Introduction à la théorie de l'information

Chapitre I : Notions générales

Prof. Tewfiq EL MALIKI
Bachlor ITI,
Laboratoire de télécommunicaitons

Contenu

- Introduction de Shannon
- Les théorèmes de Shannon
- Définition des Bruits
- Première Théorème
- Deuxième Théorème
- Troisième Théorème
- Exercices

Le cours

- Théorie un mois: Mardi 14.00 - 17.00
  Vendredi 10.00 - 12.00
- Pratique : 5 fois
  - Fréquence des lettres
  - Codage
  - Code correcteur
  - Cryptage
- Support de cours : théorie de l'information,

Qu’est ce qu’est la théorie de l’information

- La théorie de l'information concerne la mesure et la transmission d'informations par un canal bruité.
- Une base fondamentale dans ce domaine est la théorie de l'information de Shannon, qui fournit de nombreux outils utiles qui sont basés sur les mesures d’information en termes de bits, bit/s et corrections d’erreurs.

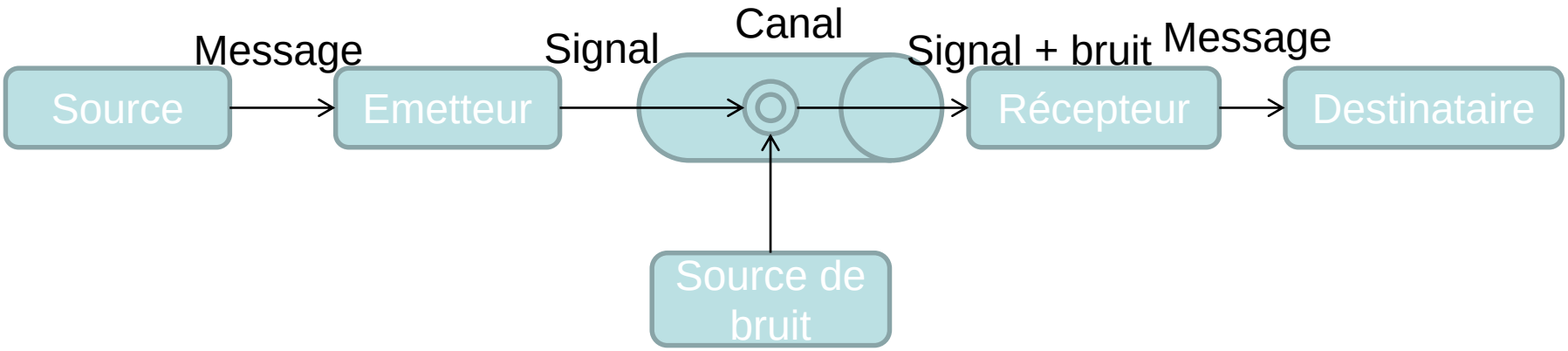
Les idées de Shannon

- Former la base pour le champ de la théorie de l'information
- Fournir les critères permettant de mesurer l'efficacité d'un système de communication.
- Identifié les problèmes qui devaient être résolus pour arriver à des systèmes de communication idéaux

Théorie de l’information

- Théorie mathématique issue des travaux de Shannon et Weaver publiés en 1964.
- Nyquist au début du siècle vers 1904 a déjà posé des jalons.
- Shannon a défini un modèle de transmission basé sur le schéma de communication de base.

Schéma de communication



- La source d'information produit un message sous la forme d'une suite d'information qu'on suppose binaire
- Le message est transformé en signal adapté au canal (milieu de transmission : faisceau hertzien, câble coaxial, fibre, ou bus d'ordinateur) dont la puissance P_s
- Canal est bruité par un bruit qu'on suppose Gaussien de puissance P_n
- Le récepteur accomplit la fonction inverse pour restituer le message initial et le délivrer au destinataire

Trois questions fondamentales

- Quelle est la compression de données maximale pour une source d'information?
- Quelle quantité de données (bits / s) peut être envoyée de manière fiable sur un canal de communication bruyant?
- Avec quelle précision peut-on représenter un échantillon (par exemple, audio ou image) en fonction du nombre de bits utilisés ?

Bruit

- **Définition**
  - Signal qui peut dénaturer le message, le rendre difficilement perceptible ou causer sa perte partielle ou totale. Le bruit peut être considéré Comme une donnée sans sens.
  - Deux propriétés
    - Pas de corrélation entre les échantillons
    - Un effet gênant et perturbateur
  - Un perturbateur est un signal électrique parasite qui vient se superposer à un signal utile
  - Remarque : **le signal perturbateur est gênant d'autant plus le signal utile est faible**

Bruit utile ou inutiles?

- Le bruit peut être gênant mais aussi utile.
- Dans le cas d'une classe un étudiant qui parle pendant le cours perturbe les autres
- En revanche, s'il veut cacher le message que le professeur veut communiquer sur lui et perturbe les autres c'est utile pour lui et gênant pour le professeur

Canal bruité

- Le signal transmis peut être bruité entre l'émetteur et le récepteur
- Pour retrouver le message émis à partir d'un signal reçu, l'émetteur va ajouter de la redondance. Ainsi, le récepteur est capable de détecter ou corriger une ou plusieurs erreurs.
- Dans le premier cas, c'est un code détecteurs et dans le second un code correcteurs.

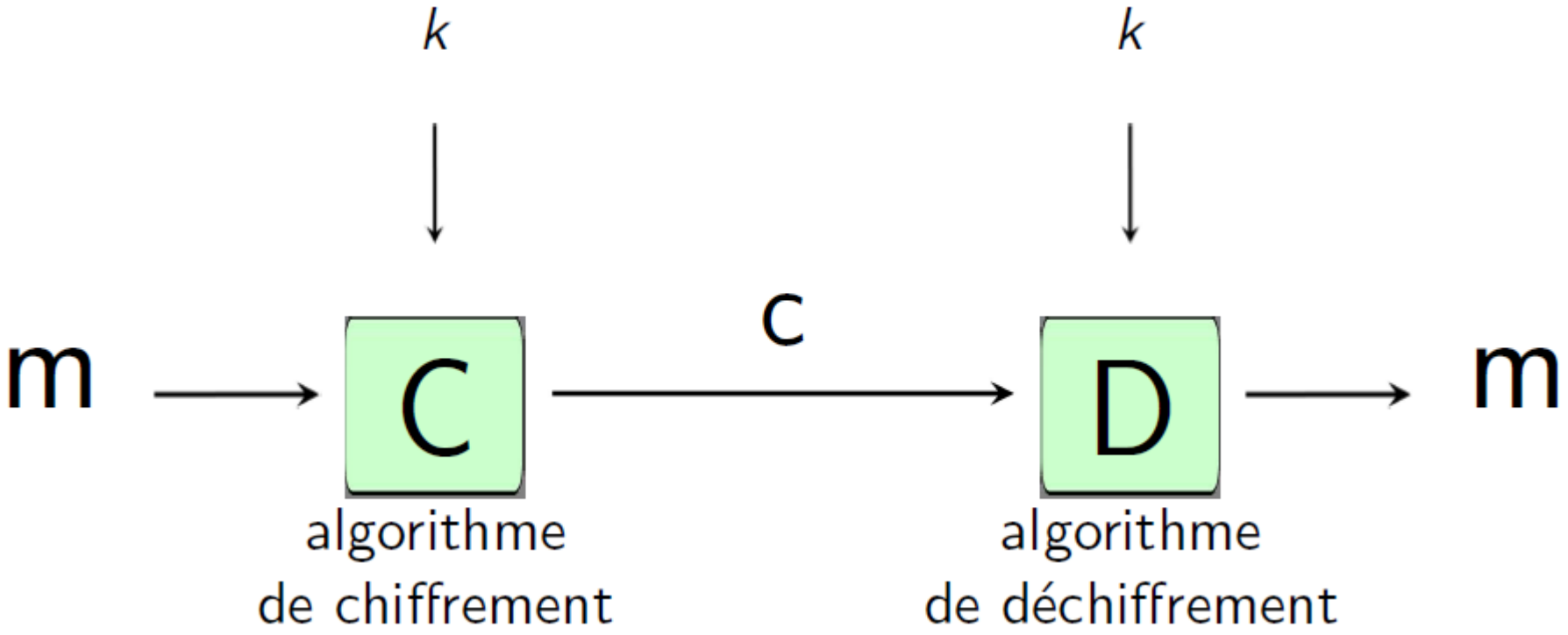
Canal bruité : but

- Le but de la théorie est de transmettre rapidement mais correctement un message
- Dans le cas de la problématique du secret, le bruit est le vecteur perturbateur du message pour qu'il ne soit pas clair.
- Le but est alors de construire une perturbation du message dans l'intention de rendre le message incompréhensible mais détectable par le récepteur.

Cryptographie

- La cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages c'est-à-dire de les rendre inintelligibles.
- Les efforts conjoints d'IBM et de la NSA conduisent à l'élaboration du DES (Data Encryption Standard), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXème siècle.

Modèle de cryptage



- Si la clef est la même, le cryptage est symétrique; autrement il est asymétrique

Comment avoir un système de chiffrement sûr et efficace?

- La théorie de Shannon préconisant de mêler confusion et diffusion
  - Confusion : masquer la relation entre le clair et le chiffré
  - Diffusion : cacher la redondance en répartissant l'influence d'un bit de clé sur tout le chiffré

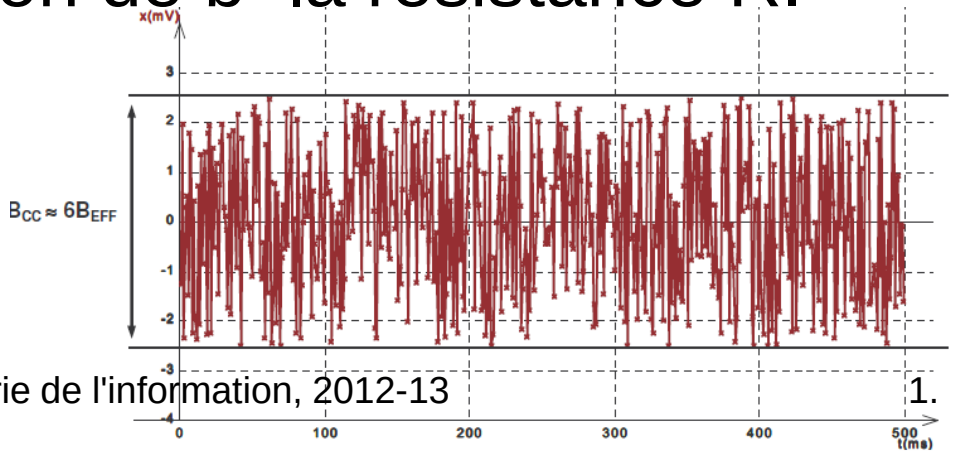
Origines du bruit

- Origine technique :
  - Mauvaise conception de circuit, manque de blindage, mauvais contact
- Origine environnementale :
  - Actions de grandeurs d’influence telles que température ou humidité (vieillissement, défaut)
- Origine fondamentale
  - La structure microscopique bruit de fond

Bruit de Fond

- C'est un signal aléatoire b(t) qui est superposé à un signal utile
  - S'agissant d'un signal aléatoire il a autant de probabilité d'avoir la valeur +u que la valeur –u donc la moyenne est nulle. Par contre, la valeur efficace est différent de zéro et se calcule en fonction de b^2 la résistance R.
  - La puissance

est $P_n=B_{eff}/R$



Trois théorèmes fondamentales (Shannon)

- Codage de source
- Codage de canal
- Débit-distortion
- (Echantillonnage)

Problèmes encore posés

- Shannon a défini avec ses théorèmes les limites théoriques mais n’a pas démontré comment en arriver.
- Ainsi, Hamming, Solomon, Reed et Shannon lui-même ont contribué à trouver du moins certains algorithmes pour s’approcher des limites théoriques

Après Shannon

- Des méthodes pratiques ont été inventées et mis en œuvre:
  - Codage de source: les codages de Huffman (compact), Shannon-Fano, Lempel-Ziv (compresse, gzip)
  - codage de canal: codes correcteurs d'erreurs (Hamming, Reed-Solomon, convolution, treillis, turbo)
  - débit-distorsion: vocodeurs, minidisques, MP3, JPEG, MPEG

Applications

- Théorie de la communication
  - L'article de Shannon publié en 1948 a présenté les trois principaux théorèmes et leurs **démonstrations**. Les limites fournies par les théorèmes sont utiles, ils nous donnent des objectifs à tendre vers (compression optimale des données, le débit le plus élevé) et nous donnent l'optimum d'un système de communications qui ne sera pas dépassé selon cette théorie.
  - La compression des données:

    Codes de Huffman, les codes arithmétiques, Lempel-Ziv.
  - Théorie des sciences informatiques:
    Bornes inférieures sur temps de calcul, la complexité
  - VLSI: complexité communication:

    le calcul par rapport à la communication
  - Mathématiques et statistiques:

    investissements et théorie des jeux

Trois domaines de recherches

- Efficience : Théorie de l'information
- Correction d'erreurs : Théorie de codage
- Secret : Cryptographie

Information

- Dans la définition de l'information, Shannon a identifié les relations critiques entre le des éléments d'un système de communication; à savoir
  - la puissance à la source d'un signal
  - la largeur de la bande ou de la fréquence d'un canal d'information à travers laquelle le signal se déplace
  - le bruit qui va modifier le signal connu par sa puissance
  - le récepteur, qui doit décoder le signal.

Shannon Théorie

- Les mots sont des symboles pour transporter des informations entre les gens.
- Dire bonjour à un français est compréhensible mais dit à un chinois donnera un regard interrogateur le français est un code non compréhensible par un chinois.

Chaine de communication

- Toute communication comporte trois étapes

1. Codage du message à sa source

2. Transmettre ce message par un canal de communication

3. Le décodage du message à sa destination.

Discret vs Continue

- Nous codons le message qui peut être discret ou continue.
- S’il est continue il faut le numériser pour profiter des avantages de la numérisation
- Théorème d’échantillonnage est démontrée par Nyquist est reprise par Shannon.

Transmission

- Un message doit être codé et transmis à quelqu'un ou, dans le cas d'un ordinateur, à quelque chose.
- La transmission peut se faire par la voix, une conversation téléphonique, une émission de radio ou de télévision.
- Le destinataire est quelqu'un ou quelque chose qui doit recevoir les symboles, puis les décoder en les combinant avec le codage préétablis par son interlocuteur

Exemple de codage

- Supposons que nous suivons de voitures passant sur une autoroute et que 50% des voitures sont noirs, 25% sont blancs,12,5% sont rouges, et 12,5% sont bleus sans perdre de généralité
- Prenons l'autoroute une source de voitures: noir, blanc, rouge et bleu. Une façon simple d'encodage en symboles binaires serait d'associer chaque couleur avec deux bits, qui est : **noir = 00**, blanc= 01, rouge = 10, et bleu = 11 , une moyenne de 2,00 bits de par couleur.

Efficacité par théorie de l'info

- Un meilleur encodage peut être construit en associant la fréquence d'apparition de certains symboles ou des mots:
  noir = 0, blanc = 10, rouge = 110, bleu = 111.
  Comment est-ce codage mieux?
  0,50 noir x 1 bit = .500
  0,25 blanches x 2 bits = .500
  0.125 rouges x 3 bits = .375
  0.125 bleu x 3 bits = .375
  Moyenne – lmoy =1.750 bits par voiture

Entropie

- Une mesure quantitative du désordre d'un système et est inversement proportionnelle à la quantité d'énergie disponible pour effectuer un travail dans un système isolé. Plus l'énergie est devenue dispersée, le moins de travail qu'il peut effectuer et plus l'entropie est élevée.

Mesure de Shannon Sh

Soit S un espace d'échantillons avec la distribution de probabilité p.

Alors le Quantité d'information moyenne de l'information est donnée par:

Q= log(1/pi)

$$H(S) = - \Sigma\ p_i \log_2(p_i)$$

Note: logarithme en base 2 est utilisé

H est communément connu comme l'entropie interprétée comme «incertitude»

Interprétation I

- Des informations apparues dans un journal local
  - A. Un chien dangereux du type pitbull a mordu un passant qui l'a excité
  - B. le meilleur étudiant de la classe est présent dans le cours de base de télécommunications
  - Quelle est la quantité d'information des deux informations?

Interprétation II

- Des informations apparues dans un journal international
  - A. Un passant dangereux du type pitbull a mordu un chien qui l'a excité
  - B. le mauvais étudiant de la classe est présent dans le cours de base de télécommunications
  - Quelle est la quantité d'information des deux informations?

Calcule des quantités d’info

Exemple des voitures

- Quelle est l’entropie?
- Quelle est votre conclusion?

Propriété de la mesure de Shannon

- H est continue par rapport p
- H est symétrique, c'est à dire l'ordre de p n'influence pas la valeur de H
- H est additif, si X et Y sont deux espaces d'échantillons indépendants, alors H (X, Y) = H (X) + H (Y)
  H prend sa valeur maximale si P est uniforme

Other properties

- $H(P) \leq \log n$ avec $H(P) = \log n$ si $p = 1 / n$
- $H(P) \geq 0$, avec $H(P) = 0$ si $p_k = 1$

- Remarque: deux autres distributions de probabilité P & Q peuvent conduire à la même entropie H (P) = H (Q); par exemple P = {0,5, 0,25, 0,25}, Q = {0,48, 0,32, 0,2} ==> H (p) = H (Q) = 1,5

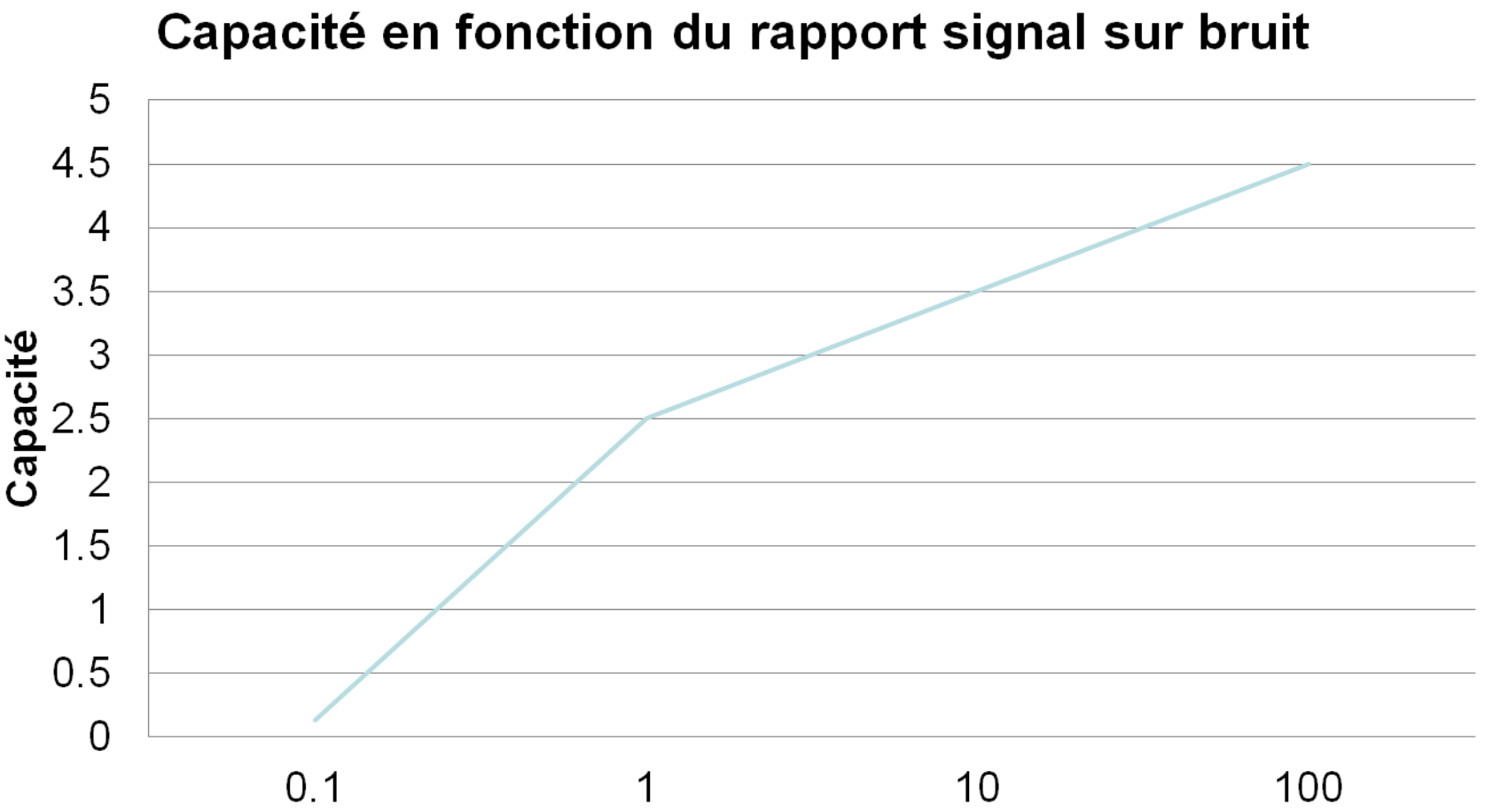
Capacité d'un canal

- La capacité d'information (ou capacité de canal) C d'un canal avec une bande passante B en Hertz perturbé par un bruit blanc gaussien de densité spectrale de puissance $N_0/2$, sur une largeur de bande B

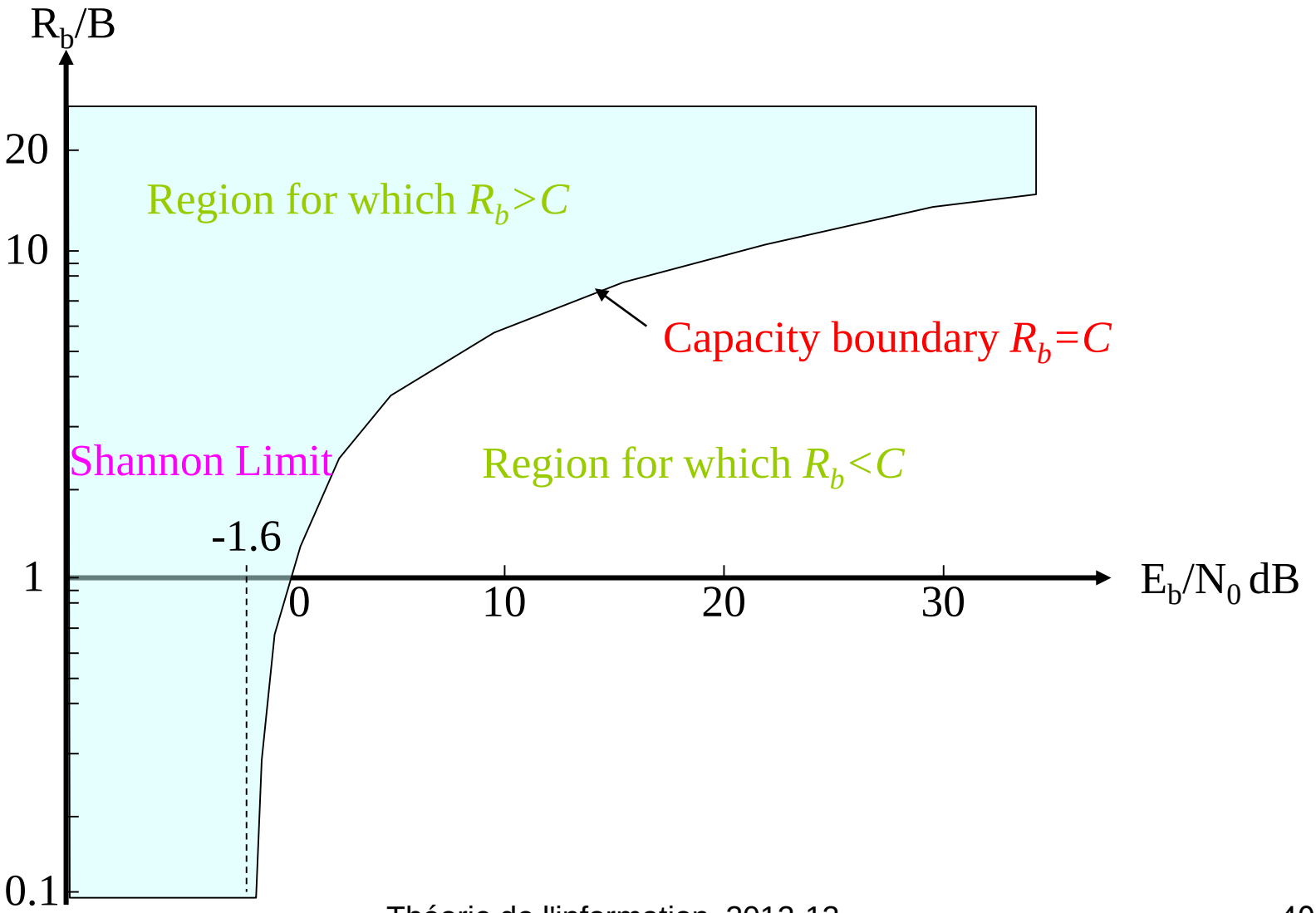
$$C = B\log_2\left(1+\frac{P}{N_0 B}\right) bits/s$$

  - où P est la puissance du signal émis
  - $P = E_b.R_b$ (pour un système idéal, $R_b = C$).
  - E_b est l'énergie transmise par bit,
  - R_b est la vitesse de transmission.

Capacité d’un canal



Shannon Limit



Théorèmes de Shannon I & II

1. Soit une source amnésique dont l'entropie est H [Sh], tout codage de source pour la compression d'information peut atteindre un nombre moyen lmoy [bit/sym] aussi bas que possible; mais jamais inférieur a H $\leq$lmoy
2. Une communication à travers un canal de capacité C peut atteindre une probabilité inférieure à ε moyennant un code correcteur ssi le débit binaire est inférieur à C.

Théorèmes de Shannon II

Supposons que nous voulons transmettre des informations d’une source à l'utilisateur avec une distorsion ne dépassant pas D. Comment faire ?

Théorèmes de Shannon III

La théorie débit-distorsion nous dit qu'au moins R (D) bits / symbole de l'information de la source doit parvenir à l'utilisateur. La capacité du canal est C (où C <H), alors H - C bits / symbole seront perdus lors de la transmission de cette information sur le canal donné .

Pour avoir le moindre espoir de reconstruire avec un maximum de distorsion D, nous devons imposer l'exigence que l'information perdue dans la transmission ne dépasse pas la perte maximale tolérable de H - R (D) bits / symbole.

Cela signifie que la capacité du canal doit être au moins aussi grand que R (D).