformations ne dépendent pas de l'origine des temps



$$[X.Y]=\begin{bmatrix} x_1y_1 & x_1y_2 & \dots & x_1y_m \\ x_2y_1 & x_2y_2 & & x_2y_m \\ \dots & & & \dots \\ x_ny_1 & x_ny_2 & \dots & x_ny_m \end{bmatrix}$$

$$[P(X,Y)]=\begin{bmatrix} p(x_1,y_1) & p(x_1,y_2) & \dots & p(x_1,y_m) \\ p(x_2,y_1) & p(x_2,y_2) & & p(x_2,y_m) \\ \dots & & & \dots \\ p(x_n,y_1) & p(x_n,y_2) & \dots & p(x_n,y_m) \end{bmatrix}$$

- Probabilités marginales

$$p(x_i)=\sum_{j=1}^{m} p(x_i,y_j)$$

$$p(y_j)=\sum_{i=1}^{n} p(x_i,y_j)$$

$$H(X)=-\sum_{i=1}^{n} p(x_i).\log(p(x_i))$$

$$H(Y)=-\sum_{j=1}^{m} p(y_j).\log(p(y_j))$$

- Entropie réunie ou conjointe

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j).\log(\, p(x_i, y_j))$$

- Entropie conditionnelle ou équivoque

$$H(X/Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j).\log(\, p(x_i / y_j))$$

- Canaux non perturbés

$$H(X/Y) = H(Y/X) = 0$$

$$H(X,Y) = H(X) = H(Y)$$

- Canaux très (très) perturbés

$$H(X/Y) = H(X) \quad \text{et} \quad H(Y/X) = H(Y)$$

$$H(X,Y) = H(X) + H(Y)$$

Transinformation & capacité

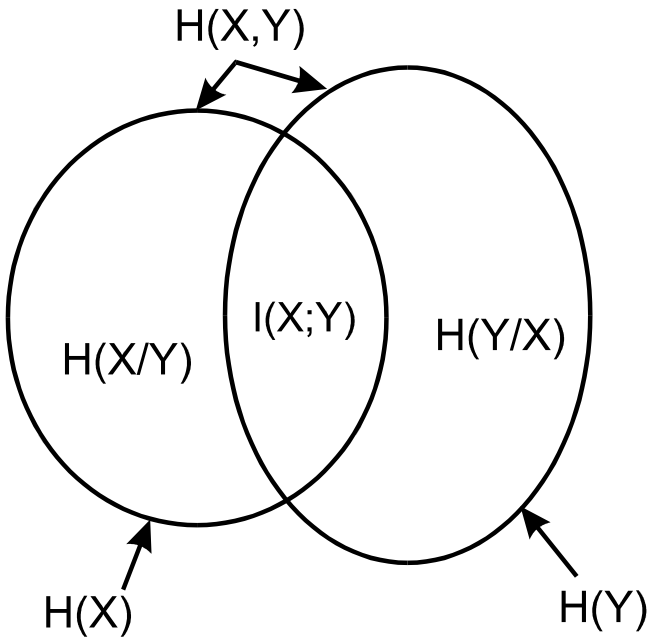
- Information mutuelle

$$i(x;y) = \log(\, p(x/y)/\, p(x)) \qquad \rightarrow i(x;y) = i(y;x)$$

- **Transinformation**

$$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j).\log(\frac{p(x_i, y_j)}{p(x_i).p(y_j)})$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$
$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X)$$



- **Capacité d'un canal**

$$C = \underset{p(x)}{Max}(I(X;Y))$$

- **Redondance d'un canal**

$$Rc = C - I(X;Y) \qquad \rho_c = 1 - \frac{I(X;Y)}{C}$$

- **Efficacité d'un canal**

$$\eta_c = \frac{I(X;Y)}{C}$$

Ex → canal binaire