Introduction à la Théorie de l'Information

2019-2020

Plan

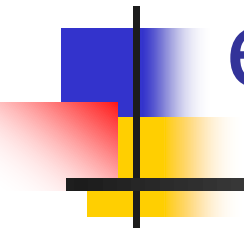
- Quantité d'information et entropie d'une source
- Le codage de source
  - Théorème du codage de source
  - Codage de Shannon-Fano
  - Codage binaire de Huffman
  - Codage Arithmétique
  - Codage LZ78
- Introduction au codage de canal
  - Codes linéaires
  - Codes cycliques
  - Codes convolutifs
- Conclusion

« Théorie de l'information » ???

- Dans le langage courant, « information » est utilisé dans divers contextes
  - pour le journaliste : les actualités
  - pour le policier : des renseignements
- Dans le domaine des télécommunications, la « théorie de l'information » se préoccupe des systèmes de communication et de leur efficacité.

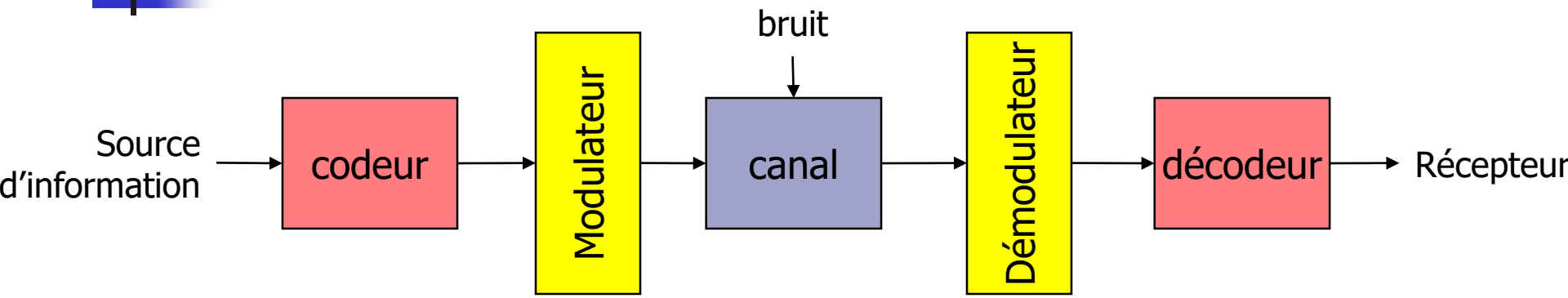
- La théorie de l'information est récente (1948, publication de l'article *Mathematical Theory of Communications* de Claude Shannon). Shannon montre que l'information contenue dans un message est une grandeur physique mesurable.

- Les domaines de la théorie de l'information
  - le codage,
  - la compression de données,
  - la cryptographie.



Quantité d’information et entropie d’une source

Système de communication



- Source : entité qui génère le message. Exemples :
  - Une personne qui parle : message = mots prononcés
  - Un ordinateur : message = bits égaux à 0 ou 1
- Canal : le support de la communication. Ex. : Une ligne téléphonique, une transmission satellite, …
- Codeur : il met en forme le message de la source pour l'adapter au canal. Ex. : Compression, cryptographie, code correcteur d'erreur…
- Décodeur : il restitue l'information émise par la source à partir de la sortie du canal
- Modulateur : il met en forme le signal analogique émis sur le canal.

Système de communication

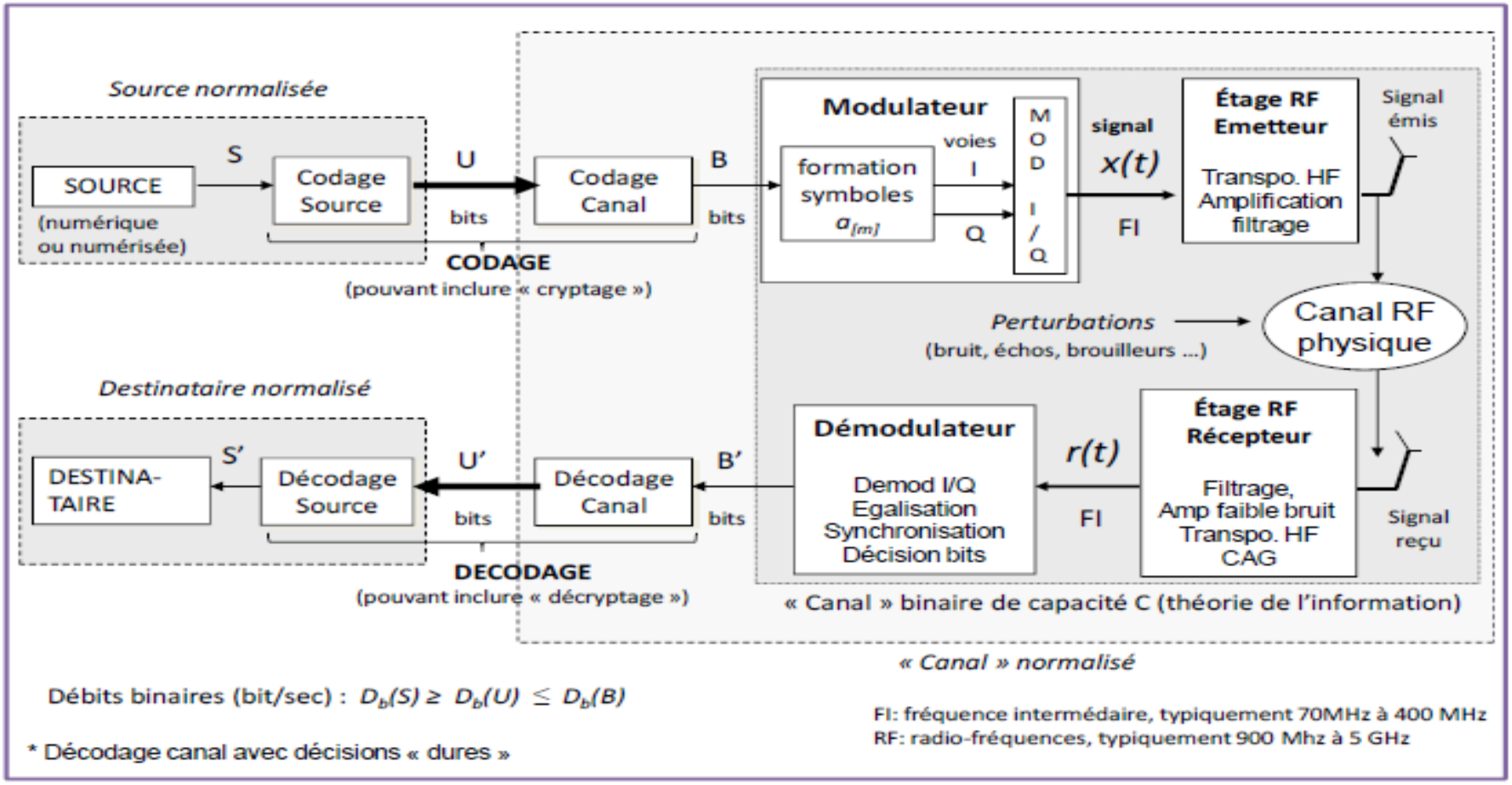


Schéma global typique d'une transmission numérique sur fréquence porteuse

Contenu informatif d'un message

- Avant de coder le message (le transformer en une suite de 0 et de 1), il est nécessaire de déterminer le contenu informatif du message.

- Exemple
  - La source transmet toujours le même message, la lettre A. Son contenu informatif est nul, car le récepteur n'apprend rien en recevant le message.
  - La source émet soit oui, soit non. Elle fournit une information et une seule au récepteur.
  - La source émet le temps qu'il fera demain : le contenu informatif est très riche, dans la mesure où le message de la source peut prendre des valeurs très diverses.

- Finalement, un message est « riche » en information s'il apporte une réponse à une situation de grande incertitude, c'est-à-dire s'il peut prendre beaucoup de valeurs différentes.

Contenu informatif d'un message et codage

- Il est important de connaître le contenu informatif d'un message avant de le coder, i.e. choisir les mots binaires qui vont représenter le message.
- Or en télécommunication, on veut toujours économiser le nombre de bits transmis pour
  - Gagner du temps (ex. : téléchargement d'une page web sur Internet : il faut qu'elle s'affiche rapidement)
  - Faire passer le plus de messages possibles sur un même support (par exemple, au cœur des réseaux téléphoniques, on transmet les conversations de plusieurs utilisateurs sur la même fibre optique).

  ⇨ Influence directe sur le coût des transmissions…!
- Ainsi, on souhaiterait coder l'information pertinente du message et elle seule !
- Mais comment mesurer le contenu informatif d'un message ? La Théorie de l'Information fournit une unité de mesure de la quantité d'information.

Entropie 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)

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

Entropie propre:

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

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

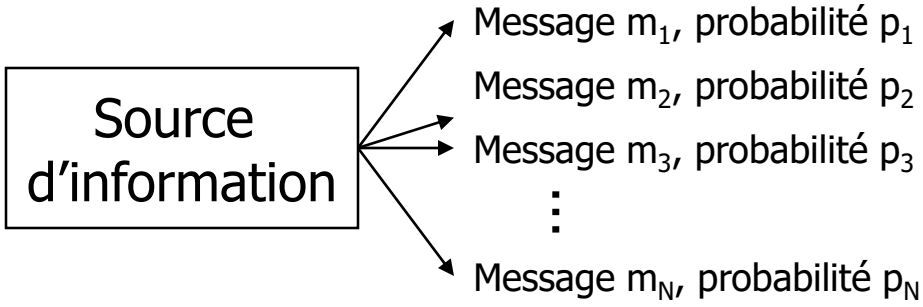
Règle de Bayes : $p(x,y) = p(x/y).p(y) = p(y/x).p(x) = p(y,x)$

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

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

Entropie d'une source

- Considérons une source pouvant émettre N messages différents. Notons p_i la probabilité d'émission du message m_i.



- Par définition, on appelle entropie H(S) de la source S la grandeur, exprimée en Shannon,

$$H(S) = \sum_{i=1}^{N} - p_i \cdot \log_2(p_i) = \sum_{i=1}^{N} p_i \cdot \log_2\left(\frac{1}{p_i}\right)$$

- L'entropie fournit une mesure de la quantité d'information associée à la source.

Exemples

- On considère une source émettant des symboles successifs égaux à 0 ou 1. La probabilité du 1 est 0,3. Celle du 0 vaut 0,7. Calculez son entropie.

$$H(S) = -0,7 \times \log_2(0,7) - 0,3 \times \log_2(0,3) = 0,88\text{sh}$$

- La source considérée transmet le résultat d'un lancé de dé truqué : P(1)=P(6) = 0,2 ; P(2)=P(3)=P(4)=P(5) = 0,15. Calculez son entropie.

$$H(S) = 2 \times \left[-0,2 \times \log_2(0,2)\right] + 4 \times \left[-0,15 \times \log_2(0,15)\right]$$
$$= 2,571\text{sh}$$

- Calculez l'entropie de la source si le dé n'est pas truqué.

$$P(1) = P(2) = P(3) = P(4) = P(5) = P(6) = \frac{1}{6}$$

$$H(S) = 6 \times \left[-\frac{1}{6} \times \log_2\left(\frac{1}{6}\right)\right] = 2,585\text{sh}$$

Remarque : L'entropie est plus grande quand les messages sont équiprobables.

Cas de messages équiprobables

- Calculons l'entropie d'une source pouvant émettre N messages équiprobables.
- La probabilité de chacun des messages est 1/N.

$$H(S) = \underbrace{\left[-\frac{1}{N}\cdot\log_2\left(\frac{1}{N}\right)\right] + \left[-\frac{1}{N}\cdot\log_2\left(\frac{1}{N}\right)\right] + \cdots + \left[-\frac{1}{N}\cdot\log_2\left(\frac{1}{N}\right)\right]}_{N\,\text{fois}}$$

$$= -N \times \frac{1}{N}\cdot\log_2\left(\frac{1}{N}\right) = -\log_2\left(\frac{1}{N}\right) = \log_2(N)$$

- On retiendra cette formule :

$$H(S) = \log_2(N)$$ pour N messages équiprobables

Exemples

- Exemple 1

  On considère une source transmettant toujours le même message, la lettre A.

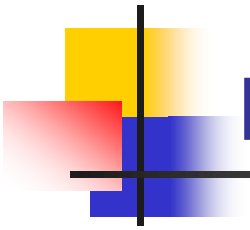
  - Analyse intuitive

    Qu'apprend le récepteur par cette source ? Rien, puisque le message est toujours le même ! Cette source ne produit aucune information utile.

  - Analyse par la théorie de l'information

    Le résultat de l'expérience est toujours le même (lettre A). Le message peut prendre une seule valeur possible : N=1

    Par définition la quantité d'information (l'entropie) associée à cette expérience est $\log_2(1) = 0$sh



Exemples

- Exemple 2

  On considère une source pouvant transmettre deux valeurs : oui/non. Les résultats sont équiprobables.

  - Analyse intuitive

    Qu'apprend le récepteur par cette source ? Quand la source émet un message, le récepteur reçoit une seule information : soit le résultat est oui, soit il vaut non.

  - Analyse par la théorie de l'information

    Deux résultats existent : « oui » et « non ». Ces résultats sont équiprobables.

    Par définition la quantité d'information (l'entropie) associée à cette expérience est $\log_2(2) = 1$ sh. Le récepteur reçoit une unité d'information.

Exemples

- Exemple 3

  On considère une source pouvant transmettre trois valeurs : oui/non/je ne sais pas. Les résultats sont équiprobables.

  - Analyse intuitive

    Trois résultats différents peuvent se produire. Le message émis par cette source est « plus riche » en information que la source de l'exemple 2. On peut dire que la quantité d'information de cette expérience est supérieure à la précédente.

  - Analyse par la théorie de l'information

    Trois résultats existent : « oui » et « non », « je ne sais pas ». Ces résultats sont équiprobables.

    Par définition la quantité d'information associée à cette expérience est $\log_2(3) = 1{,}58$ sh.

Conclusion

- La théorie de l'information fournit un modèle mathématique permettant de quantifier l'information émise par la source d'une communication.
- Constat 1 : Plus les résultats d'une expérience peuvent prendre de valeurs différentes, plus la quantité d'information mesurée est élevée.
  - Intuitivement, ce résultat est logique. Une source pouvant transmettre beaucoup de messages différents fournit plus d'information qu'une source transmettant une seule valeur.
- Constat 2 : Lorsqu'une source peut produire beaucoup de valeurs différentes, l'incertitude quant au résultat de l'expérience est élevée. Or la quantité d'information transmise est d'autant plus grande que le nombre de résultats possibles est différent.

La quantité d'information reçue est d'autant plus importante que l'incertitude est grande !

Propriété de l'entropie

- On admettra la propriété suivante, qui découle des constatations précédentes :

L'entropie d'une source S pouvant produire N messages différents est maximale lorsque les messages sont équiprobables.

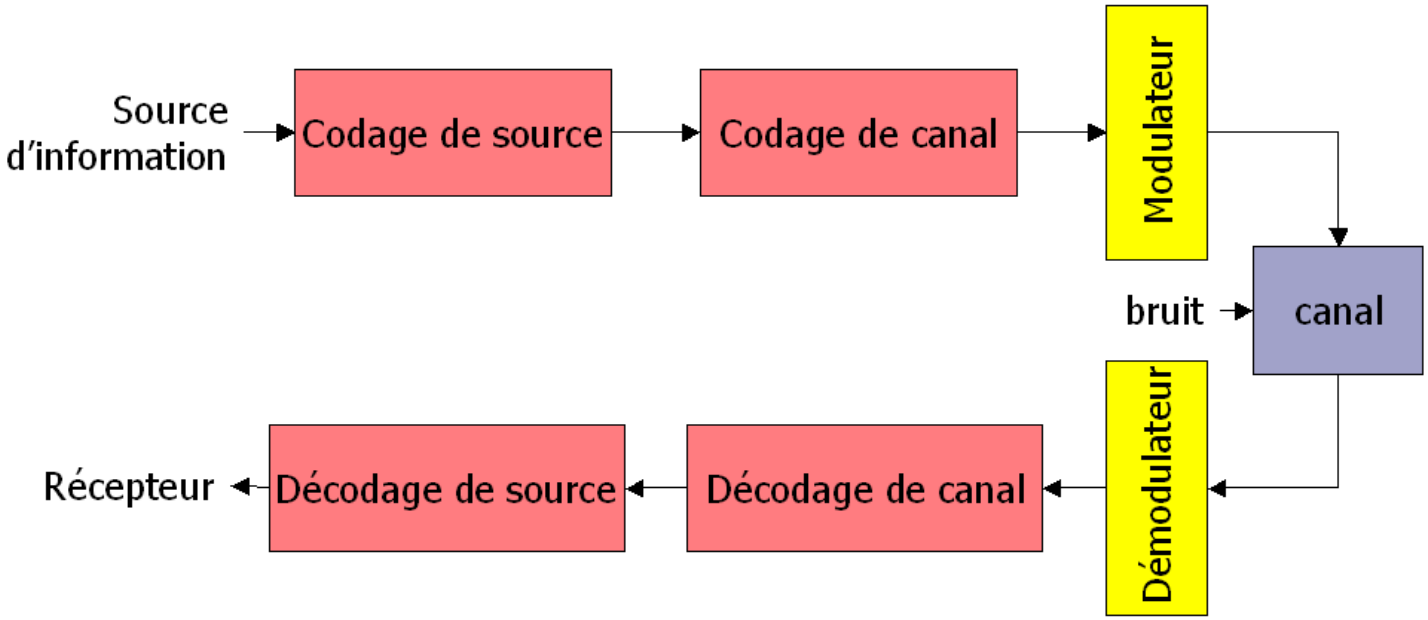
- Ce qui signifie que la quantité d'information est maximale lorsqu'on a le plus de difficulté à prévoir le résultat.
- Exemple : La source émet deux symboles : A et B

	P(A)	P(B)	H(S)
Cas 1	0,8	0,2	0,722
Cas 2	0,5	0,5	1

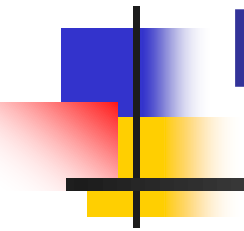
⇨ Cas 1 : La lettre A a « plus de chance » d'être reçue que B. On a moins d'information que dans le cas 2, où on est incapable de prévoir la lettre reçue.

Système de communication : codage de source et codage de canal

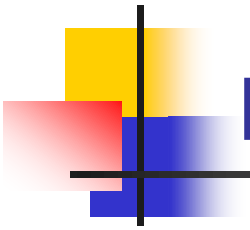
- Maintenant que nous savons mesurer l'information contenue dans un message, nous pouvons le coder.



- Le codage de source représente le message sous la forme la plus économique possible en terme de nombre de bits
- Le codage de canal ajoute des informations permettant au récepteur de reconstituer le message malgré les erreurs éventuellement apparues à cause du bruit sur le canal.



Le codage de source

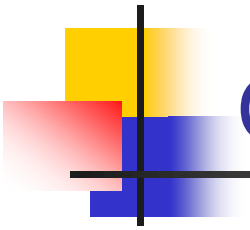


Enjeu du codage de source

- Le but du codage de source est de trouver une traduction binaire des messages émis par la source économisant les bits et tenant compte de leur contenu informatif.

- Par exemple, si la source émet
  - la lettre A avec la probabilité 0,8,
  - et les lettres B, C, D et E avec la probabilité 0,05,

  on sent intuitivement qu'il vaut mieux coder A avec peu de bits, car cette lettre revient souvent, tandis que B, C, D et E peuvent être codées sur un plus grand nombre de bits.



Capacité d'un canal

- En pratique, le débit binaire autorisé sur un canal est limité (influence du bruit, nature du support, etc. …).

- Le débit le plus élevé auquel on peut transmettre sur un canal, quel que soit le message produit par la source, est appelé la capacité C du canal.

Théorème de Shannon

- Le théorème de Shannon montre qu'on peut toujours trouver un codage de source permettant de transmettre à la capacité du canal si le débit Ds des symboles émis par la source et l'entropie de la source vérifient

$$H(S) \times Ds \leq C$$

Pb : il ne dit pas comment le trouver !

- Exemple : On considère une source émettant les lettres A, B, C, D et E avec les probabilités $p_A = 0,8$ et $p_B = p_C = p_D = p_E = 0,05$. Les lettres sont émises au débit $Ds = 10^6$ lettres/s. Le canal a une capacité C = 2 Mbit/s.
  - Entropie de la source : H(S) = 1,12 sh
  - $H(S) \times Ds = 1,12.10^6 < 2.10^6$
  - Donc il existe un code permettant de transmettre ces lettres sur le canal.

Exemple de recherche d'un codage de source

- On considère une source mettant 800 lettres par minute
  - Des lettres A avec une probabilité $p_A = 0,8$
  - Des lettres B avec une probabilité $p_B = 0,2$
- Le canal utilisé présente un débit binaire $D_b = 10$ bit/s

- 1er essai : Codage direct
  - On choisit par exemple

    Lettre A $\rightarrow$ 0 Lettre B $\rightarrow$ 1
  - Longueur moyenne des mots du code : Lmoy = 1bit/lettre
  - Le débit binaire nécessaire sur le canal est alors 13,33 bit/s.
  - Ce code ne convient donc pas.

Exemple de recherche d'un codage de source

- 2ème essai : Codage fractionné
  - On regroupe les lettres 2 par 2 et on code chaque groupe de lettres par un nombre de bits qui décroît selon la probabilité d'apparition du groupe de lettres (méthode de Fano).

Groupement de lettres	Probabilités	Codage	Nombre pondéré de bits
AA	0,64	0	0,64
AB	0,16	10	0,32
BA	0,16	110	0,48
BB	0,04	111	0,12
			1,56

  - Lmoy = 0,78 bit/lettre
  - Débit nécessaire sur le canal : 13,33×0,78 = 10,4 bit/s.
  - Ce codage ne convient pas. Cependant, il est meilleur que le précédent.

Exemple de recherche d'un codage de source

- 3ème essai : Codage fractionné
  - On regroupe cette fois les lettres 3 par 3.

Groupement de lettres	Probabilités	Codage	Nombre pondéré de bits
AAA	51,20%	0	0,512
AAB	12,80%	100	0,384
ABA	12,80%	101	0,384
BAA	12,80%	110	0,384
ABB	3,20%	11100	0,160
BAB	3,20%	11101	0,160
BBA	3,20%	11110	0,160
BBB	0,80%	11111	0,040
			2,184

  - Lmoy = 0,728 bit/lettre
  - Débit nécessaire sur le canal : 13,33×0,728 = 9,7 bit/s. Ce code convient.

Exemple de codage de source : La méthode de Fano

- La méthode de Fano fournit un codage binaire instantané (i.e. décodable à la volée). Elle est proche de la méthode de Huffman, utilisée dans les compressions JPEG et MPEG notamment (voir cours SRC2).

- La méthode de Fano permet d'attribuer peu de bits aux messages qui reviennent le plus souvent. Les messages les plus rares sont codés par plus de bits. On parle de codage à longueur variable ou RLE (*Run Length Encoding*) ou code entropique.

Mode opératoire de la méthode de Fano

1. Classer les messages de la source dans l'ordre des probabilités décroissantes.

2. Diviser l'ensemble des messages en deux groupes de probabilités aussi proches que possibles et
   - Attribuer 0 par exemple au premier
   - Attribuer 1 au second.

3. Recommencer les subdivisions successivement.

Exemple

- On reprend l'exemple précédent. La source émet les lettres A et B avec les probabilités p_A=0,8 et p_B=0,2. On groupe les lettres 3 par 3.

1er regroupement

messages	probabilités	probabilités regroupées	1er bit
AAA	51,20%	51,20%	0
AAB	12,80%	48,80%	1
ABA	12,80%		1
BAA	12,80%		1
ABB	3,20%		1
BAB	3,20%		1
BBA	3,20%		1
BBB	0,80%		1

Exemple

2ème regroupement

messages	probabilités	probabilités regroupées	1er bit	2ème bit
AAA	51,20%		0	
AAB	12,80%	24,80%	1	0
ABA	12,80%		1	0
BAA	12,80%	24,00%	1	1
ABB	3,20%		1	1
BAB	3,20%		1	1
BBA	3,20%		1	1
BBB	0,80%		1	1

Exemple

3ème regroupement

messages	probabilités	probabilités regroupées	1er bit	2ème bit	3ème bit
AAA	51,20%		0		
AAB	12,80%	12,80%	1	0	0
ABA	12,80%	12,80%	1	0	1
BAA	12,80%	12,80%	1	1	0
ABB	3,20%	10,40%	1	1	1
BAB	3,20%		1	1	1
BBA	3,20%		1	1	1
BBB	0,80%		1	1	1

Deux sous-regroupements

Exemple

4ème regroupement

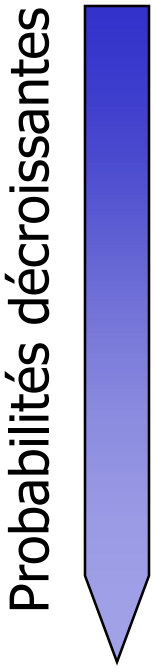
messages	probabilités	probabilités regroupées	1er bit	2ème bit	3ème bit	4ème bit
AAA	51,20%		0			
AAB	12,80%		1	0	0	
ABA	12,80%		1	0	1	
BAA	12,80%		1	1	0	
ABB	3,20%	6,40%	1	1	1	0
BAB	3,20%		1	1	1	0
BBA	3,20%	4%	1	1	1	1
BBB	0,80%		1	1	1	1

Exemple

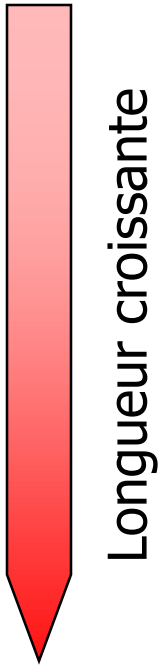
5ème regroupement

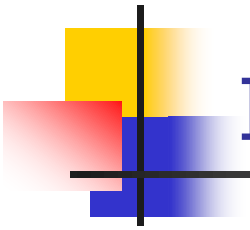
messages	probabilités	probabilités regroupées	1er bit	2ème bit	3ème bit	4ème bit	5ème bit
AAA	51,20%		0				
AAB	12,80%		1	0	0		
ABA	12,80%		1	0	1		
BAA	12,80%		1	1	0		
ABB	3,20%	3,20%	1	1	1	0	0
BAB	3,20%	3,20%	1	1	1	0	1
BBA	3,20%	3%	1	1	1	1	0
BBB	0,80%	0,80%	1	1	1	1	1

Exemple



Messages	Probabilités	Code
AAA	51,20%	0
AAB	12,80%	1 0 0
ABA	12,80%	1 0 1
BAA	12,80%	1 1 0
ABB	3,20%	1 1 1 0 0
BAB	3,20%	1 1 1 0 1
BBA	3,20%	1 1 1 1 0
BBB	0,80%	1 1 1 1 1





Intérêt pour le décodage

- Le code de Fano est un code à décodage direct.

- Il n'y a pas d'ambiguïté au décodage car aucun mot n'est la début d'un autre mot.

Méthodes à dictionnaire Méthode LZ78

Principe:

- Le principe commun consiste à encoder des séquences de caractères par les références à leurs emplacements dans un dictionnaire.
- Le dictionnaire est construit à partir du texte lui-même
- Il contient toutes les séquences déjà rencontrées

Méthodes à dictionnaire Méthode LZ78

Méthode LZ78 :

- Le dictionnaire sera construit au fur et à mesure de la lecture du texte à compresser.
- A tout instant le dictionnaire représente la partie du texte déjà lu, découpée en séquences numérotées.
- Le numéro 0 est réservé à la chaîne de caractères vide.
- Chaque séquence codée sera remplacée par un couple : (i , c).
- i est le numéro d'entrée dans le dictionnaire du préfixe composé des n-1 premiers caractères.
- c est le dernier caractère de la séquence codée.
- On parcourt le texte restant à compresser à partir du caractère courent tant que la séquence lue existe dans le dictionnaire. On s'arrête dès qu'une séquence nouvelle, non encore enregistrée dans le dictionnaire, est trouvée. Ce procédé garantit que la nouvelle séquence s est de la forme

Méthodes à dictionnaire Méthode LZ78

ELLE EST BELLE CETTE ECHELLE ETERNELLE. ELLE EST REELLE.

- On initialise le dictionnaire avec la séquence vide à l'emplacement 0.

On lit le caractère "E". Cette séquence n'est pas présente dans le dictionnaire. On le remplace par le couple $(0^j, E^j)$ et enregistre dans le dictionnaire la séquence "E" à l'adresse i = 1

- Le caractère lu : "L". Cette séquence n'est pas dans le dictionnaire. On la remplace par le couple $(0^j, L^j)$ et on enregistre "L" dans le dictionnaire à l'emplacement i = 2.
- Caractère lu : "L". Séquence présente dans le dictionnaire à l'adresse i = 2.
- On lit le caractère suivant. La séquence en attente devient : "LE". Elle n'est pas dans le dictionnaire. On la remplace par le couple $(2, E)$ et on l'enregistre dans le dictionnaire à l'adresse i = 3.

LZ78. Exemple

ELLE EST BELLE CETTE ECHELLE ETERNELLE. ELLE EST REELLE.

indice	Dictionnaire	Code	indice	Dictionnaire	Code
0	null		13	*H*E	(4,E)
1	E	(0,E)	14	CH	(10,H)
			15	ELL	(8,L)
			16	E*H*	(1,*H*)
			17	ETE	(11,E)
			18	R	(0,R)
6	T	(0,T)	19	N	(0,N)
7	*H*B	(4, B)	20	ELLE	(15,E)
8	EL	(1,L)	21	.	(0,.)
9	LE*H*	(3, *H*)	22	*H*ES	(13,S)
10	C	(0,C)	23	T*H*	(6,*H*)
11	ET	(1,T)	24	RE	(18,E)
12	TE				

LZ78. Exemple

ELLE EST BELLE CETTE ECHELLE ETERNELLE. ELLE EST REELLE.

indice	Dictionnaire	Code	indice	Dictionnaire	Code
0	null		13	*H*E	(4,E)
1	E	(0,E)	14	CH	(10,H)
2	L	(0,L)	15	ELL	(8,L)
			16	E*H*	(1,*H*)
			17	ETE	(11,E)
			18	R	(0,R)
6	T	(0,T)	19	N	(0,N)
7	*H*B	(4, B)	20	ELLE	(15,E)
8	EL	(1,L)	21	.	(0,.)
9	LE*H*	(3, *H*)	22	*H*ES	(13,S)
10	C	(0,C)	23	T*H*	(6,*H*)
11	ET	(1,T)	24	RE	(18,E)
12	TE				

LZ78. Exemple

ELLE EST BELLE CETTE ECHELLE ETERNELLE. ELLE EST REELLE.

indice	Dictionnaire	Code	indice	Dictionnaire	Code
0	null		13	*H*E	(4,E)
1	E	(0,E)	14	CH	(10,H)
2	L	(0,L)	15	ELL	(8,L)
3	LE	(2,E)	16	E*H*	(1,*H*)
			17	ETE	(11,E)
			18	R	(0,R)
6	T	(0,T)	19	N	(0,N)
7	*H*B	(4, B)	20	ELLE	(15,E)
8	EL	(1,L)	21	.	(0,.)
9	LE*H*	(3, *H*)	22	*H*ES	(13,S)
10	C	(0,C)	23	T*H*	(6,*H*)
11	ET	(1,T)	24	RE	(18,E)
12	TE				

LZ78. Exemple

ELLE EST BELLE CETTE ECHELLE ETERNELLE. ELLE EST REELLE.

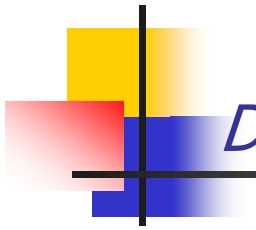
Indice	Dictionnaire	Code	Indice	Dictionnaire	Code
0	Null		14	CH	(10, H)
1	E	(0,E)	15	ELL	(8, L)
2	L	(0,L)	16	E␣	(1, ␣)
3	LE	(2,E)	17	ETE	(11, E)
4	␣	(0, ␣)	18	R	(0, R)
5	ES	(1,S)	19	N	(0, N)
6	T	(0, T)	20	ELLE	(15, E)
7	␣B	(4, B)	21	.	(0, .)
8	EL	(1, L)	22	␣EL	(13, L)
9	LE␣	(3, ␣)	23	LE␣L	(9, L)
10	C	(0, C)	24	␣ES	(13, S)
11	ET	(0, T)	25	T␣	(6, ␣)
12	TE	(6, E)	26	RE	(18, E)
13	␣E	(4, E)	27	ELLE.	(20, .)

Décodage

Voici le décodage du code de notre premier exemple :

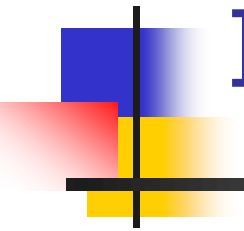
(0E, 0L, 2E, 0*H*, 1S, 0T, 4B, 1L, 3*H*, 0C, 1T, 6E, 4E, 10H, 8L, 1*H*, 11E, 0R, 0N,

- Le dictionnaire est initialisé par la chaîne de caractères vide à l'adresse 0.
- Couple (0, E). Séquence décodée : 'E'. Adresse dans le dictionnaire : i = 1. Texte='E'
- Couple (0, L). Séquence décodée : 'L'. Adresse dans le dictionnaire : i = 2. Texte='EL'
- Couple (2, E). Séquence décodée : 'LE'. Adresse dans le dictionnaire : i = 3. Texte='ELLE'
- Couple (0, *H*). Séquence décodée : '*H*'. Adresse dans le dictionnaire : i = 4. Texte='ELLE '
- Couple (1, S). Séquence décodée : 'ES'. Adresse dans le dictionnaire : i = 5. Texte='ELLE ES'

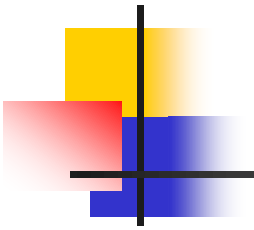


Décodage

- Couple (0, T). Séquence décodée : 'T'. Adresse dans le dictionnaire :
  i = 6. Texte='ELLE EST'
- Couple (4, B). Séquence décodée : '*H*B'. Adresse dans le dictionnaire :
  i = 7. Texte='ELLE EST B'
- Couple (1, L). Séquence décodée : 'EL'. Adresse dans le dictionnaire :
  i = 8. Texte='ELLE EST BEL'
- Couple (3, *H*). Séquence décodée : 'LE '. Adresse dans le dictionnaire :
  i = 9. Texte='ELLE EST BELLE '
- Couple (0, C). Séquence décodée : 'C'. Adresse dans le dictionnaire :
  i = 10. Texte='ELLE EST BELLE C'
- Couple (1, T). Séquence décodée : 'ET'. Adresse dans le dictionnaire :
  i = 11. Texte='ELLE EST BELLE CET'
- etc

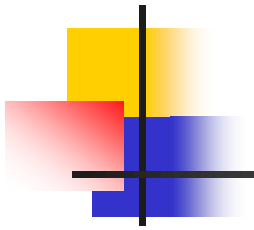


Introduction au codage de canal



Codage du canal

- Généralités
- Théorème du codage de canal
- Codes linéaires
- Codes cycliques
- Codes convolutifs



- Codes linéaires
  - Codes groupes

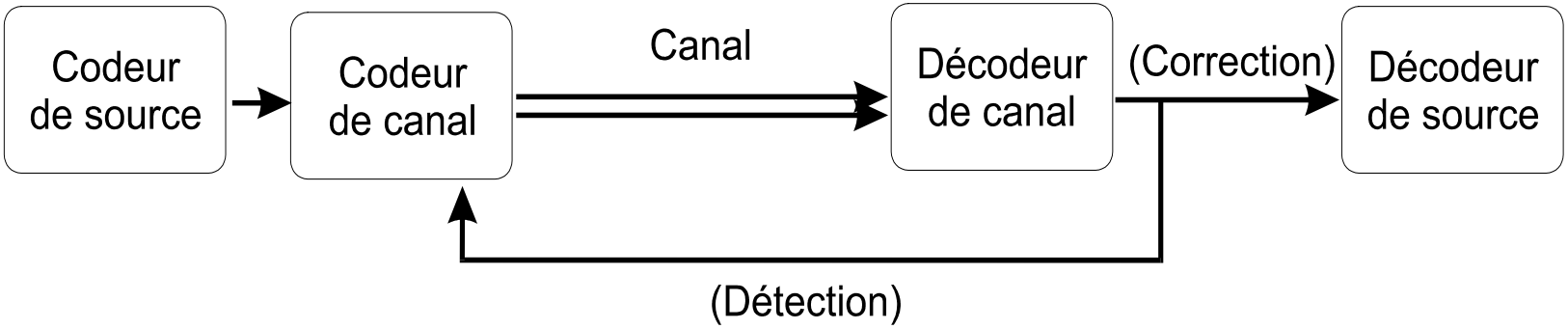
    Parité, Code de Hamming
  - Codes cycliques

    CRC/FCS, code BCH, Golay

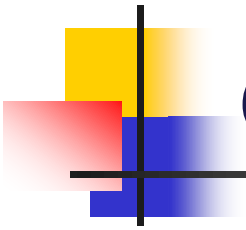
- Codes convolutifs

  Algorithme de Viterbi

Généralités



Codeur de canal ↖ **introduire** une **redondance** utilisable



Généralités

Les canaux discrets :

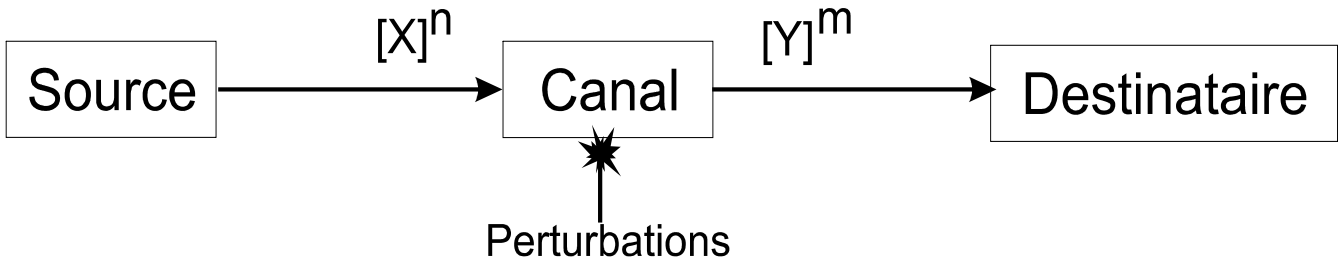
- **Canal** : milieu de transmission de l'information situé entre la source et la destination. Le canal opère une transformation entre l'espace des symboles à l'entrée et celui de la sortie.

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

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

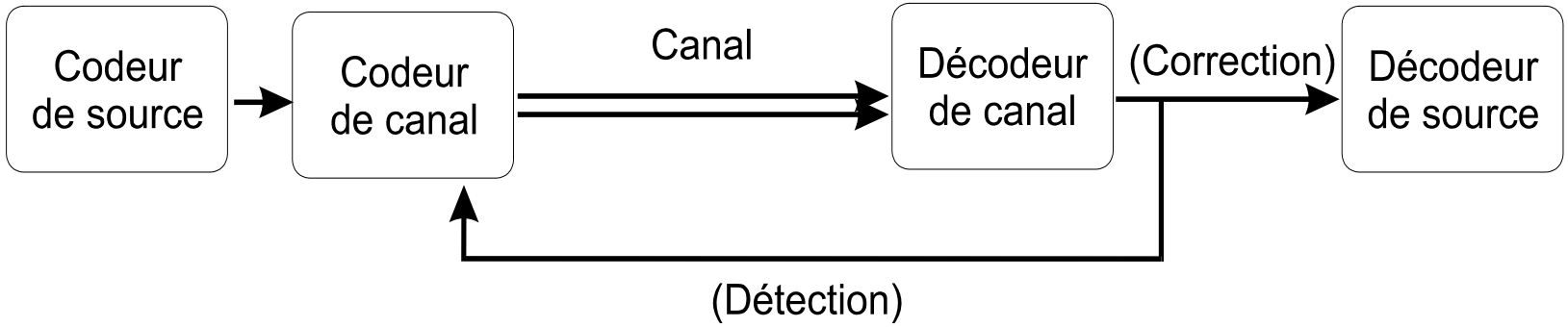
- **Canal stationnaire** : si les transformations ne dépendent pas de l'origine des temps

Généralités



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

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



Généralités

Transinformation & capacité

- Capacité d'un canal

$$C = Max(I(X;Y))$$

- Redondance d'un canal

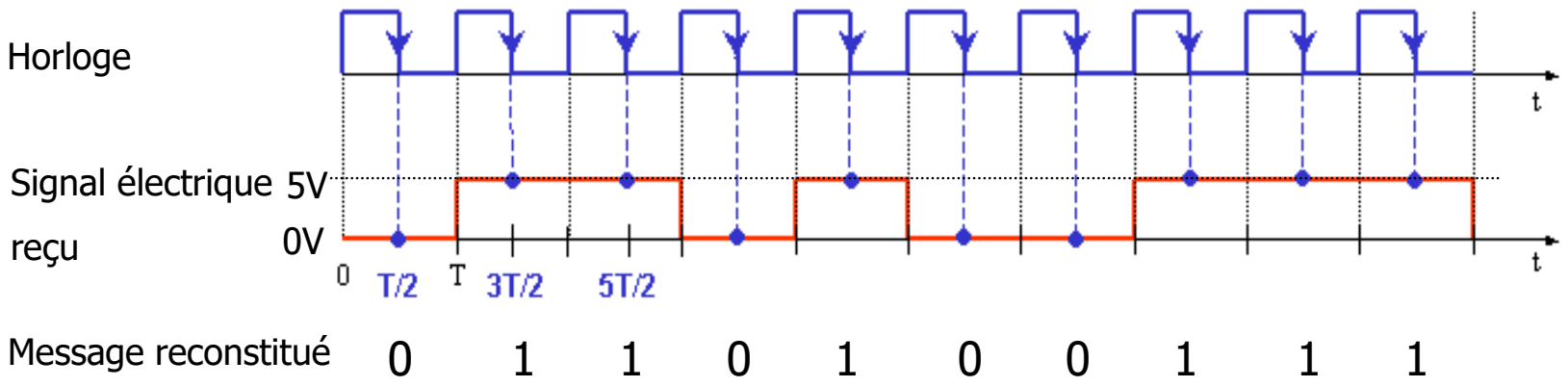
$$Rc = C - I(X;Y)$$

- Efficacité d'un canal

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

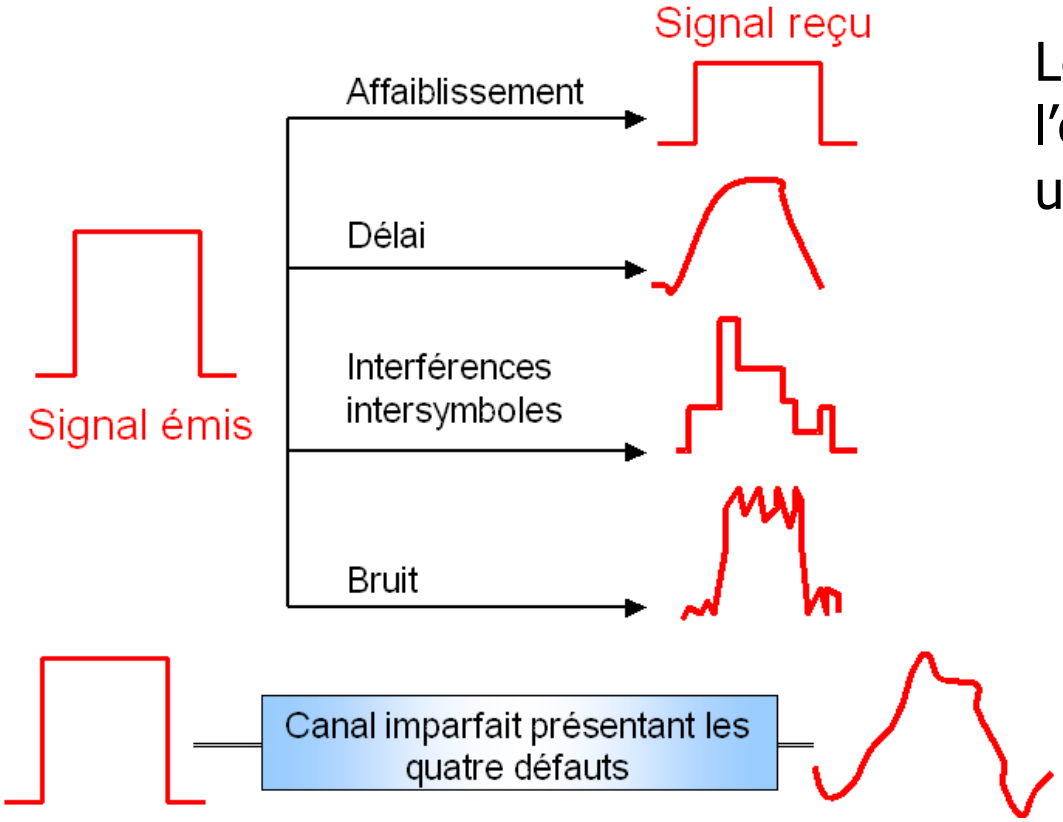
Enjeu du codage de canal

- Le codage de canal rajoute de l'information pour permettre au récepteur de détecter ou corriger les erreurs éventuellement apparues.
- Comment le récepteur lit-il les données reçues ?
  - Il échantillonne le signal physique reçu à intervalle de temps fixe, au milieu du bit. Suivant le niveau de tension lu, il déduit la valeur du bit : 0 ou 1.

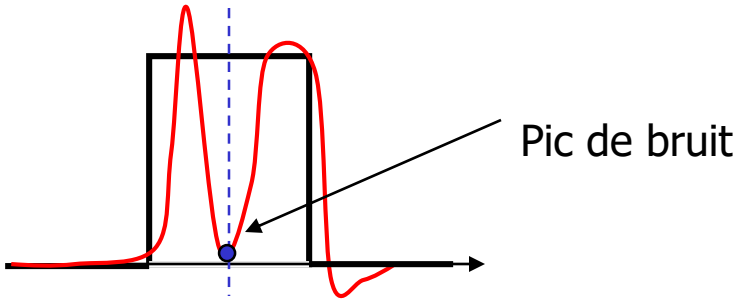


Enjeu du codage de canal

- D'où viennent les erreurs ?



Le signal est déformé sur le canal : l'échantillonnage peut se faire sur une perturbation.



A l'échantillonnage, le récepteur interprète le niveau de tension comme un 0.

- Conclusion : Puisque le récepteur ne peut se fier au signal électrique reçu, on va rajouter des bits dans les messages qui permettront de repérer les erreurs.

Détection/correction d'erreur

- Certains codes permettent de détecter des erreurs, d'autres de détecter et corriger les erreurs.
- La correction d'erreur contraint à ajouter plus de bits que la détection d'erreur.
- Par conséquent, on adopte un code correcteur d'erreur quand on ne peut pas retransmettre les messages :
  - Transmission dans un seul sens (émission TV)
  - Transmission satellite (la retransmission prend trop de temps)
  - Transmission en temps réel.

Détection d ’erreur par bit de parité

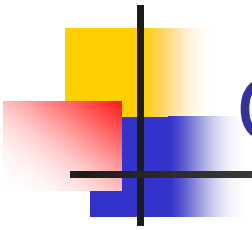
- **VRC (**Vertical Redundancy Check)
  - Asynchrone

Caractère	O	S	I
Bit 0	1	1	1
Bit 1	0	0	0
Bit 2	0	1	0
Bit 3	1	0	1
Bit 4	1	0	0
Bit 5	1	1	0
Bit 6	1	1	1
Bit de parité	1	0	1
Bit d'imparité	0	1	0

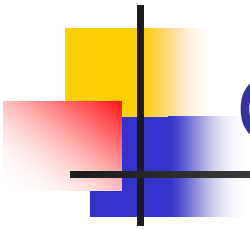
- **LRC (**Longitudinal Redundancy Check)
  - Synchrone

	H	E	L	L	O	LRC →
bit 1	0	1	0	0	1	0
bit 2	0	0	0	0	1	1
bit 3	0	1	1	1	1	0
bit 4	1	0	1	1	1	0
bit 5	0	0	0	0	0	0
bit 6	0	0	0	0	0	0
bit 7	1	1	1	1	1	1
VRC ↓	0	1	1	1	1	0

0001001	0	1010001	1	0011001	1	0011001	1	1111100	1	0100001	0
H		E		L		L		O		LRC	



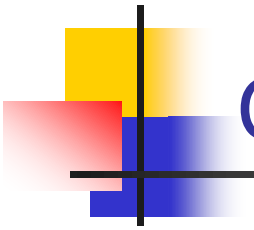
Code de hamming



Conclusion

- Les techniques de détection et correction d'erreurs seront étudiées dans le cours sur la transmission en bande de base (semestre 2).

- Ce qu'il faut retenir
  - Le codage de source a pour but de transmettre le contenu informatif du message en économisant les bits.
  - Le codage de canal rajoute au message des bits qui seront utilisés par un algorithme de réception pour déterminer s'il y a des erreurs et les corriger éventuellement.
  - Paradoxalement, le codage de canal ajoute de la redondance, alors que le codage de source a pour tâche de l'éliminer !
  - C'est le prix à payer pour garantir la qualité de la communication.
  - La solution est de bien connaître le canal, afin de déterminer la probabilité d'erreur et de ne rajouter que les bits strictement nécessaires.



Conclusion

Bibliographie

- « Théorie de l'Information », R. Beauvillain, ENSEA, support de cours, 1998.
- http://encyclopedie.snyke.com/
- « Théorie de l'Information et Codage », M. P. Béal (université de Marne La Vallée) & Nicolas Sendrier (INRIA), mars 2004