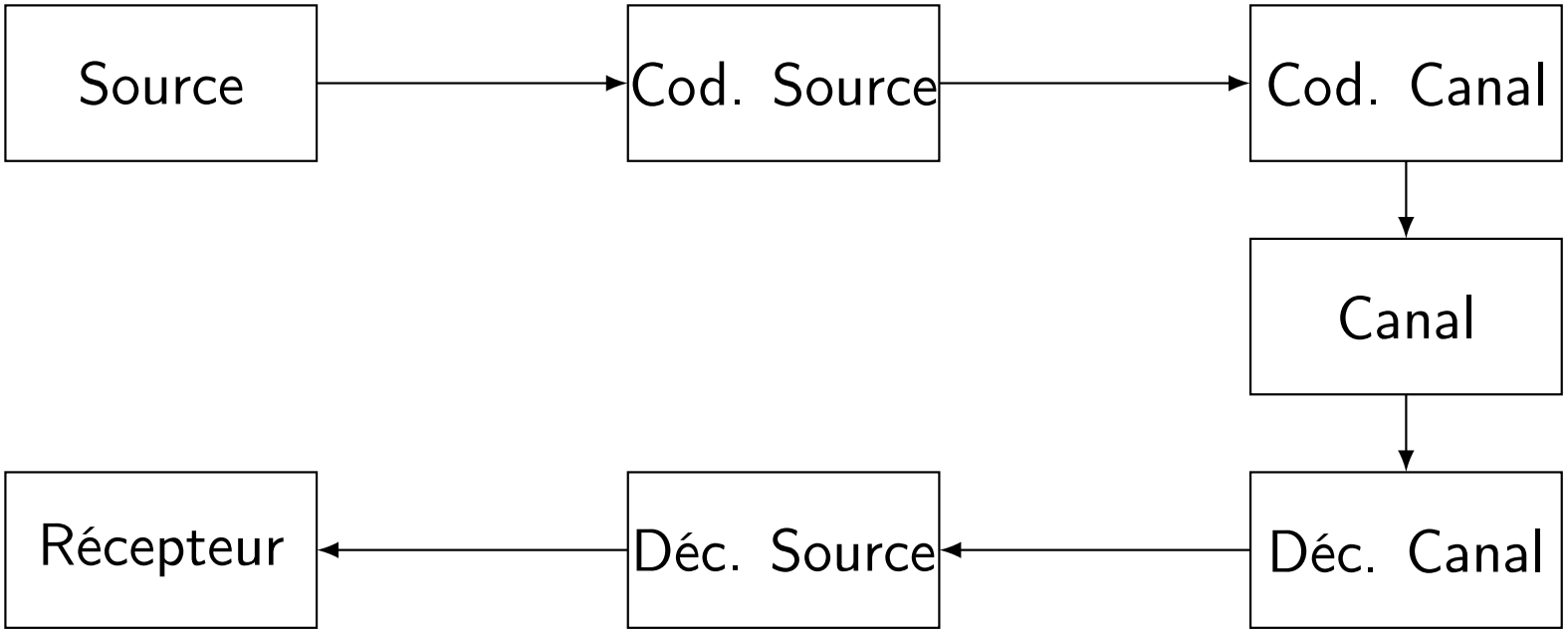
Théorie de l'information
MMA331

Nicolas Barbot

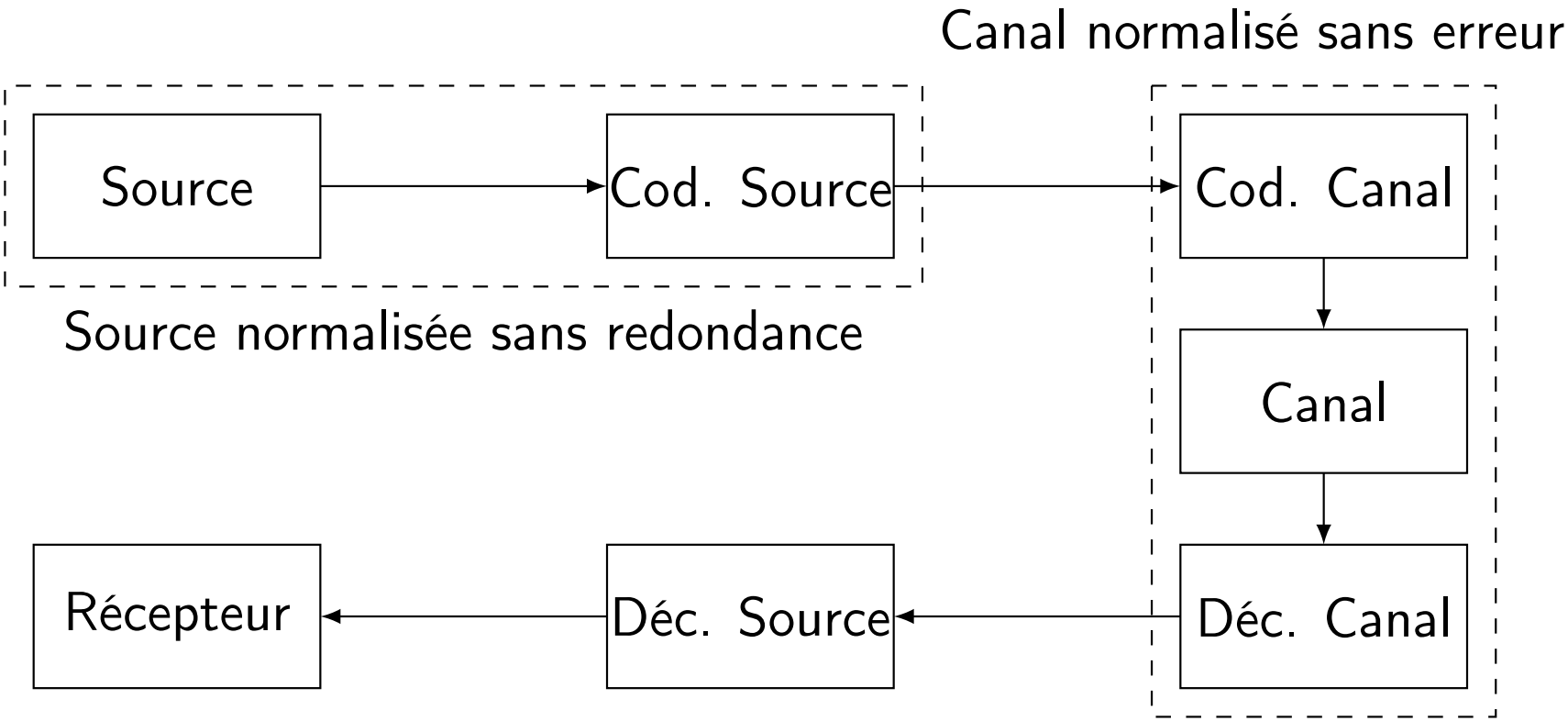
nicolas.barbot@esisar.grenoble-inp.fr

2016-2017

Paradigme de Shannon



Paradigme de Shannon



- Codage de source: élimination de la redondance de la source
- Codage de canal: élimination des perturbations du canal

Théorie de l'information

La théorie élabore un cadre mathématique de la notion d'information basée sur les probabilités d'apparition des messages (la théorie ne considère pas le contenu des messages).

La théorie de l'information permet de déterminer les bornes en performance des opérations de codage de source et de codage de canal.

Aspect qualitatif

On cherche à donner une définition mathématique de l'information. Intuitivement, les critères suivants doivent être respectés pour quantifier l'information:

Aspect qualitatif

On cherche à donner une définition mathématique de l'information. Intuitivement, les critères suivants doivent être respectés pour quantifier l'information:

- la quantité d'information d'un message est inversement proportionnelle à la probabilité de réalisation du message

Aspect qualitatif

On cherche à donner une définition mathématique de l'information. Intuitivement, les critères suivants doivent être respectés pour quantifier l'information:

- la quantité d'information d'un message est inversement proportionnelle à la probabilité de réalisation du message
- quand la probabilité d'une réalisation est 1, il n'y a pas d'information

Aspect qualitatif

On cherche à donner une définition mathématique de l'information. Intuitivement, les critères suivants doivent être respectés pour quantifier l'information:

- la quantité d'information d'un message est inversement proportionnelle à la probabilité de réalisation du message
- quand la probabilité d'une réalisation est 1, il n'y a pas d'information
- l'information de deux réalisations indépendantes est égale à la somme de l'information de chaque réalisation.

Aspect qualitatif

On cherche à donner une définition mathématique de l'information. Intuitivement, les critères suivants doivent être respectés pour quantifier l'information:

- la quantité d'information d'un message est inversement proportionnelle à la probabilité de réalisation du message
- quand la probabilité d'une réalisation est 1, il n'y a pas d'information
- l'information de deux réalisations indépendantes est égale à la somme de l'information de chaque réalisation.
- l'information moyenne d'une source augmente avec le nombre de messages possibles

Mesure de l'information

La quantité d'information apportée par une réalisation ayant une probabilité p vaut:

$$h = \log_2 \frac{1}{p} \tag{1}$$

Exemples:

- Faire face avec une pièce:
- Faire 3 avec un dé:
- Gagner au loto:
- Perdre au loto:

Mesure de l'information

La quantité d'information apportée par une réalisation ayant une probabilité p vaut:

$$h = \log_2 \frac{1}{p} \tag{1}$$

Exemples:

- Faire face avec une pièce: $h = 1$ bit
- Faire 3 avec un dé:
- Gagner au loto:
- Perdre au loto:

Mesure de l'information

La quantité d'information apportée par une réalisation ayant une probabilité p vaut:

$$h = \log_2 \frac{1}{p} \tag{1}$$

Exemples:

- Faire face avec une pièce: $h = 1$ bit
- Faire 3 avec un dé: $h = 2.585$ bits
- Gagner au loto:
- Perdre au loto:

Mesure de l'information

La quantité d'information apportée par une réalisation ayant une probabilité p vaut:

$$h = \log_2 \frac{1}{p} \tag{1}$$

Exemples:

- Faire face avec une pièce: $h = 1$ bit
- Faire 3 avec un dé: $h = 2.585$ bits
- Gagner au loto: $h \approx 24$ bits
- Perdre au loto:

Mesure de l'information

La quantité d'information apportée par une réalisation ayant une probabilité p vaut:

$$h = \log_2 \frac{1}{p} \tag{1}$$

Exemples:

- Faire face avec une pièce: $h = 1$ bit
- Faire 3 avec un dé: $h = 2.585$ bits
- Gagner au loto: $h \approx 24$ bits
- Perdre au loto: $h \approx 7.5 \times 10^{-8}$ bit

À vous de jouer !

Règles:

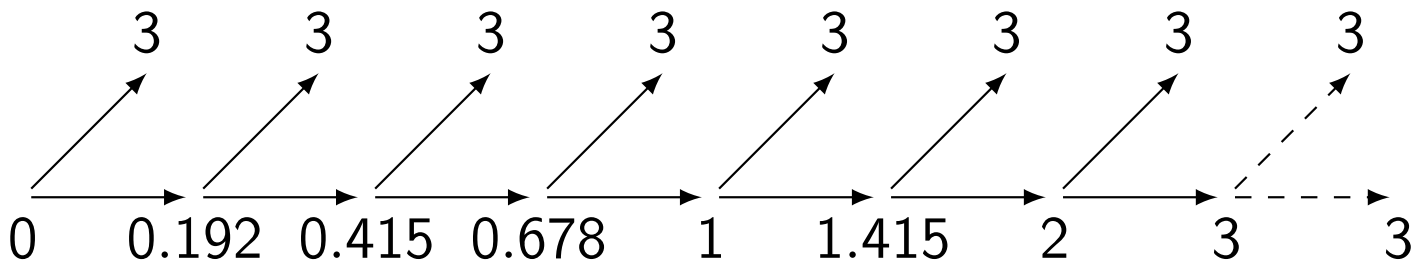
- Le prof choisit un nombre entier entre 0 et 7
- Les étudiants doivent poser des questions pour l'identifier
- Le prof ne peut répondre que par "vrai" ou "faux"
- Les étudiants doivent calculer l'information gagnée

Objectifs:

- Trouver le nombre (ainsi que l'information gagnée...)
- Trouver la stratégie optimale

À vous de jouer !

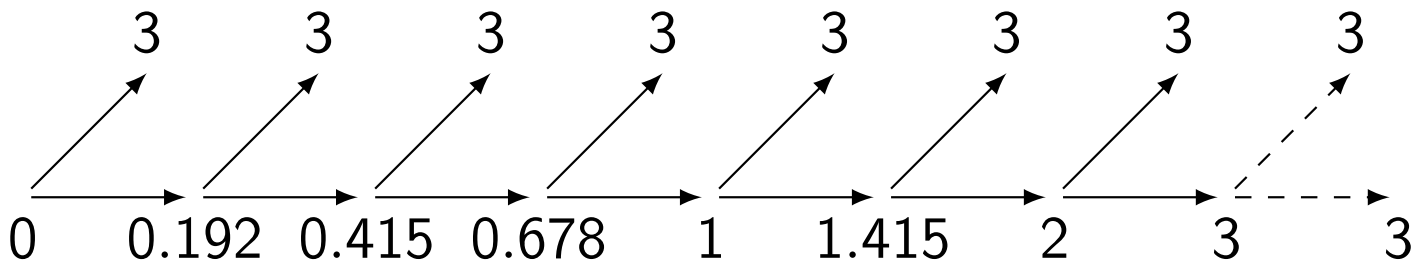
Stratégie 1: (naïve): "Est ce que le nombre est 0, 1, ... ?"



Nécessite 3.5 questions en moyenne...

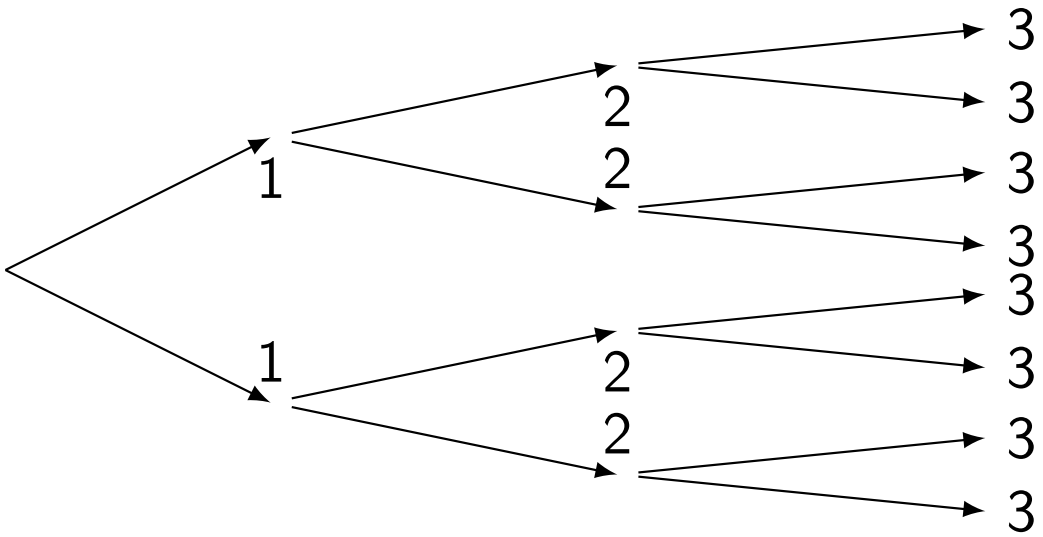
À vous de jouer !

Stratégie 1: (naïve): "Est ce que le nombre est 0, 1, ... ?"



Nécessite 3.5 questions en moyenne...

Stratégie 2: "Est ce que le nombre est ≥ 4, ... ?"



Entropie

L'entropie d'une source X est définie comme la valeur moyenne de l'information calculée sur l'ensemble des sorties possibles :

$$H(X) = \sum_{x \in \mathcal{A}_X} p(x) \log_2 \frac{1}{p(x)} = E_X \left(\log_2 (1/p(x)) \right) \qquad (2)$$

L'entropie représente l'incertitude d'une source (variable aléatoire).

Exemples:

- Lancer d'une pièce:
- Lancer un dé:
- Faire 3 avec un dé:
- Jouer au loto:

Entropie

L'entropie d'une source X est définie comme la valeur moyenne de l'information calculée sur l'ensemble des sorties possibles :

$$H(X) = \sum_{x \in \mathcal{A}_X} p(x) \log_2 \frac{1}{p(x)} = E_X \left(\log_2 (1/p(x)) \right) \qquad (2)$$

L'entropie représente l'incertitude d'une source (variable aléatoire).

Exemples:

- Lancer d'une pièce: $H = 1$ bit
- Lancer un dé:
- Faire 3 avec un dé:
- Jouer au loto:

Entropie

L'entropie d'une source X est définie comme la valeur moyenne de l'information calculée sur l'ensemble des sorties possibles :

$$H(X) = \sum_{x \in \mathcal{A}_X} p(x) \log_2 \frac{1}{p(x)} = E_X \left(\log_2 (1/p(x)) \right) \qquad (2)$$

L'entropie représente l'incertitude d'une source (variable aléatoire).

Exemples:

- Lancer d'une pièce: $H = 1$ bit
- Lancer un dé: $H = 2.585$ bits
- Faire 3 avec un dé:
- Jouer au loto:

Entropie

L'entropie d'une source X est définie comme la valeur moyenne de l'information calculée sur l'ensemble des sorties possibles :

$$H(X) = \sum_{x \in \mathcal{A}_X} p(x) \log_2 \frac{1}{p(x)} = E_X \left(\log_2 (1/p(x)) \right) \qquad (2)$$

L'entropie représente l'incertitude d'une source (variable aléatoire).

Exemples:

- Lancer d'une pièce: $H = 1$ bit
- Lancer un dé: $H = 2.585$ bits
- Faire 3 avec un dé: $H = 0.65002$ bit
- Jouer au loto:

Entropie

L'entropie d'une source X est définie comme la valeur moyenne de l'information calculée sur l'ensemble des sorties possibles :

$$H(X) = \sum_{x \in \mathcal{A}_X} p(x) \log_2 \frac{1}{p(x)} = E_X \left(\log_2 (1/p(x)) \right) \qquad (2)$$

L'entropie représente l'incertitude d'une source (variable aléatoire).

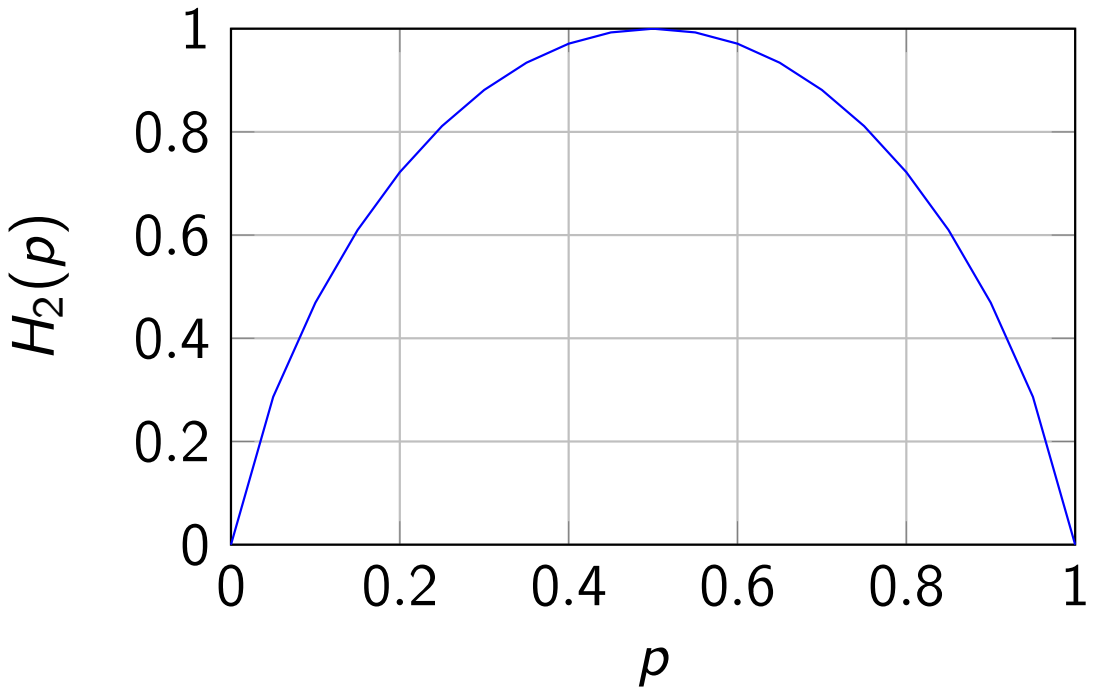
Exemples:

- Lancer d'une pièce: $H = 1$ bit
- Lancer un dé: $H = 2.585$ bits
- Faire 3 avec un dé: $H = 0.65002$ bit
- Jouer au loto: $H \approx 7.57 \times 10^{-8}$ bit

Fonction d'entropie binaire

L'entropie d'une source dont l'alphabet est $\mathcal{A}_X = \{a, b\}$ et la distribution de probabilités est $\mathcal{P}_X = \{p, (1-p)\}$ vaut:

$$H_2(p) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p} \tag{3}$$



$\max_p H_2(p) = 1$ bit
$\Rightarrow \mathcal{P}_X^* = 0.5$

Fonction d'entropie

Pour une source X pouvant prendre K valeurs, l'entropie vaut:

$$H(X) = \sum_{i=1}^{K} p_i \log_2 \frac{1}{p_i}$$

En appliquant l'inégalité de Jensen:

$$\begin{aligned} \sum_{i=1}^{K} p_i \log_2 \frac{1}{p_i} &\leq log_2 \left(\sum_{i=1}^{K} p_i \frac{1}{p_i} \right) \\ &\leq log_2 K \end{aligned}$$

Donc $H_{max} = \log_2 K$
De plus pour $p_i = 1/K$, on a $H = \log_2 K = H_{max}$ ainsi $p_i^* = 1/K$

Exercice

Une source peut générer 4 symboles avec les probabilités suivantes:

$$X = \begin{cases} a & \text{avec une probabilité } 1/2 \\ b & \text{avec une probabilité } 1/4 \\ c & \text{avec une probabilité } 1/8 \\ d & \text{avec une probabilité } 1/8 \end{cases}$$

Combien de bits sont nécessaires pour coder chaque symbole ?
Quelle est l'entropie de X ?

Exercice

Après avoir lancé une pièce (non biaisée) 2 fois, on construit la variable aléatoire suivante:

$$X = \begin{cases} a & \text{si le nombre de face est 0} \\ b & \text{sinon} \end{cases}$$

Déterminez les probabilités $p(a)$ et $p(b)$ de X.
Calculez l'entropie de cette source.

$$X = \begin{cases} 0 & \text{avec une probabilité } 0.9 \\ 1 & \text{avec une probabilité } 0.1 \end{cases}$$

Contenu bit brut

$$H_0(X) = \log_2 |\mathcal{A}_X|$$

Si $|\mathcal{A}_X|$ est une puissance de 2, c'est le nombre de bits permettant de coder X

Contenu bit essentiel

$$H_\delta(X) = \log_2 |S_\delta|$$

où S_δ est le plus petit ensemble de $|\mathcal{A}_X|$ pour lequel $p(x \in S_\delta) \geq 1 - \delta$. C'est le nombre de bits permettant de coder X au risque δ près

Extension d'une source

On considère maintenant que cette même source émet des symboles constitués de N réalisations indépendantes.

Extension d'une source

On considère maintenant que cette même source émet des symboles constitués de N réalisations indépendantes.

m	p
00	0.81
01	0.09
10	0.09
11	0.01

Extension d'une source

On considère maintenant que cette même source émet des symboles constitués de N réalisations indépendantes.

m	p
00	0.81
01	0.09
10	0.09
11	0.01

m	p
000	0.73
001	0.08
010	0.08
100	0.08
011	9e-3
101	9e-3
110	9e-3
111	1e-3

Extension d'une source

On considère maintenant que cette même source émet des symboles constitués de N réalisations indépendantes.

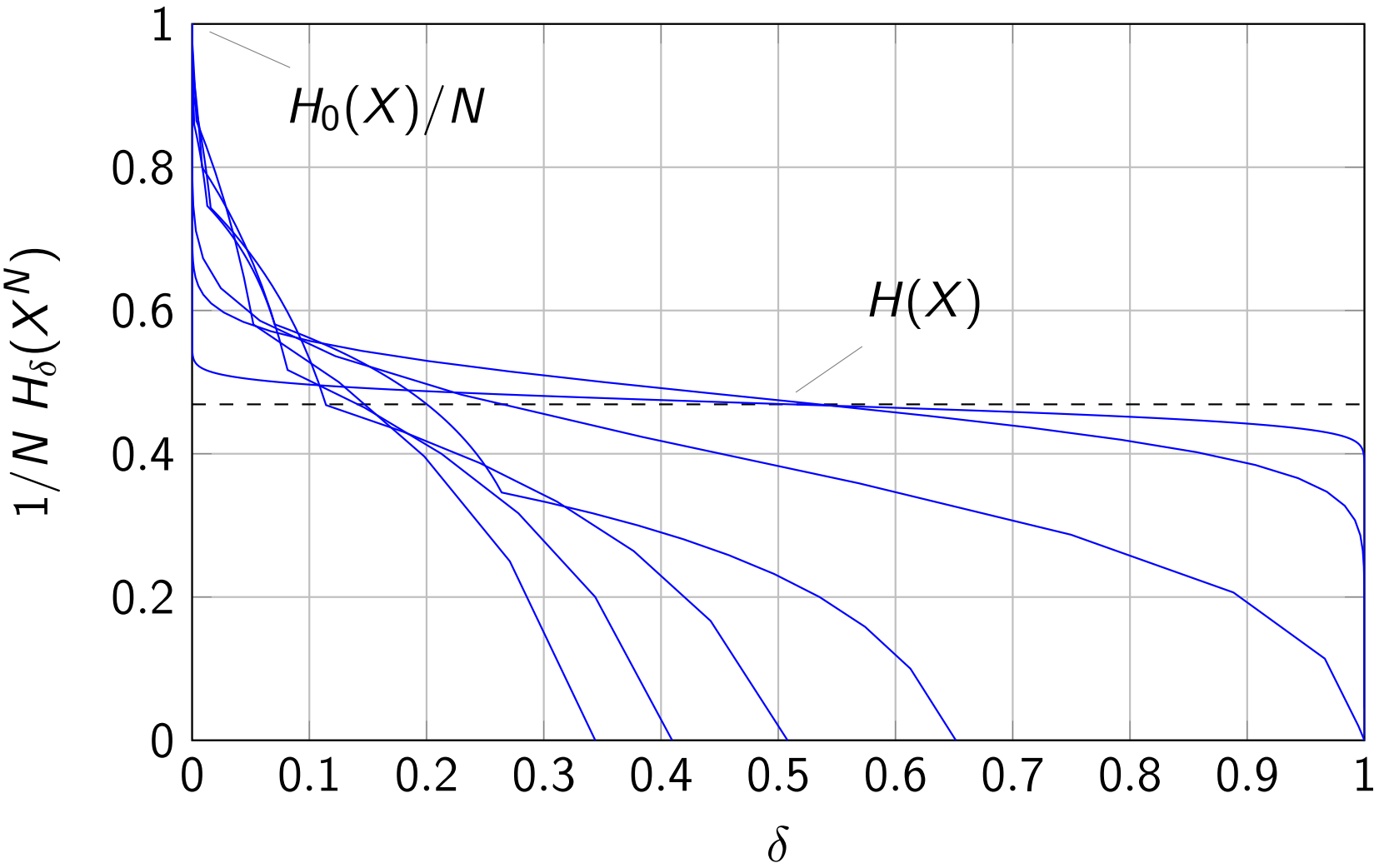
m	p
00	0.81
01	0.09
10	0.09
11	0.01

m	p
000	0.73
001	0.08
010	0.08
100	0.08
011	9e-3
101	9e-3
110	9e-3
111	1e-3

m	p
0000	0.65
0001	0.07
0010	0.07
0100	0.07
1000	0.07
0111	9e-4
1011	9e-4
1101	9e-4
1110	9e-4
1111	1e-4

m	p
00000	0.59
00001	0.06
00010	0.06
00100	0.06
01000	0.06
10111	9e-5
11011	9e-5
11101	9e-5
11110	9e-5
11111	1e-5

Impact de la longueur



1er Théorème de Shannon

Théorème du codage de source

Soit X un ensemble d'entropie $H(X) = H$ bits. Pour $\epsilon > 0$ et $0 < \delta < 1$ donnés, il existe un nombre positif entier N_0 tel que pour $N > N_0$,

$$\left| \frac{1}{N} H_\delta(X^N) - H \right| < \epsilon \tag{4}$$

1er Théorème de Shannon

Théorème du codage de source

Soit X un ensemble d'entropie $H(X) = H$ bits. Pour $\epsilon > 0$ et $0 < \delta < 1$ donnés, il existe un nombre positif entier N_0 tel que pour $N > N_0$,

$$\left| \frac{1}{N} H_\delta(X^N) - H \right| < \epsilon \tag{4}$$

1. Si $1/N\ H_\delta(X^N) < H + \epsilon$ alors le nombre de bit par symbole moyen peut passer de $H_0(X)$ à $H + \epsilon$ tout en limitant le risque δ à un niveau arbitrairement faible.

1er Théorème de Shannon

Théorème du codage de source

Soit X un ensemble d'entropie $H(X) = H$ bits. Pour $\epsilon > 0$ et $0 < \delta < 1$ donnés, il existe un nombre positif entier N_0 tel que pour $N > N_0$,

$$\left| \frac{1}{N} H_\delta(X^N) - H \right| < \epsilon \tag{4}$$

1. Si $1/N\ H_\delta(X^N) < H + \epsilon$ alors le nombre de bit par symbole moyen peut passer de $H_0(X)$ à $H + \epsilon$ tout en limitant le risque δ à un niveau arbitrairement faible.
2. Si $1/N\ H_\delta(X^N) > H - \epsilon$ alors le risque δ tend vers 1 et aucune information ne peut être récupérée.

Petit retour en arrière...

Dans le jeu slide 6 :

- Calculez $H_0(X)$
- Calculez $H(X)$
- Quel gain peut être apporté par un codeur de source parfait

Dans l'exercice slide 11 :

- Calculez $H_0(X)$ et $H(X)$
- Quel gain peut être apporté par un codeur de source parfait
- Essayez de trouver un codage où le nombre moyen de symboles est $< H_0(X)$

Même questions pour l'exemple slide 13

Entropie conjointe

Soit deux variables aléatoires X et Y de distribution de probabilité conjointe $p(x, y)$. L'entropie de l'ensemble est alors définie par:

$$H(X,Y) = \sum_{x \in \mathcal{A}_X} \sum_{y \in \mathcal{A}_Y} p(x,y) \log_2 \frac{1}{p(x,y)} \tag{5}$$

$$= E_{X,Y}\left(\log_2 \frac{1}{p(X,Y)} \right) \tag{6}$$

Propriétés

- $H(X,Y) = H(X) + H(Y)$ si X et Y sont indépendants
- $H(X,Y) \leq H(X) + H(Y)$ sinon

Entropie conditionnelle

On définit l'entropie conditionnelle de X sachant $y = b_k$:

$$H(X|y = b_k) = \sum_{x \in \mathcal{A}_X} p(x|y = b_k) \log_2 \frac{1}{p(x|y = b_k)}$$

L'entropie conditionnelle $H(X|Y)$ de X sachant Y est la moyenne sur y de l'entropie conditionnelle de X sachant y:

$$H(X|Y) = \sum_{y \in \mathcal{A}_Y} p(y) \left(\sum_{x \in \mathcal{A}_X} p(x|y) log_2 \frac{1}{p(x|y)} \right) \quad (7)$$

$$= \sum_{x \in \mathcal{A}_X} \sum_{y \in \mathcal{A}_Y} p(x, y) log_2 \frac{1}{p(x|y)} \quad (8)$$

Cette quantité mesure l'incertitude moyenne qui reste de X lorsque Y et connue

Quelques propriétés

Propriétés

- $0 \leq H(X) \leq \log_2 K$ où $K = |\mathcal{A}_X|$
  L'entropie est toujours positive et est maximum lorsque la source est équiprobable
- $H(Y|X) \leq H(Y)$
  Le conditionnement réduit l'entropie. L'égalité est obtenue si X et Y sont indépendants
- $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
  De plus si X et Y sont indépendants
  $H(X,Y) = H(X) + H(Y)$

Information mutuelle

On cherche à quantifier la quantité d'information qu'un événement $Y = y$ fournit sur la réalisation d'un événement $X = x$. On définit cette quantité par:

$$i(x; y) = \log_2 \frac{p(x|y)}{p(x)} \tag{9}$$

$i(x; y)$ est appelée l'information mutuelle entre les réalisations x et y. L'information mutuelle entre les variables aléatoires X et Y correspond à la moyenne de la quantité précédente:

$$I(X; Y) = \sum_{x \in \mathcal{A}_X} \sum_{y \in \mathcal{A}_Y} p(x, y) log_2 \frac{p(x|y)}{p(x)} \tag{10}$$

Information mutuelle

L'information mutuelle est une mesure de la quantité d'information qu'une variable aléatoire apporte sur une autre.

$$I(X;Y) = H(X) - H(X|Y) \tag{11}$$
$$= H(Y) - H(Y|X) \tag{12}$$
$$= I(Y;X) \tag{13}$$

$I(X;Y)$ représente donc la réduction de l'incertitude d'une VA lorsque l'autre est connue.

Propriétés

- $I(X;Y) = 0$ si X et Y sont indépendants
- $I(X;Y) = H(X) = H(Y)$ si $X = Y$

Information mutuelle conditionnelle

L'information mutuelle conditionnelle entre X et Y pour une valeur $Z = z$ donnée est:

$$I(X;Y|Z=z) = H(X|Z=x) - H(X|Y,Z=z)$$

L'information mutuelle conditionnelle entre X et Y sachant Z est la moyenne par rapport à Z de la quantité précédente:

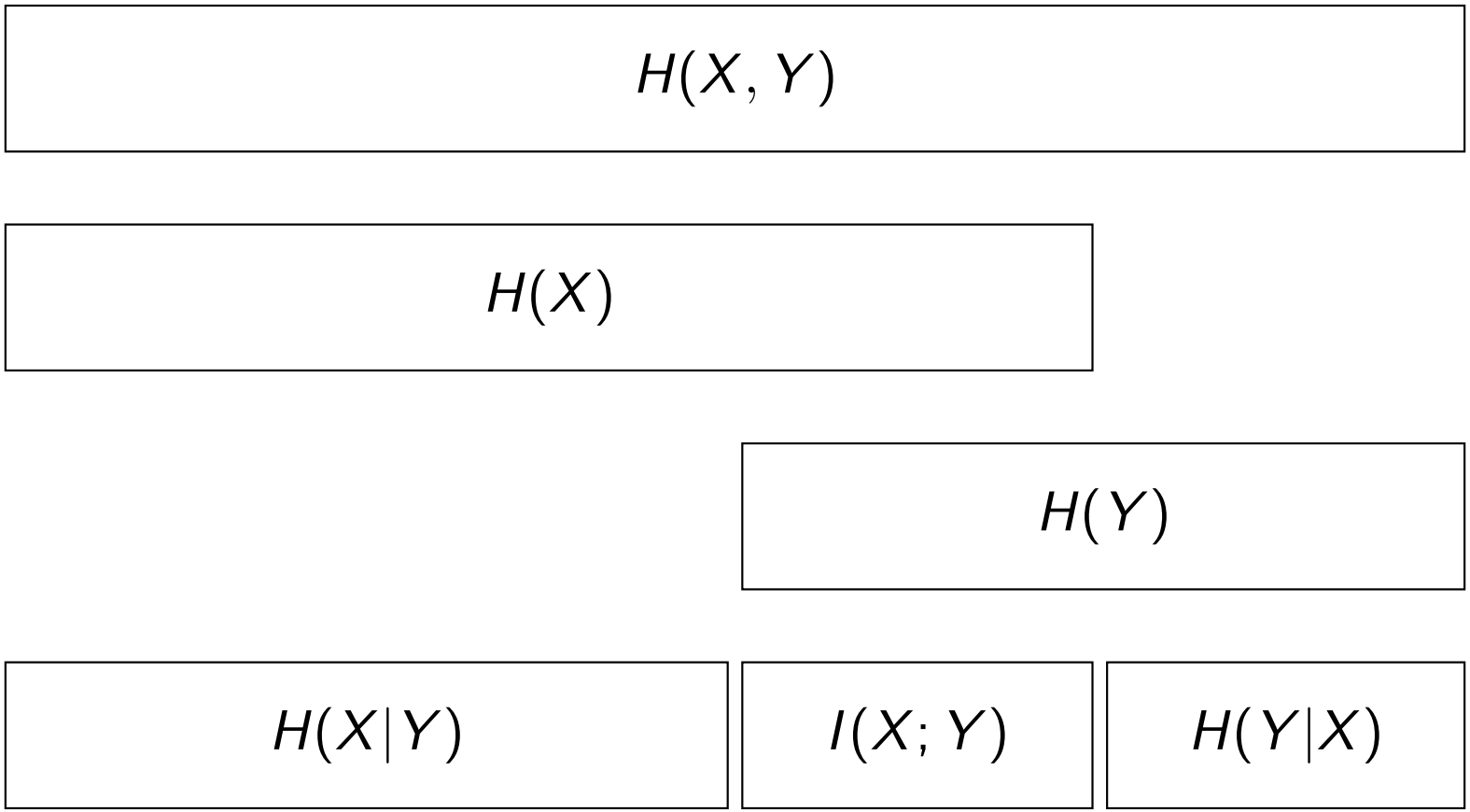
$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) \tag{14}$$

Quelques propriétés

Propriétés

- $0 \leq I(X;Y) \leq H(X)$
  L'information mutuelle est toujours positive et est maximum lorsque $X = Y$
- $I(X_1, X_2; Y) = I(X_1; Y) + I(X_2; Y|X_1)$ (chain rule)
  De plus si X_1 et X_2 sont indépendants
  $I(X_1, X_2; Y) = I(X_1; Y) + I(X_2; Y)$

Diagramme de l'information mutuelle



Exercice

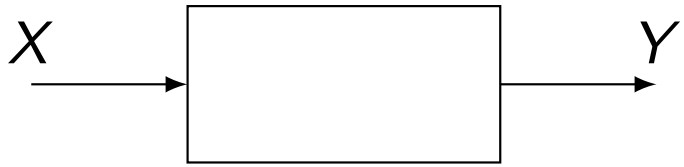
Après avoir lancé une pièce (non biaisée) 2 fois, on construit les variables aléatoires X et Y en utilisant la règle suivante:

$$X = \begin{cases} a & \text{si le nombre de face est 0} \\ b & \text{sinon} \end{cases}$$

$$Y = \begin{cases} a & \text{si le nombre de pile est 0} \\ b & \text{sinon} \end{cases}$$

Déterminez les probabilités de chaque événement
Calculez $H(X, Y)$ et $H(X|Y)$ et $I(X; Y)$.

Canal discret sans mémoire



Un canal discret sans mémoire est caractérisé par:

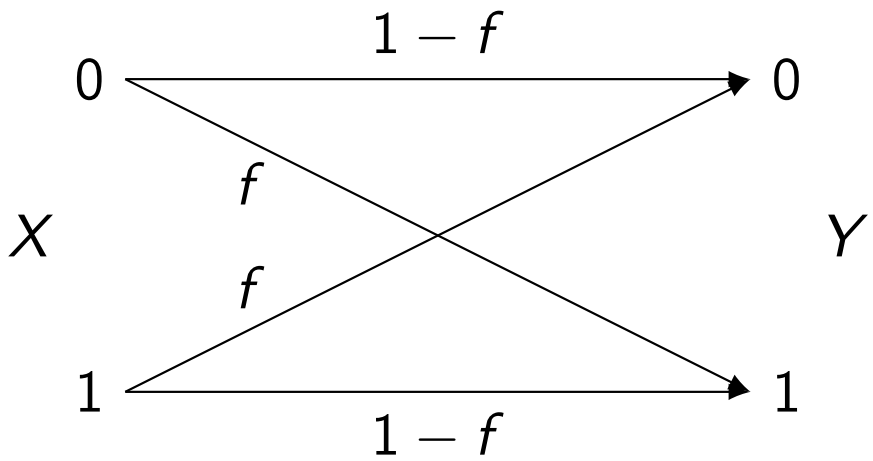
- un alphabet d'entrée $\mathcal{A}_X$
- un alphabet de sortie $\mathcal{A}_Y$
- une matrice de transition telle que:

$$Q_{j|i} = p(y = b_j | x = a_i)$$

La sortie du canal à un instant t ne dépend que de la valeur de l'entrée à ce même instant (ni avant, ni après).

Canal binaire symétrique

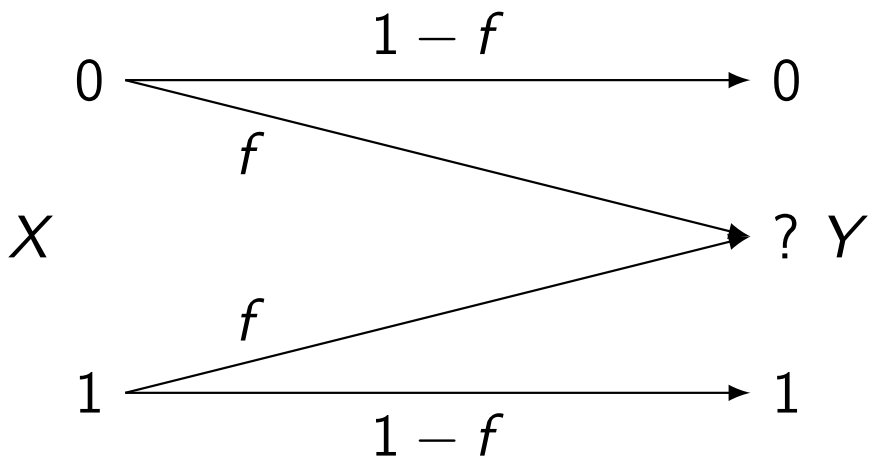
Le canal binaire symétrique transmet le symbole présent à son entrée vers sa sortie avec une probabilité $1-f$ et inverse le symbole avec une probabilité f.



$$p(y=0|x=0)=1-f \quad p(y=0|x=1)=f$$
$$p(y=1|x=0)=f \quad p(y=1|x=1)=1-f$$

Canal binaire à effacement

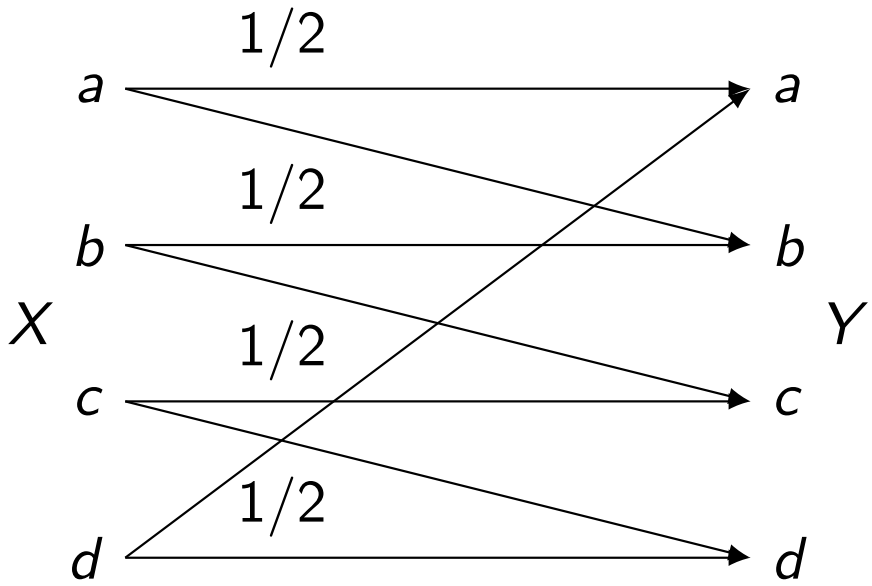
Le canal binaire à effacement transmet le symbole présent à son entrée vers sa sortie avec une probabilité $1-f$ et efface le symbole avec une probabilité f (le récepteur détecte l'effacement).



$$p(y=0|x=0)=1-f \quad p(y=0|x=1)=0$$
$$p(y=?|x=0)=f \quad p(y=?|x=1)=f$$
$$p(y=1|x=0)=0 \quad p(y=1|x=1)=1-f$$

Exercice

Soit une source X uniforme, placée à l'entrée du canal suivant:



Calculez $H(X)$, $H(Y)$, $H(Y|X)$ ainsi que $I(X;Y)$.
Trouvez un codage permettant de transmettre une information fiablement

Exercice

On considère un canal binaire symétrique avec une probabilité d'erreur $f = 0.15$.
De plus on considère une source X non-équiprobable telle que $p(X = 0) = 0.9$ et $p(X = 1) = 0.1$.

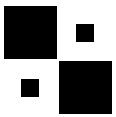
Calculez $p(y|x)$ et $p(y)$.
En déduire $H(X)$, $H(Y)$, $H(X|Y)$ et $I(X;Y)$.

Extension d'un canal

On considère maintenant le canal binaire symétrique avec $f = 0.1$ où des symboles constitués de N bits.

Extension d'un canal

On considère maintenant le canal binaire symétrique avec $f = 0.1$ où des symboles constitués de N bits.

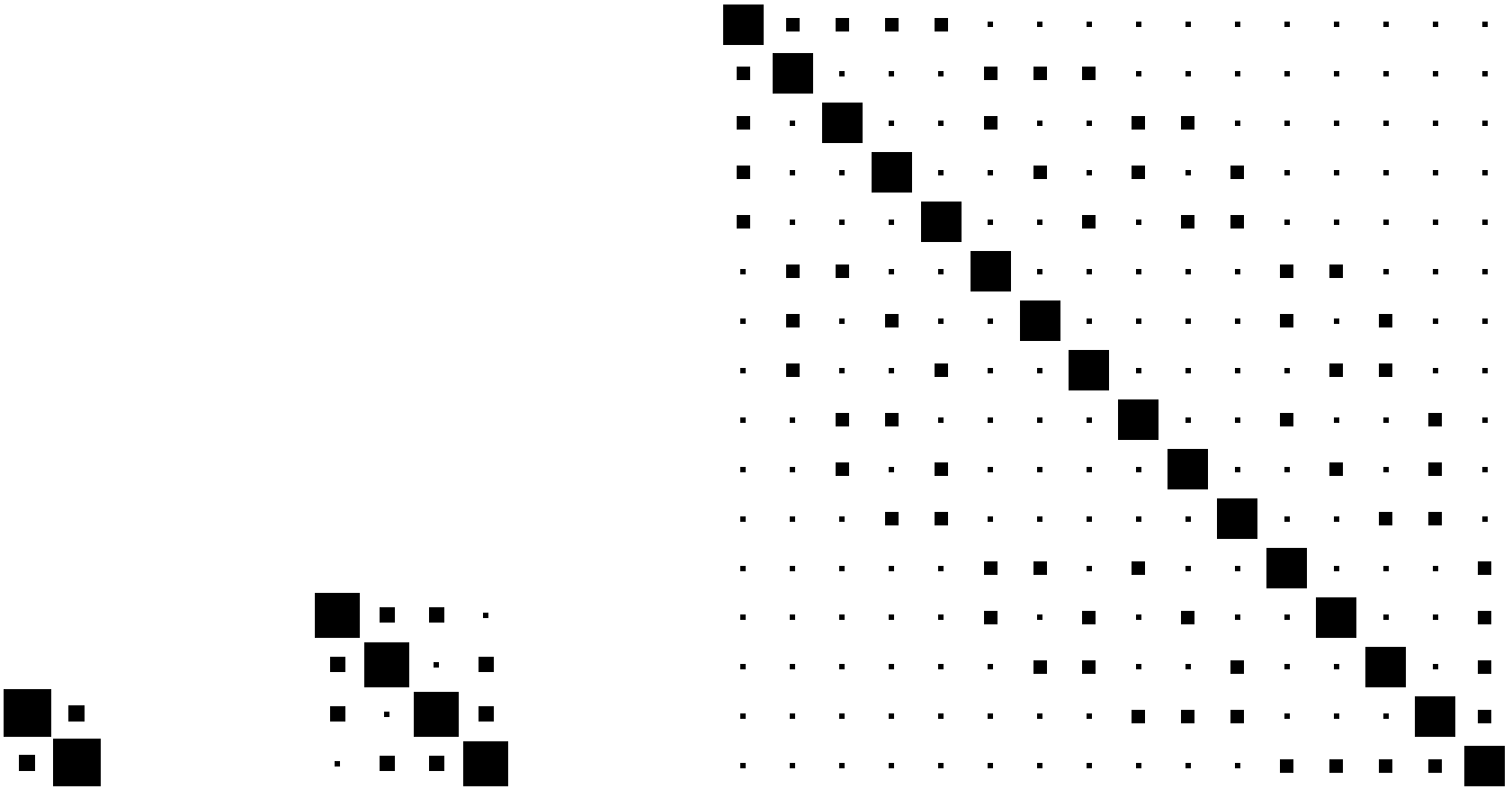


Extension d'un canal

On considère maintenant le canal binaire symétrique avec $f = 0.1$ où des symboles constitués de N bits.

Extension d'un canal

On considère maintenant le canal binaire symétrique avec $f = 0.1$ où des symboles constitués de N bits.



Capacité

La capacité d'un canal discret sans mémoire est définie par:

$$C = \max_{\mathcal{P}_X} I(X;Y) \tag{15}$$

La distribution $\mathcal{P}_X$ qui maximise l'information mutuelle est appelée la distribution d'entrée optimale, notée $\mathcal{P}_X^*$.

Pour tous les canaux symétriques, la distribution d'entrée optimale est uniforme sur tous les symboles d'entrée.

Second théorème de Shannon

Théorème du codage de canal

1. Pour tous les canaux discrets sans mémoire, il est possible de transmettre un message sans erreur tant que $R < C$ avec:

$$C = \max_{\mathcal{P}_X} I(X;Y)$$

2. si un taux d'erreur binaire p_b est acceptable, on peut transmettre

$$R(p_b) = \frac{C}{1 - H_2(p_b)}$$

3. pour tous p_b, des débits plus grands que $R(p_b)$ ne sont pas atteignables

Capacité du canal binaire symétrique

Le canal binaire symétrique peut être modélisé par $Y = X \oplus Z$ où Z est une variable aléatoire binaire de probabilité f.
Si X est connue, l'information sur Y est identique à celle de Z.
Ainsi $H(Y|X) = H(Z) = H_2(f)$
L'information mutuelle entre X et Y vaut alors:

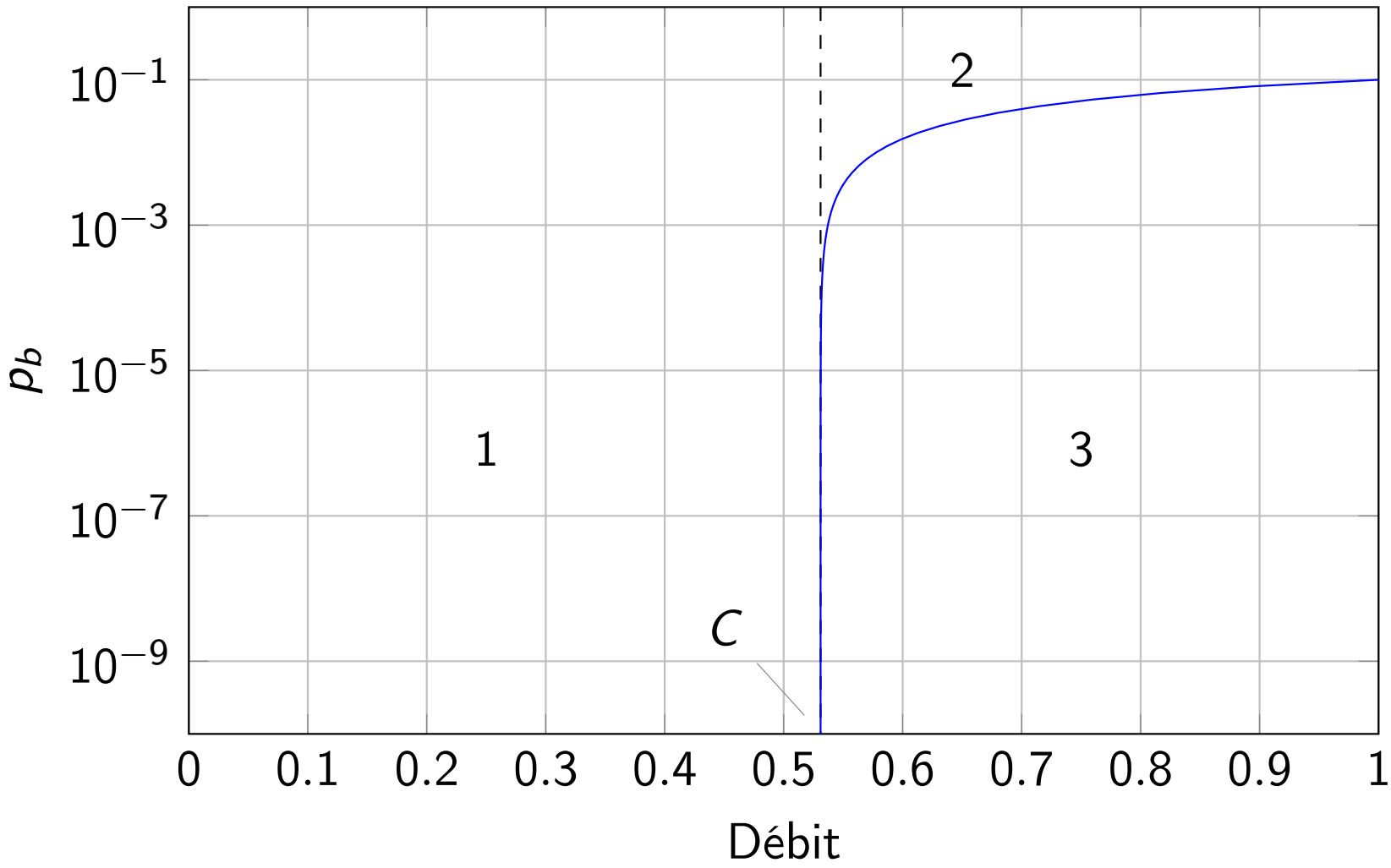
$$I(X;Y) = H(Y) - H_2(f)$$

avec $H(Y) < 1$. Par symétrie, la maximisation est obtenue pour une distribution d'entrée uniforme ($p(0) = p(1) = 0.5$) et vaut:

Capacité du BSC

$$C_{BSC} = 1 - H_2(f) \tag{16}$$

Capacité du canal binaire symétrique



Capacité du canal binaire à effacement

L'information mutuelle entre X et Y vaut:

$$I(X;Y) = H(X) - H(X|Y)$$

Par symétrie, la distribution optimale est $p(0) = p(1) = 0.5$ ce qui implique que $H(X) = H_2(0.5)$. L'entropie conditionnelle $H(X|Y)$ est $\sum_y p(y)H(X|y)$. Quand y est connu, x est incertain seulement si $y = ?$ qui arrive avec une probabilité $f/2 + f/2$ donc $H(X|Y) = f\ H_2(0.5)$.

Capacité du BEC

$$C_{BEC} = 1 - f \tag{17}$$

Cas des variables aléatoires continues

Entropie différentielle

$$H(X) = \int_{-\infty}^{+\infty} p(x) \log \frac{1}{p(x)} dx \tag{18}$$

$$H(X|Y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(x,y) \log \frac{1}{p(x|y)} dxdy \tag{19}$$

$$H(X,Y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(x,y) \log \frac{1}{p(x,y)} dxdy \tag{20}$$

Information mutuelle

$$I(X;Y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(x)p(y|x) \log \frac{p(y|x)}{p(y)} dxdy \tag{21}$$

Cas des variables aléatoires continues

Propriétés

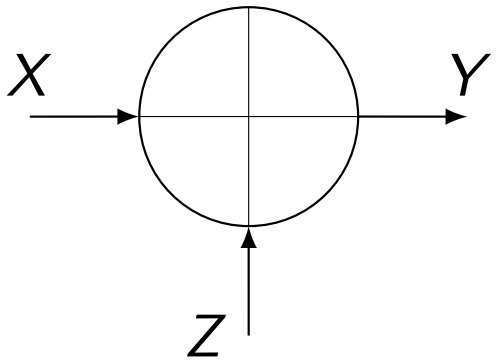
- $H(X_1, X_2 \dots X_n) \leq \sum_{i=1}^{n} H(X_i)$
- $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$

Cependant, à la différence de l'entropie "classique", l'entropie différentielle:

- n'est pas invariante par changement de variable (hors simple translation)
- peut être négative

Canal Gaussien

Le canal gaussien possède une entrée réelle X et une sortie réelle Y (le canal reste discret en temps).



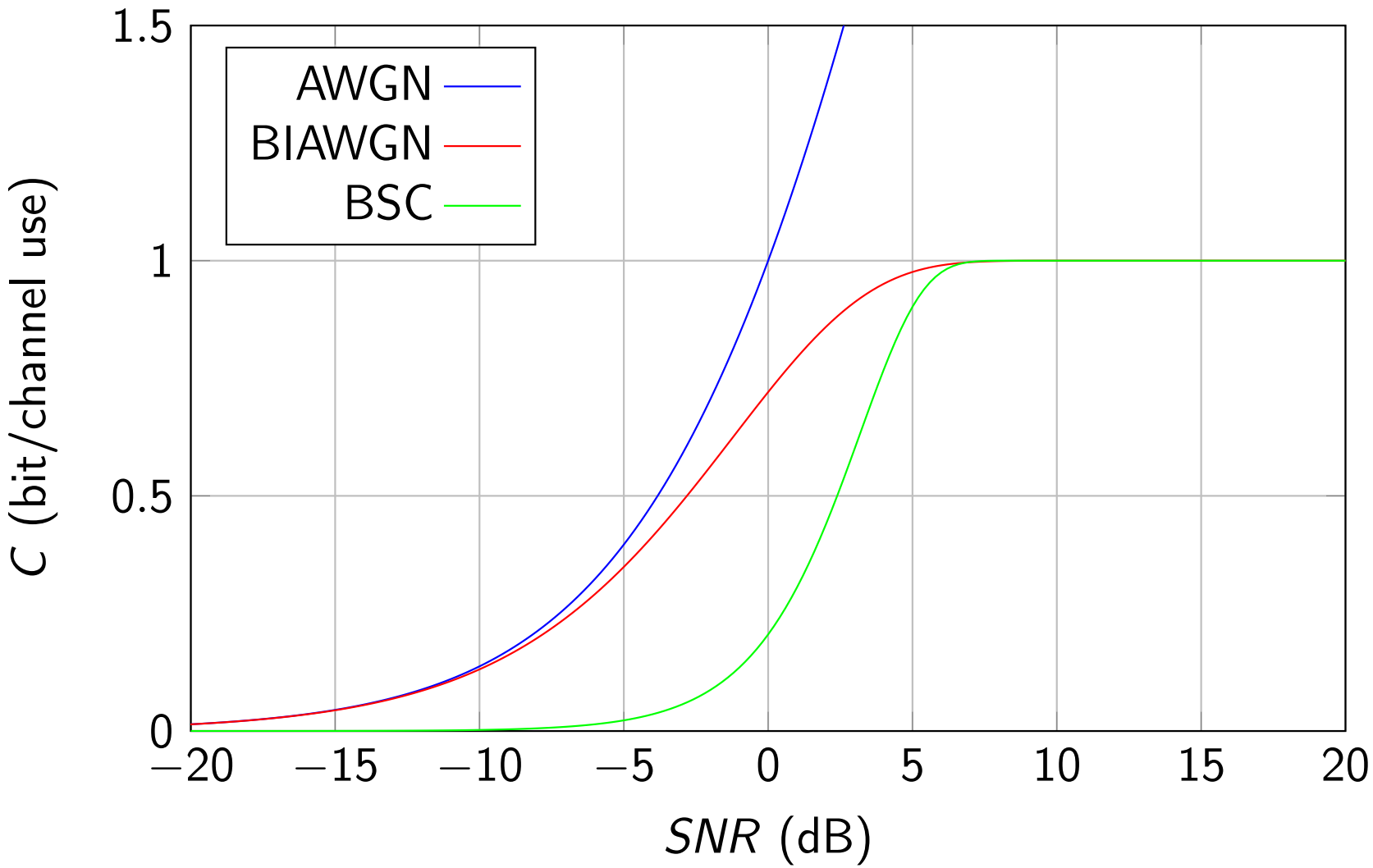
$$P(x|y) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp[-(y-x)^2/2\sigma^2]$$

Sous contrainte la $E(x^2) = v$, la capacité du canal gaussien est obtenue pour une distribution d'entrée gaussienne et vaut:

Capacité du canal AWGN

$$C_{AWGN} = \frac{1}{2} \log\left(1 + \frac{v}{\sigma^2}\right) \tag{22}$$

Canal Gaussien



Canal Gaussien à bande passante limitée

On considère maintenant un canal AWGN continu en temps de bande B et de DSP $N_0/2$. Les puissances du signal analogique et du bruit sont respectivement P et $N_0 B$.
Le théorème de l'échantillonnage impose que:

$$f_e \geq 2B$$

Pour $f_e = 2B$, il y a $2B$ échantillons par seconde. Les puissances par échantillons du signal et du bruit deviennent respectivement $P/2B$ et $N_0/2$. La capacité du canal AWGN (en bit/s) vaut alors:

Théorème de Shannon-Hartley

$$C = B \log \left(1 + \frac{P}{N_0 B}\right) \tag{23}$$

Canal gaussien à bande illimitée

$$
\begin{aligned}
C^{\infty} &= \lim_{B\to\infty} B \log_2\left(1+\frac{P}{N_0 B}\right) \\
&= \lim_{B\to\infty} \frac{BN_0P}{N_0P} \log_2\left(1+\frac{P}{N_0 B}\right) \\
&= \lim_{B\to\infty} \frac{P}{N_0} \log_2\left(1+\frac{P}{N_0 B}\right)^{\frac{BN_0}{P}}
\end{aligned}
$$

Or $\lim_{x\to\infty}(1+1/x)^x = e$ d'ou:

Capacité du canal gaussien à bande illimitée

$$C^{\infty} = \frac{P}{N_0} \log_2 e \text{ bit/s} \tag{24}$$

Efficacité spectrale

En définissant l'efficacité spectrale $r = R/B$ et pour $R < C$ on a:

$$r < \log_2(1 + \frac{P}{N_0 B})$$

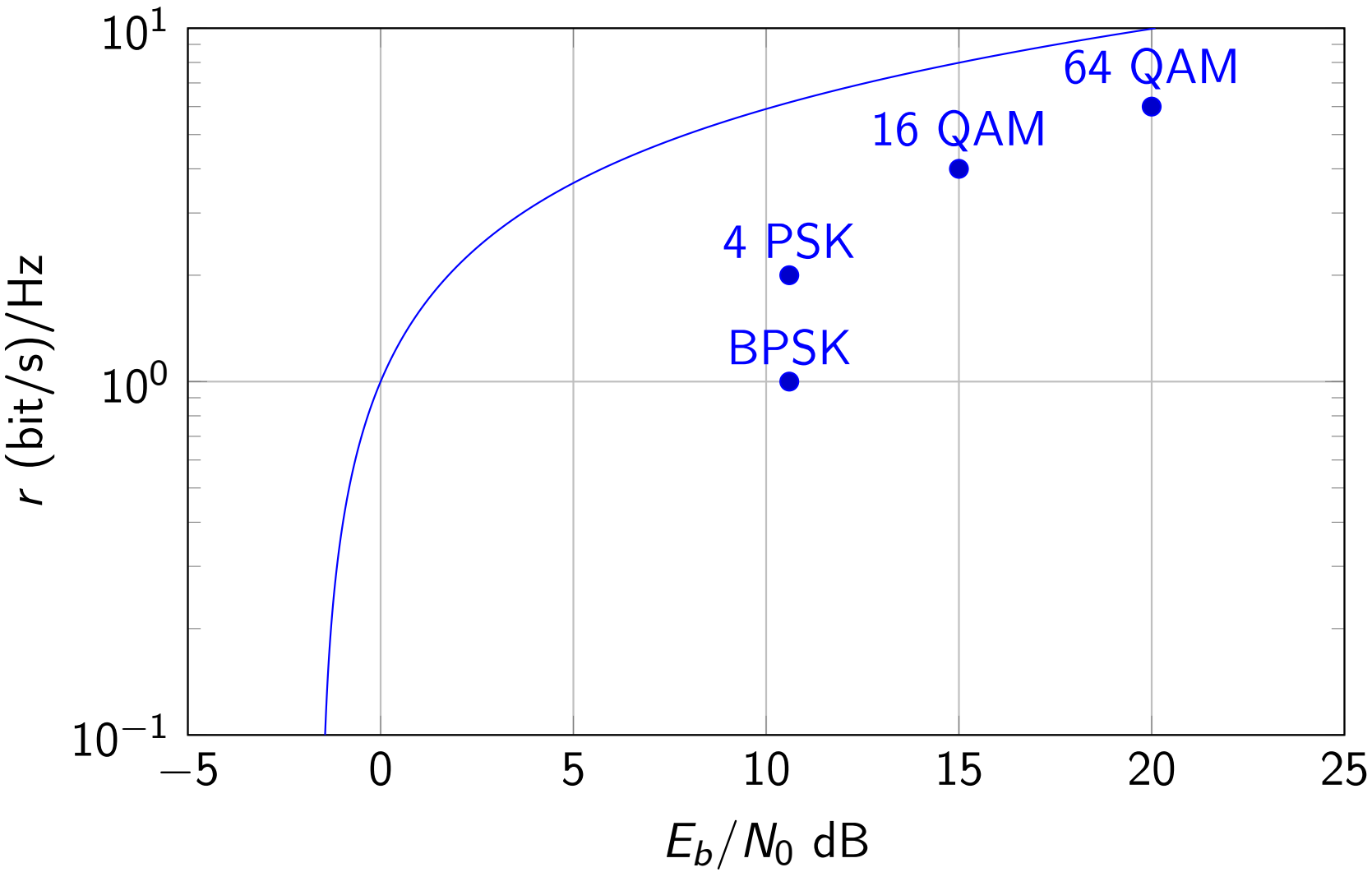
avec $P = E_b R$, on peut alors isolé le rapport E_b/N_0 en fonction de l'efficacité spectrale r:

$$\frac{E_b}{N_0} > \frac{2^r - 1}{r}$$

Pour $r \to 0$, la valeur de E_b/N_0 minimale permettant de transmettre une information de manière fiable est:

$$\frac{E_b}{N_0} > \ln 2 \approx -1.6 \text{ dB}.$$

Efficacité spectrale



Petit retour en arrière...

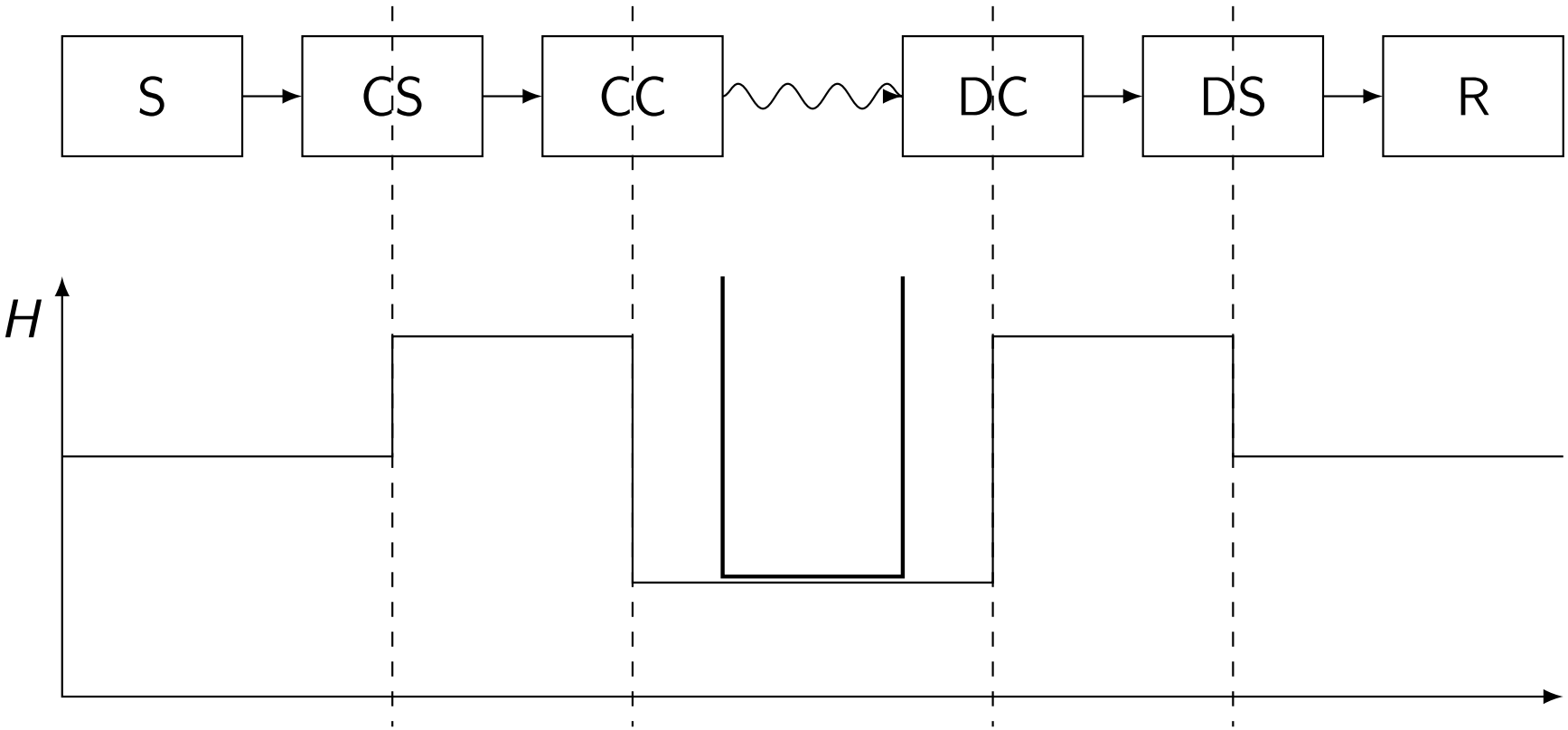
Dans l'exercice slide 30:

- Déterminez la capacité du canal
- En déduire si le codage proposé est optimal

Proposez un codage permettant de communiquer une information de manière (quasi) fiable sur:

- le canal binaire à effacement
- le canal binaire symétrique

Paradigme de Shannon



Conclusion

Shannon a posé les bases de la théorie de l'information et a déterminé les performances limites des systèmes de communication.

De plus, il a montré qu'il est possible de **séparer** les opérations de codage de source et de codage de canal (tout en garantissant l'optimalité).

Cependant, la théorie de l'information n'indique pas **comment** réaliser ces opérations.