Théorie de l'information et du Codage

Cours Master RSSI

Par : Faraoun Kamel Mohammed

Objectifs de ce Cours

Etude des mesures de l'Information selon les théories de Claude Shannon avec ses applications dans deux domaines :

1. **Compression de données**
2. **Détection /Correction d'erreurs de transmission**

Sommaire

- Introduction, historique et principe de la THI et des systèmes de communications
- Mesures de la quantité d'information et Entropie
- Codage de la source (discrète sans mémoire)
  - Codes et Codage (codage optimale, prefixe , Huffman, 1^{ier} Théorème de Shanon …)
  - Redondance et compression (Lampel Ziv, Shannon,…)
- Codage du canal (Discret symétrique)
  - Codage du canal
  - Capacité d'un canal (2^{ième} Théorème de Shanon)
  - Correction et codes correcteurs (Représentations, Hamming, Linéaire, Polynomiaux,…)

Ce dont on va parler dans ce cours . . .

- **Notions mathématiques :** entropie, information mutuelle
- **Codage et décodage :** codes, déchiffrabilité, efficacité d'un code …
- **Compression des données :** essentiellement, compression sans pertes (conservative)
- **Transmission de l'information :** comment transmettre correctement une information en présence d'erreurs de transmission ….
- Le langage mathématique utilisé est celui de la **théorie des probabilités :** variables aléatoires et processus discrets (élémentaires)

Chapitre 1: Introduction, historique et principes de la THI

Introduction

- La théorie de l'information définie des bases **formelles** et **quantitatives** à la notion d'**information**, de façon à ce que celle-ci devienne techniquement utilisable dans un certain nombre de disciplines qui traitent de l'information.
- Elle fournit essentiellement des **outils de modélisation** et **d'analyse** dans le domaine du traitement de l'information.

Introduction

- C'est une théorie **probabiliste** permettant de quantifier le contenu moyen en information d'un ensemble de messages, dont le **codage** informatique satisfait une **distribution statistique** précise.
- Elle fournit une **mesure quantitative de la notion d'information** apportée par un message (ou une observation).
- Dans un sens plus général, une théorie de l'information vise à **quantifier** et **qualifier** la notion de contenu en information présent dans un ensemble de donnée.

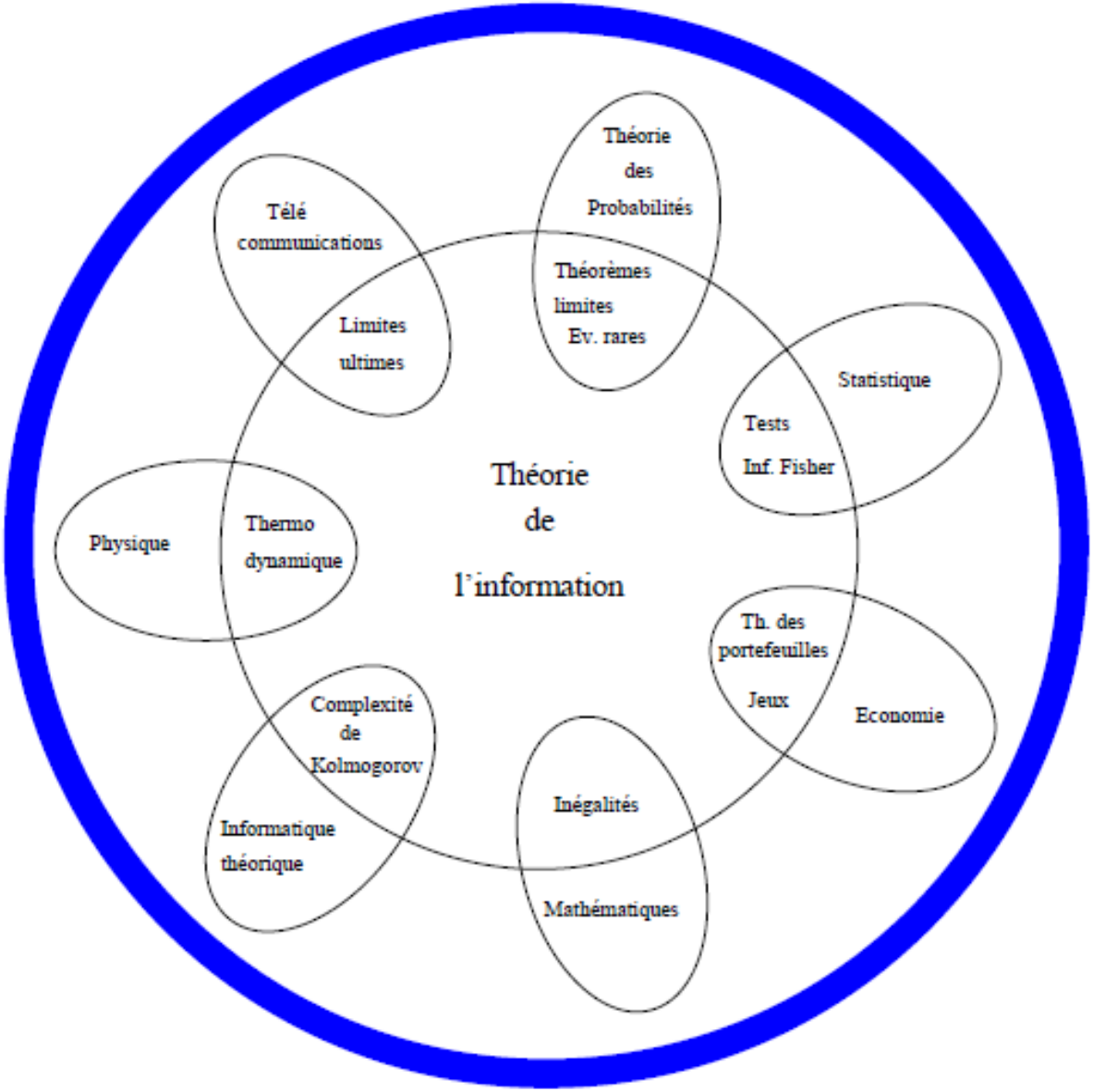
Objectifs et applications

- Codage efficace de l'information.
- Mesure quantitative de redondance d'un texte.
- Evaluation et minimisation des coûts de transmission et de stockage (Compression de données): Huffman, Lampel-Ziv, RLE....
- Contrôle des erreurs de transmission (Détection et Correction d'erreurs) : Codes à répétition, Hamming, Reed Solomon....
- Cryptologie : Cryptographie et Cryptanalyse …
- Sociologie …..

- Les principales questions auxquelles elle apporte une réponse sont les suivantes :

1. Quelle est la limite ultime en matière de compression des données digitales réversible (Codage d'une source de transmission);
2. Quel est le débit maximal de transmission fiable de ce type d'information sur un canal bruité (la capacité C d'un canal de transmission); et comment préserver la qualité de transmission sur de tels canaux;
3. Sous quelles conditions un code de chiffrement est-il sûre (Cryptologie)

Relations …

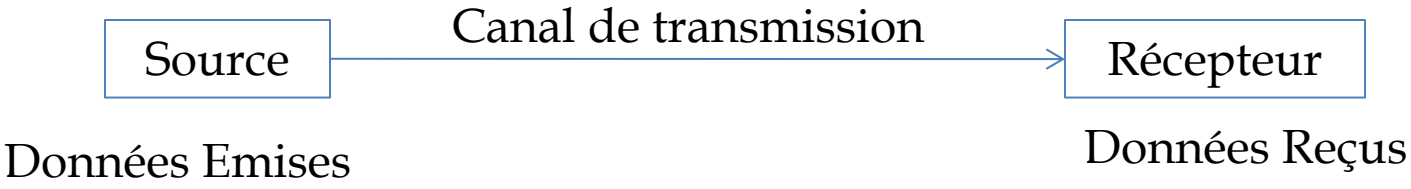

Théorie
de
l'information
Théorie
des
Probabilités
Théorèmes
limites
Ev. rares
Télé
communications
Limites
ultimes
Statistique
Tests
Inf. Fisher
Physique
Thermo
dynamique
Th. des
portefeuilles
Jeux
Economie
Complexité
de
Kolmogorov
Informatique
théorique
Inégalités
Mathématiques

Historique

- Cette théorie fut conçue par **Claude E. Shannon** peu après la seconde guerre mondiale pour répondre à certaines interrogations fondamentales dans le domaine des **techniques de communication**.
- Comme le suggère l'intitulé de l'article fondateur de Shannon (*The mathematical theory of communication*, 1948), cette théorie peut être vue comme une discipline **mathématique**.
- Claude Shannon est ingénieur de la société Bell qui s'intéresser à la qualité des communication téléphoniques.

Notion d'information

- Considérons le problème de la communication entre une source et un récepteur : la source émet un message que le récepteur lit.



- On voudrait quantifier l'« **information** » que contient chaque message émis. Par exemple, il est clair que si l'émetteur dit toujours la même chose, la quantité d'information apportée par une répétition supplémentaire est nulle.

Notion d'information

Le cas le plus simple est le suivant : le récepteur attend une information de type *oui/non*, le oui et le non étant a priori aussi vraisemblables l'un que l'autre.

Lorsque la source transmet soit un *oui* soit un *non*, on considère que le récepteur reçoit une unité d'information (**un *bit***).

Autrement dit : une unité d'information, c'est quand on a a priori un ensemble de deux possibilités équiprobables, et que l'une d'elles se réalise.

Donc une information désigne, parmi un ensemble d'événements, un ou plusieurs événements possibles.

Notion d'information : Incertitude

- En théorie, l'information **diminue l'incertitude**. Plus un récepteur reçoit de l'information, plus son incertitude envers le message à transmettre diminue.
- Avant le début de la transmission, le récepteur n'a aucune information sur le message : l'incertitude est maximale. A la fin de la transmission, son incertitude devient nulle.
- Pendant la transmission, l'incertitude est dans un état intermédiaire équivalent (quantitativement) à la quantité d'information non encore reçue.

Quantité d'information: Exemple d'illustration

Considérons **N boîtes homogènes numérotées de 1 à N**.

- Un individu « **A** » a caché au hasard un objet dans une de ces boîtes.
- Un individu « **B** » doit trouver le numéro de la boîte où est caché l'objet.
- Pour cela, « **B** » a le droit de poser des questions à l'individu « **A** »
- « **A** » doit répondre sans mentir par **OUI** ou **NON.**
- Chaque question posée représente un coût à payer par l'individu « **B** » (par exemple un euro).

Quantité d'information: Exemple d'illustration

- Un autre individu « **C** » sait dans quelle boîte est caché l'objet. Il a la possibilité de vendre cette information à l'individu « **B** ».
- « **B** » n'acceptera ce marché que si le prix de « **C** » est inférieur ou égal au coût moyen que « **B** » devrait dépenser pour trouver la boîte en posant des questions à « **A** ».
- L'information détenue par « **C** » a donc un certain prix qui représente: « la quantité d'information représentée par la connaissance de la bonne boîte: le nombre moyen de questions à poser pour identifier cette boîte ». Nous la noterons « I ».

Quantité d'information: Exemple d'illustration

Cas de figure :

- Si N = 1 alors I = 0 : Il n'y a qu'une seule boîte. Aucune question n'est nécessaire.
- Si N = 2 alors I = 1: On demande si la bonne boîte est la boîte n°1. La réponse OUI ou NON détermine alors sans ambiguïté quelle est la boîte cherchée.
- Si N = 4 alors I = 2: On demande si la boîte porte le n°1 ou 2. La réponse permet alors d'éliminer deux des boîtes et il suffit d'une dernière question pour trouver quelle est la bonne boîte parmi les deux restantes.

Quantité d'information: Exemple d'illustration

- Si $N = 2^k$ alors $I = k$: On écrit les numéros des boîtes en base 2 (sont au plus sur k chiffres binaires). Pour chacun des rangs de ces chiffres, on demande si la boîte cherchée possède la valeur 0 ou 1.
- En k questions, on peut déterminé tous les chiffres binaires de la bonne boîte. Cela revient également à poser k questions, chaque question ayant pour but de diviser successivement le nombre de boîtes considérées par 2 (méthode de dichotomie).
- On est donc amené à poser $\mathbf{I = \log_2(N)}$, mais cette configuration ne se produit que dans le cas de N événements équiprobables.

Quantité d'information: Exemple d'illustration

- Supposons maintenant que les boîtes soient colorées, et qu'il y ait **n** boîtes rouges.
- Supposons également que « C » sache que la boîte où est caché l'objet est rouge. Quel est le prix de cette information?
- Sans cette information, le prix à payer est $\log_2(N)$. Muni de cette information, le prix à payer n'est plus que $\log_2(n)$. Le prix de l'information «la boîte cherchée est rouge » est donc :

$$\log_2(N) - \log_2(n) = \log_2(N / n).$$

Quantité d'information: Exemple d'illustration

- On définit ainsi la quantité d'information comme une fonction croissante de N/n avec :
- N : le nombre d'évènements possibles
- n : le cardinal du sous-ensemble délimité par l'information
- Afin de mesurer cette quantité d'information, on pose :

$$I=\log_2(N/n)$$

- I est exprimé en bit (ou logon, unité introduite par Shannon), ou bien en « Nat » si on utilise le logarithme naturel à la place du logarithme de base 2.

Notion de quantité d'information

Supposons maintenant que les boîtes soient de diverses couleurs :

n_1 boîtes de couleur C_1,
n_2 boîtes de couleur C_2,
...
...
n_k boîtes de couleurs C_k,

avec $\boldsymbol{n_1 + n_2 + \ldots + n_k = N}$.

Notion de quantité d'information

La personne « **C** » sait de quelle couleur est la boîte recherchée.

Quel est le prix de cette information ?

L'information « la boîte est de couleur C_1 » vaut $\log_2 (N/n_1)$, et cette éventualité a une probabilité n_1/N.

L'information « la boîte est de couleur C_2 » vaut $\log_2(N/n_2)$, et cette éventualité a une probabilité n_2/N.

……

……

L'information « la boîte est de couleur C_k » vaut $\log_2 (N/n_k)$, et cette éventualité a une probabilité n_k/N.

Notion de quantité d'information

Le prix moyen de l'information est donc:

$$(n_1/\mathrm{N})\log_2(\mathrm{N}/n_1)+ (n_2/\mathrm{N})\log_2(\mathrm{N}/n_2)+\ldots + (n_k/\mathrm{N})\log_2(\mathrm{N}/n_k)$$

Plus généralement, si on considère k évènements disjoints de probabilités respectives p_1, p_2, ..., p_k avec : $p_1 + p_2 + \ldots + p_k = 1$, alors la quantité d'information correspondant à cette distribution de probabilité est:

$$p_1 \log 1/p_1 + \ldots + p_k \log 1/p_k$$

Cette quantité s'appelle « Entropie de la distribution de probabilité »

Entropie d'information (Shanon)

L'entropie permet de mesurer la quantité d'information moyenne d'un ensemble d'évènements (en particulier de messages) et de mesurer son incertitude. On la note *H* :

$$H = \sum_{i \in I} p_i . Log_2\left(\frac{1}{p_i}\right) = -\sum_{i \in I} p_i . Log_2(p_i)$$

avec $p_i = \frac{n_i}{N}$ la probabilité associée à l'évènement *i*.

L'entropie de Shannon, est une fonction mathématique qui correspond à la quantité d'information moyenne contenue ou délivrée par une source d'information.

Entropie d'information (Shanon)

La définition de l'entropie d'une source selon Shannon est telle que plus la source est redondante, moins elle contient d'information.

En l'absence de contraintes particulières, l'entropie H est maximale pour une source dont tous les symboles sont équiprobables.

Dans le cas particulier d'un système de communication, l'entropie de la source d'information (le transmetteur) indique l'incertitude du récepteur par rapport à ce que la source va transmettre.

Entropie d'information :Exemple

Une source qui envoi toujours le même symbole, disons la lettre « a », a une entropie nulle, c'est-à-dire minimale (H=0).

En effet, un récepteur qui connait seulement les statistiques de transmission de la source est assuré que le prochain symbole sera un « a », sans jamais se tromper.

Le récepteur n'a pas besoin de recevoir de signal pour lever l'incertitude sur ce qui a été transmis par la source car celle-ci n'engendre pas d'hasard.

Entropie d'information :Exemple

Par contre, si la source envoi un « a » la moitié du temps et un « b » l'autre moitié, le récepteur est incertain de la prochaine lettre à recevoir.

L'entropie de la source dans ce cas est donc non nulle (positive) et représente quantitativement l'incertitude qui règne sur l'information émanant de la source.

« Du point de vue du récepteur, l'entropie indique la quantité d'information qu'il lui faut obtenir pour lever complètement l'incertitude (ou le doute) sur ce que la source a transmis »

Notion d'incertitude

- Pour Shannon, l'information présente un caractère essentiellement aléatoire. Un événement aléatoire est par définition incertain. Cette incertitude est prise comme mesure de l'information.
- Une information sera donc uniquement définie par sa probabilité ($I = - \log_2(p)$). Donc l'information est aussi la mesure de l'incertitude calculée à partir de la probabilité de l'événement.
- Shannon a donc confondu la notion d'information et de mesure d'incertitude :

« Plus une information est incertaine, plus elle est intéressante, et un événement certain ne contient aucune information »

Notion d'incertitude : Exemple(1)

- Considérons une urne contenant plusieurs boules de différentes couleurs, dont on tire une boule au hasard.
- Si toutes les boules ont des couleurs différentes, alors notre incertitude sur le résultat d'un tirage est maximale. En particulier, si nous devions parier sur le résultat d'un tirage, nous ne pourrions pas privilégier un choix plutôt qu'un autre.
- Par contre, si une certaine couleur est plus représentée que les autres (par exemple si l'urne contient d'avantage de boules rouges), alors notre incertitude est légèrement réduite : la boule tirée a plus de chances d'être rouge:

« Révéler le résultat du tirage fournit en moyenne d'avantage d'information dans le premier cas que dans le second »

Notion d'incertitude : Exemple(2)

- Prenons un autre exemple : considérons un texte en français codé comme une chaîne de lettres, d'espaces et de ponctuations (notre source est donc une chaîne de caractères).
- Comme la fréquence de certains caractères n'est pas très importante (ex : 'w'), tandis que d'autres sont très communs (ex : 'e'), la chaîne de caractères n'est pas si aléatoire que ça.
- D'un autre côté, tant qu'on ne peut pas prédire quel est le caractère suivant, d'une certaine manière, cette chaîne est aléatoire, c'est ce que cherche à quantifier la notion d'entropie de Shannon.

Incertitude ↔ Quantité d'information

- L'incertitude est équivalente à la Quantité d'information (Quantitativement)
- Soit X une source d'information alors $I(X) = -\log_2(p_{xi})$ représente:

  - La quantité d'information fournit par X si X est connue (A posteriori)
  - L'incertitude sur X si X est inconnue (A priori)

Entropie ↔ Quantité d'information

- L'entropie et la valeur moyenne de la quantité d'information observé sur la sortie d'une source de données.
- Formellement c'est l'espérance mathématique de la quantité d'information :

$$H(X)=E(I(X))$$

Pour une source de données X (Var. Aléatoire)

Systèmes de communication

- La théorie de l'information s'intéresse particulièrement aux moyens de transmettre une information depuis la source jusqu'à un récepteur à travers un canal.
- La nature de la source peut être très variée : il peut s'agir par exemple d'une voix, d'un signal électromagnétique ou d'une séquence de symboles binaires (fichier).
- Le canal peut être une ligne téléphonique, une liaison radio, un support magnétique ou optique.

Systèmes de communication

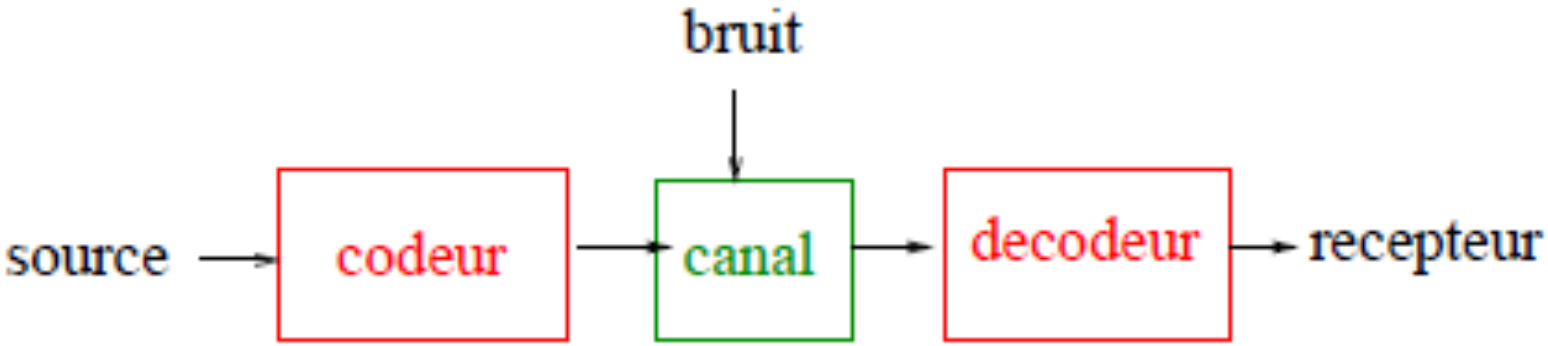


Schéma générale d'un système de communication

Source : voix, musique, image (fixe ou animée), texte,. . .
Canal : radio, fil, fibre optique, support magnétique ou optique, . . .
Bruit : perturbations électromagnétiques, rayures, . . .

Systèmes de communication

- Le codeur représente l'ensemble des opérations effectuées sur la sortie de la source avant la transmission.
- Ces opérations peuvent être par exemple la modulation, la compression, le brouillage, l'ajout de redondance pour combattre les effets du bruit, ou encore l'adaptation à des contraintes de spectre, dans le but de rendre la sortie de la source compatible avec le canal.
- Le décodeur doit être capable, à partir de la sortie du canal, de restituer de façon acceptable l'information fournie par la source.

Systèmes de communication

- Dans ce cours, nous étudieront certains de ces modèles qui, bien que considérablement plus simples que les sources et les canaux physiques, permettent de donner une bonne approximation de leur comportement.
- Pour simplifier, on étudiera séparément les modèles de sources et les modèles de canaux ainsi que leurs codages respectifs.

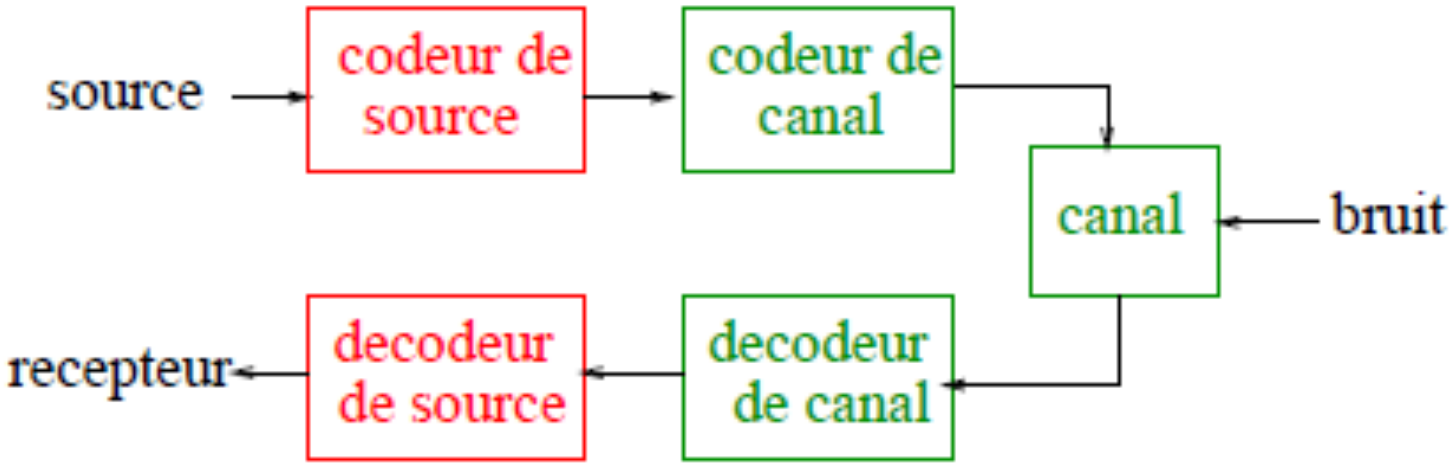


Schéma décomposé d'un système de communication (modèle de C.Shanon)

Cette séparation entre codage de source et codage de canal n'implique en pratique aucune limitation sur les performances du système complet.

Objectifs d'un codeur

- Le but du codeur de source est de représenter la sortie de la source en une séquence binaire, et cela de la façon la plus économique possible.

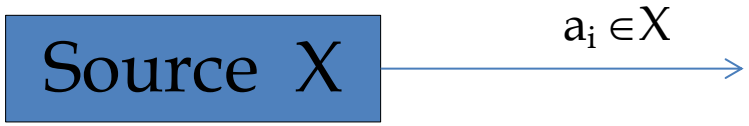
- **Efficacité :** Pour faire parvenir une quantité donnée d'information a l'utilisateur, utiliser le minimum de ressources.(codeur de source)

Objectifs d'un codeur

- Le but du codeur de canal et de son décodeur est de reproduire le plus fidèlement possible cette séquence binaire malgré le passage à travers le canal bruité.

- **Fiabilité :** Restituer a l'utilisateur une information suffisamment fidèle a celle produite par la source.(codeur de canal)

Source et codeur de source



Source de données $X = \{a_1, a_2, \ldots, a_n\}$, $|X| = n$

$X' = \{b_1, b_2, \ldots, b_m\}$ et le code adapté a la transmission par le canal

Exemple: $X = \{a_1, a_2, a_3, a_4\}$, $X' = \{0,1\}$

$a_1 \rightarrow$ 00
$a_2 \rightarrow$ 01
$a_3 \rightarrow$ 10
$a_4 \rightarrow$ 11

- Une source produit des séquences de symboles dans l'alphabet X (séquentiellement)
- Un symbole a_i est produit à un instant donné t_i avec une probabilité $p(a_i)$:
  - $X = \{a_1, a_2, ...a_k, ...a_n\}$ $\quad |X| = n$
  - "k on définit $p(a_k)$ telle que :
    - $0 \leq p(a_k) \leq 1$
    - $\sum p(a_k) = 1$
- **Définition :** Une source est un systèmes capables de sélectionner et d'émettre des séquences de signes (ou messages) appartenant à un ensemble (ou alphabet) donné X.
  - Ex. de signes : lettres, chiffres, échantillons
  - Ex. de sources : texte, fichier, message (Data)….

Source et codeur de source

- Formellement, une source est une *variable aléatoire de loi de probabilité P_X connue*.
- On peut distinguer, parmi les classes de modèles de sources:
  - Les sources discrètes avec/sans mémoire, finie ou infinie:
    - Sources sans mémoire: signes générés indépendamment les uns des autres => modèle de Bernoulli
    - Sources avec mémoire : prise en compte de la dépendance entre un signe émis et les signes précédents=> modèle de Markov
  - Les sources non discrètes, ou sources continues

Code et codage

- Soit une source discrète X munie d'un alphabet fini (a_1,…, a_K) est d'une loi de probabilité P_X.
- Définition (Code): Un code de X est une application φ: X → {0, 1}* (l'ensemble des mots binaires de longueur arbitraire). Un mot de code est un élément de φ(X).
- Définition (Codage) :Un codage de X est une application φ:X^* → {0,1}* qui a toute séquence finie de lettres de X associe une séquence binaire. A tout code φ de X on peut associer le codage: (x_1, x_2,…,x_L) → (φ(x_1) ǁ φ (x_2) ǁ ….ǁ φ (x_L)) (la réciproque n'est pas vraie).
- Définition (Régularité) : Un code (resp. codage) est régulier si deux lettres (resp. séquences de lettres) distinctes sont codées par des mots distincts. Un code non régulier implique une perte d'information.

- La probabilité P_x d'une source X influe sur sont comportement et sur le codage possible de cette source.

Exemple : $X=\{a_1,a_2,a_3,a_4\}$, $X'=\{0,1\}$

1ière loi : $P(a_1)=P(a_2)=P(a_3)=P(a_4)=1/4$ (Uniforme)

2ième loi : $P(a_1)=1/2$, $P(a_2)=1/4$, $P(a_3)=P(a_4)=1/8$

On propose deux codes :

$$\text{Code A} : \begin{cases} a_1 \rightarrow 00 \\ a_2 \rightarrow 01 \\ a_3 \rightarrow 10 \\ a_4 \rightarrow 11 \end{cases} \qquad \text{Code B} : \begin{cases} a_1 \rightarrow 0 \\ a_2 \rightarrow 10 \\ a_3 \rightarrow 110 \\ a_4 \rightarrow 111 \end{cases}$$

Quel est le meilleur code dans les deux cas?

- Loi 1:
  - Code A: Longueur moyenne = 2
  - Code B: Longueur moyenne (1/4+2/4+3/4+3/4)=2.25

  Donc le code A est mieux que B (en terme de longueur)
- Loi 2:
  - Code A: Longueur moyenne = 2
  - Code B: Longueur moyenne (1/2+2/4+3/8+3/8)=1.75

  Donc le code B est mieux que A (en terme de longueur)

« Le meilleur code dépend de la distribution (la loi de probabilité) de la source »

Entropie d'une Source

- Nous voulons établir un lien entre l'information fournie par une source et la distribution de probabilité de la sortie de cette source.
- L'apparition d'un événement peu probable apporte de l'information tandis que l'occurrence d'un événement certain ne fournit au contraire aucune information.
- Si une lettre « a » a une probabilité p(a) d'être tirée, son information propre est définie par:

$$I(a)=-\log_2(p(a))$$

- En particulier I(a) vaut zéro si p(a) = 1.
- L'information propre est inversement proportionnelle à la valeur de la probabilité.

Entropie d'une Source

- La valeur moyenne de l'information propre calculée sur l'ensemble de l'alphabet revêt une grande importance.
- Il s'agit donc de l'espérance mathématique de la variable aléatoire I. Elle est appelée entropie de la source et est notée H(A) =E(I(a)) :

$$H(A) = -\sum_{a \in A} p(a) \log_2 p(a).$$

Entropie d'une Source: Exemples

1. Source binaire équiprobable X = { 0,1 },
   P(0) = P(1) =0.5 $\Rightarrow$ H(X) = 1 bit par symbole
2. Source binaire biaisée : X = { 0,1 }, p(0) = 1-p(1)
   P(0)= 0.2 , P(1)=0.8 $\Rightarrow$ H(X) = 0.72 bit par symbole
3. Alphabet de 26 lettres : X={A,B,C,…Z}, $\forall x$ P(x)=1/26
   $\Rightarrow$ H(X) = 4.7 bits par symbole
4. Langue anglaise dépend du modèle H(X) = 4.7 ? 1.3 bits par symbole
5. Si une source émet n lettres équiprobables (loi de probabilité uniforme), son entropie est donc $H(X)=\log_2(n)$.
   Si $n = 2^r$, son entropie est alors r.

« On se limitera dans ce cours a **l'étude des sources discrètes sans mémoire** qui sont les plus utilisées dans les modèles des systèmes de communications, l'extension vers les autres types nécessite le passage vers les modèles de **Markov** et les **processus stochastiques** ».

Canaux et codeur de canal

- Pour modéliser un canal de transmission, il est nécessaire de spécifier l'ensemble des entrées et l'ensemble des sorties possibles.
- La cas le plus simple est celui du canal discret sans mémoire:

  L'entrée est une lettre prise dans un alphabet fini $A = \{a_1, \ldots, a_n\}$ et la sortie est une lettre prise dans un alphabet fini $B = \{b_1, \ldots, b_m\}$.

Canaux et codeur de canal

- Les symboles sont émises en séquence. Le canal est dit sans mémoire si chaque lettre de la séquence reçue ne dépend statistiquement que de la lettre émise de même position.
- Ainsi un canal discret sans mémoire est entièrement décrit par la donnée des probabilités conditionnelles P(b|a) pour toutes les lettres « a » de l'alphabet d'entrée et toutes les lettres « b » de l'alphabet de sortie.
- Nous allons revenir dans le chapitre suivant sur cette notion de probabilité conditionnelle.

Canaux et codeur de canal

- Définition :

  Un canal discret est défini par la donnée de:

  – Un alphabet d'entrée $X = \{a_1, \ldots, a_n\}$

  – Un alphabet de sortie $Y = \{b_1, \ldots, b_m\}$

  – une loi de transition $P(Y|X)$, i.e. une matrice stochastique:

$$M = \begin{array}{c} \begin{matrix} b_1, & \cdots\cdots\cdots\cdots & b_m \end{matrix} \\ \begin{pmatrix} P(b_1|a_1) & \cdots\cdots & P(b_m|a_1) \\ \vdots & \ddots & \vdots \\ P(b_1|a_n) & \cdots\cdots & P(b_m|a_n) \end{pmatrix} \end{array} \begin{matrix} a_1 \\ \vdots \\ a_n \end{matrix}$$

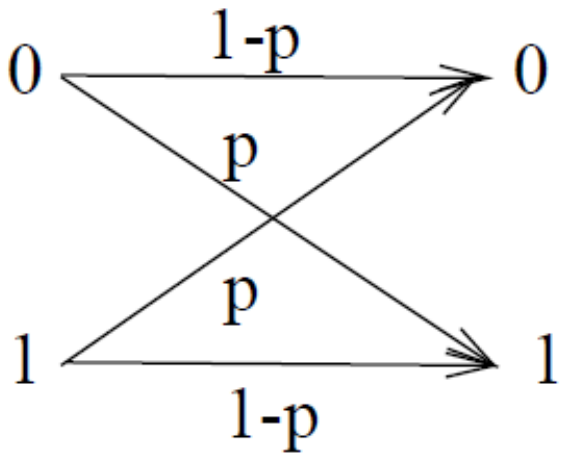
Canaux et codeur de canal

- Un canal est dit symétrique si sa matrice de transitions est symétrique par rapport à sa diagonale :

$$P(a_i \mid b_j)=P(a_j \mid b_i)\ \forall i,j.$$

- Dans la suit de ce cours, on étudiera plus particulièrement les canaux discrets causales sans mémoire symétriques définie par leurs matrice de transitions symétriques, ayant un alphabet d'entrée $X = \{a_1,\ldots. , a_n\}$ et un alphabet de sortie $Y=\{b_1,\ldots,b_m\}$.

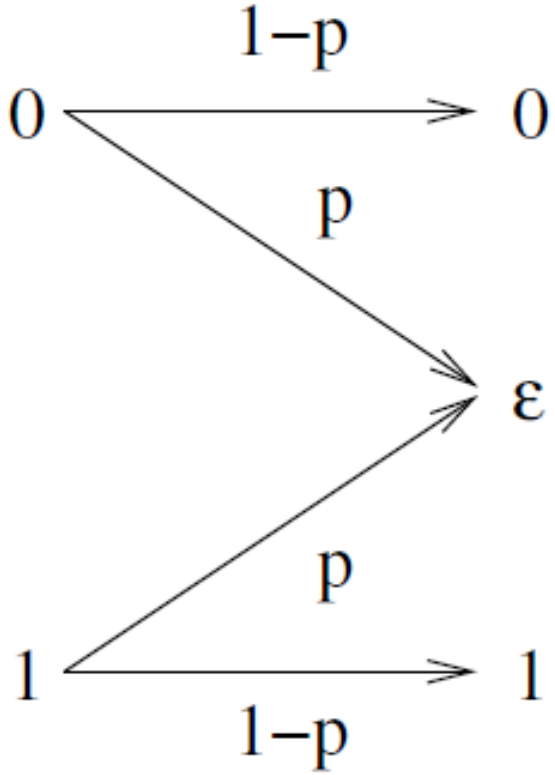
Canal discret sans mémoire: « le canal binaire symétrique »



$$M = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

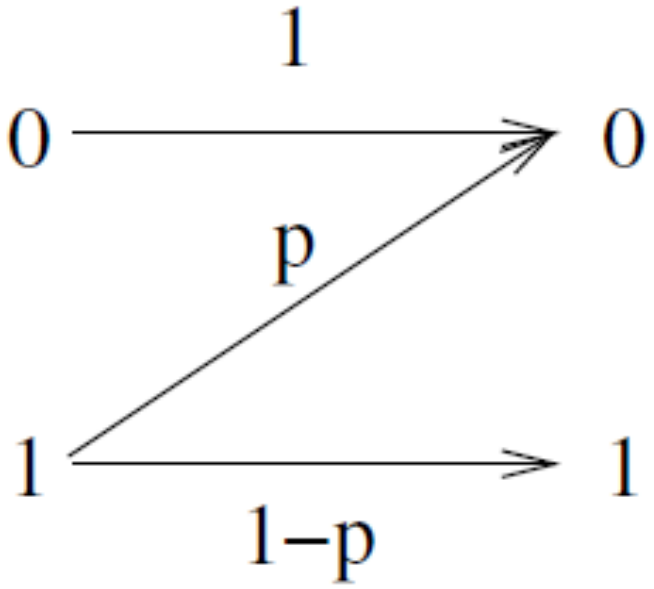
- Le plus connu est le canal binaire symétrique défini par $X = Y = \{0, 1\}$ et dont les probabilités de transition sont représentées dans la Figure. Il est entièrement décrit par sa matrice de transitions M.
- La probabilité pour qu'un symbole soit inchangé est $1-p$ $(0 \leq p \leq 1)$ donc la probabilité pour qu'il soit changé est p.

Canal discret sans mémoire: « le canal à effacement»



$$M = \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}$$

Canal discret sans mémoire: « le canal en Z»



$$M = \begin{pmatrix} 1 & 0 \\ p & 1-p \end{pmatrix}$$

Conclusion

- Un système de communication est basé principalement sur le modèle de la source et du canal de transmission.
- La source est une variable aléatoire définie sur un alphabet et munie d'une loi de probabilité, le but en utilisant la THI pour celle-ci est de :

Assurée un meilleur codage de la source en terme de représentation d'une longueur minimale (codage de la source, compression), on s'intéresse d'avantage aux source discrètes sans mémoire.

Conclusion

- Un canal est modéliser par une association Entrées/Sorties définies sur deux alphabets X et Y , et munie d'un loi de probabilité conditionnelle spécifiée par une matrice stochastique de transitions. Nous cherchons à assuré:

Une transmission avec le minimum d'erreurs possibles sur un canal bruité, tout en mesurant la capacité maximale de transmission de ce canal qui le permet. (codes correcteurs et capacité de canal)