Information Theory and Coding

Shannon's communication model

Cédric RICHARD
Université Côte d'Azur

Information Theory

Models of communication

Models of communication are conceptual models used to explain the human communication process.

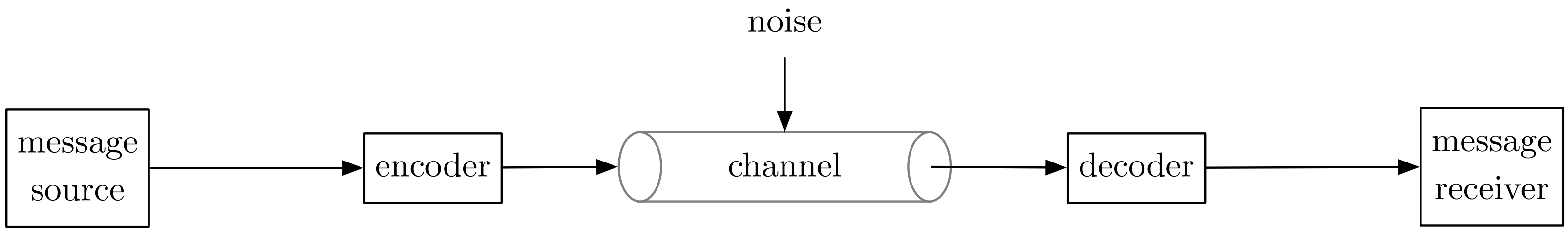
Following the basic concept, communication is the process of sending and receiving messages or transferring information from one part (sender) to another (receiver).

The Shannon-Weaver model was designed in 1949 to mirror the functioning of radio and telephone technology. It is referred to as the mother of all models.

This model has been expanded later by other scholars: Berlo (1960), ...

Information Theory

Shannon's communication model

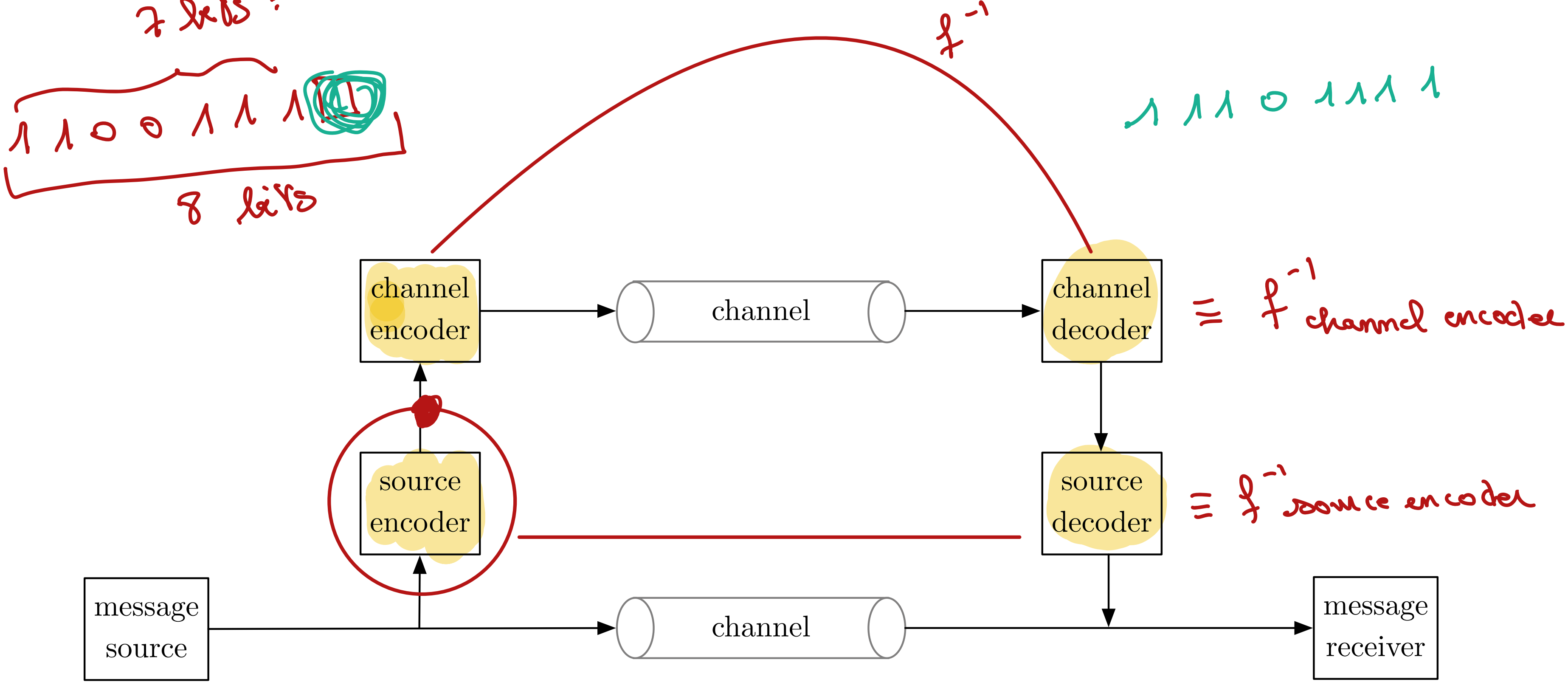


An information source, which produces a message
An encoder, which encodes the message into signals
A channel, for which signals are adapted for transmission
A decoder, which reconstructs the encoded message
An information destination, where the message arrives

Information Theory

Shannon's communication model

7 bits : information



Information Theory

Objectives

Information theory studies the quantification, storage, and communication of information.

It was originally proposed by Claude Shannon in 1948 to find fundamental limits on signal processing and communication operations such as data compression.

Applications of fundamental topics of information theory include lossless data compression, lossy data compression, and channel coding.

Information theory is used in information retrieval, intelligence gathering, gambling, statistics, and even in musical composition.

A key measure is entropy. It quantifies the amount of uncertainty involved in the value of a random variable or the outcome of a random process.

Information Theory and Coding

Quantitative measure of information

Cédric RICHARD
Université Côte d'Azur

Self-information

Information content

Let A be an event with non-zero probability $P(A)$.

The greater the uncertainty of A, the larger the information $h(A)$ provided by the realization of A. This can be expressed as follows:

$$\boxed{h(A) = f\left(\frac{1}{P(A)}\right).}$$

Function $f(\cdot)$ must satisfy the following properties:

- $f(\cdot)$ is an increasing function over $\mathbb{R}_+$
- information provided by 1 sure event is zero: $\lim_{p \to 1} f(p) = 0$
- information provided by 2 independent events: $f(p_1 \cdot p_2) = f(p_1) + f(p_2)$

This leads us to use the logarithmic function for $f(\cdot)$

A_1 and A_2 two events that are independent

ex: A_1 = " getting head with coin 1 "

A_2 = " getting head with coin 2 "

Then: $P(A_1 \text{ and } A_2) = P(A_1) \cdot P(A_2)$

def. of independance

$$P(A_1 \overset{\text{"and"}}{,} A_2) = P(A_2 \overset{\text{"given that"}}{|} A_1)\, P(A_1)$$

$$= P(A_1 | A_2)\, P(A_2)$$

with independence of A_1 and A_2 :

$$P(A_1, A_2) = P(A_1) P(A_2)$$

$$\iff \quad P(A_2 | A_1) = P(A_2)$$

$$P(A_1 | A_2) = P(A_1)$$

▷ information provided by 2 independent events: $\boxed{f(p_1 \cdot p_2) = f(p_1) + f(p_2)}$

A_1 and A_2 are indep

$$\underbrace{h(A_1, A_2)}_{\text{joint quantity of information}} \triangleq f\Big(\frac{1}{\underbrace{P(A_1, A_2)}_{\text{joint proba}}}\Big) = f\Big(\frac{1}{P(A_1)} \cdot \frac{1}{P(A_2)}\Big)$$

I want this for 2 indep. events (Shannon's axiom)

$$= f\Big(\frac{1}{P(A_1)}\Big) + f\Big(\frac{1}{P(A_2)}\Big)$$

$$= h(A_1) + h(A_2)$$

Self-information

Information content

Lemme 1. *Function* $f(p) = -\log_b p$ *is the only one that is both positive, continue over* $(0,1]$, *and that satisfies* $f(p1 \cdot p2) = f(p1) + f(p2)$.

Proof. The proof consists of the following steps:

1. $f(p^n) = n\, f(p)$
2. $f\left(p^{1/n}\right) = \frac{1}{n}\, f(p)$ after replacing p with $p^{1/n}$
3. $f\left(p^{m/n}\right) = \frac{m}{n}\, f(p)$ by combining the two previous equalities
4. $f(p^q) = q\, f(p)$ where q is any positive rational number
5. $f(p^r) = \lim_{n\to+\infty} f\left(p^{q_n}\right) = \lim_{n\to+\infty} q_n\, f(p) = r\, f(p)$ because rationals are dense in the reals

Let p and q in $(0,1[$. One can write: $p = q^{\log_q p}$, which yields:

$$f(p) = f\left(q^{\log_q p}\right) = f(q)\,\log_q p.$$

We finally arrive at: $\boxed{f(p) = -\log_b p}$

$$f(p) = -\log_b p$$

$$\log_b x = \frac{\ln x}{\ln b}$$

basis of log

$b > 0$

2. $$f\left(p^{1/n}\right) = \frac{1}{n} f(p)$$

$$f(p) = f\left(\left(p^{1/n}\right)^n\right) \overset{1.}{=} n\, f\left(p^{1/n}\right)$$

$$\Rightarrow f\left(p^{1/n}\right) = \frac{1}{n} f(p) \qquad \underline{\underline{2.}}$$

3. $$f\left(p^{m/n}\right) = \frac{m}{n} f(p)$$

$$f\left(p^{m/n}\right) = f\left(\left(p^{1/n}\right)^m\right)$$

$$\overset{1.}{=} m\, f\left(p^{1/n}\right)$$

$$\overset{2.}{=} \frac{m}{n} f(p)$$

$$p = q^{\log_q p} = \underbrace{\frac{\overset{<0}{\ln p}}{\underset{<0}{\ln q}}}_{>0}$$

$$q^{\log_q p} \overset{a}{=} q^{\frac{\ln p}{\ln q}} \overset{ⓐ\,\&\,ⓑ}{=} e^{\frac{\ln p}{\ln q} \times \ln q}$$

$$= e^{\ln p}$$

ⓑ $q = e^{\ln q}$

$$= p$$

ⓐ $e^{ab} = (e^{a})^{b}$

we have : $p = q^{\log_q p}$, $p, q \in]0,1]$

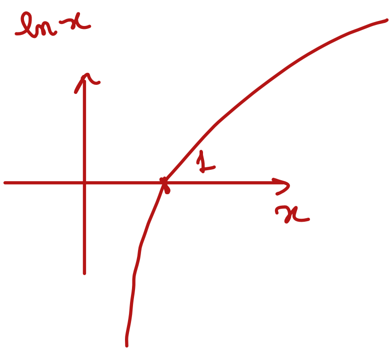
$$f(p) = f(q^{\log_q p}) = \log_q p \times f(q)$$

$$= \frac{\ln p}{\ln q} \times f(q)$$

$$\Longrightarrow \frac{f(p)}{f(q)} = \frac{\ln p}{\ln q} \Longrightarrow \underbrace{f(p)}_{} = K \underbrace{\ln p}_{<0}$$

$\forall p, q \in]0,1]$

I want it positive



$\Longrightarrow \quad K < 0$

I can write $K = -\dfrac{1}{\ln b}$ with $b > 1$

$$f(p) = -\frac{\ln p}{\ln b} \quad , \quad b > 1$$

$$\stackrel{\Delta}{=} -\log_b p \quad , \quad b > 1$$

Check : $\lim\limits_{p \to 1} -\log_b p = 0$

Self-information

Information content

Definition 1. *Let $(\Omega, \mathcal{A}, P)$ be a probability space, and A an event of $\mathcal{A}$ with non-zero probability $P(A)$. The information content of A is defined as:*

$$h(A) = -\log_b P(A). \quad , \; b > 1$$

Unit. The unit of $h(A)$ depends on the base chosen for the logarithm.

- $b = 2$ ▷ $\log_2$: Shannon, bit (binary unit)
- $b = e^1$ ▷ $\log_e$: logon, nat (natural unit) $\ln$
- $b = 10$ ▷ $\log_{10}$: Hartley, decit (decimal unit)

Vocabulary. $h(\cdot)$ represents the *uncertainty* of A, or its *information content.*

$\log_2 x$ Shannon

8 , 16

2048

if $x = 2^n$

$$\log_2 x = \log_2 2^n$$

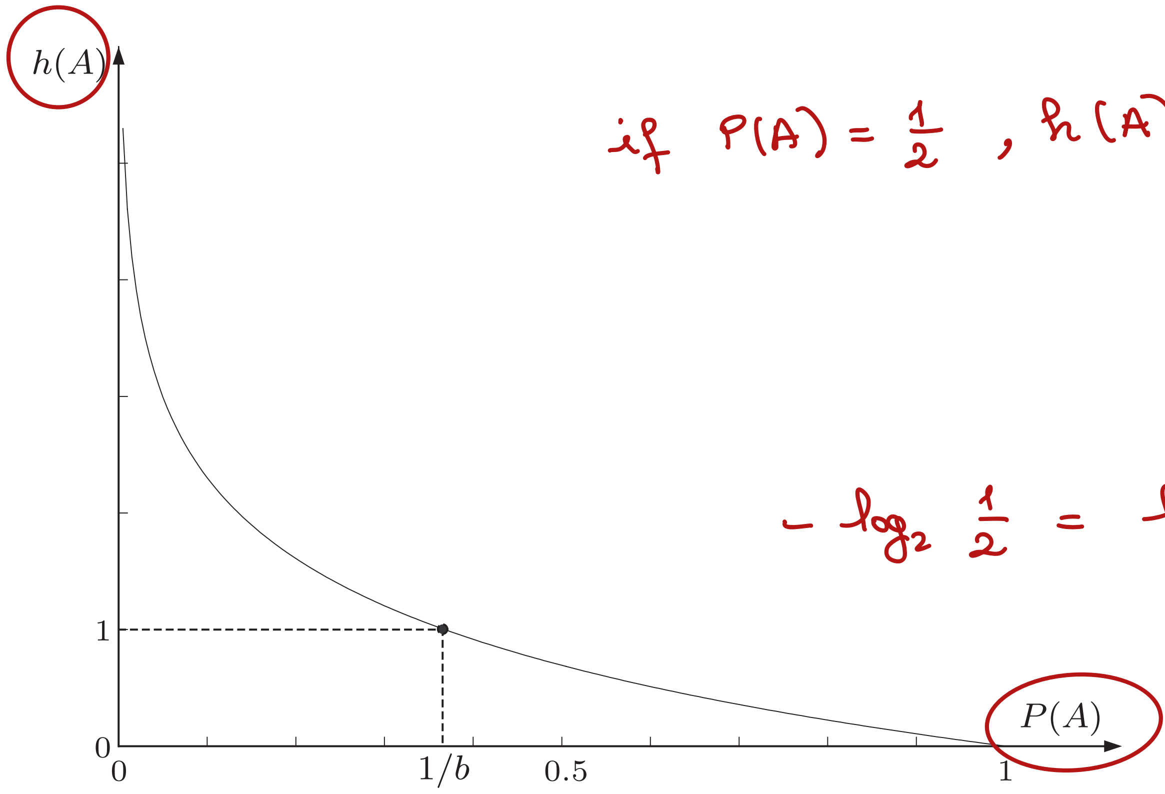
$$= \frac{\ln 2^n}{\ln 2}$$

$$= n \frac{\ln 2}{\cancel{\ln 2}}$$

Self-information

Information content

Information content or uncertainty: $h(A) = -\log_b P(A)$



if $P(A) = \frac{1}{2}$, $h(A) = -\log_2 \frac{1}{2}$

$= 1$ Sh

$-\log_2 \frac{1}{2} = \log_2 2^1 = 1$

if $b=2$

Self-information

Information content

Example 1. Consider a binary source $S \in \{0, 1\}$ with $P(0) = P(1) = 0.5$. Information content conveyed by each binary symbol is equal to: $h\left(\frac{1}{2}\right) = \log 2$, namely, 1 bit or Shannon.

Example 2. Consider a source S that randomly selects symbols s_i among 16 equally likely symbols $\{s_0, \ldots, s_{15}\}$. Information content conveyed by each symbol is $\log 16$ Shannon, that is, 4 Shannon.

Remark. The bit in Computer Science (*binary digit*) and the bit in Information Theory (*binary unit*) do not refer to the same concept.

Example 2. Consider a source S that randomly selects symbols s_i among 16 equally likely symbols $\{s_0, \ldots, s_{15}\}$. Information content conveyed by each symbol is $\log 16$ Shannon, that is, 4 Shannon.

$$P(S = s_i) = \frac{1}{16}$$

$$h(\underbrace{S = s_i}_{A\,:\,\text{" S generates } s_i \text{"}}) = -\log_2 \frac{1}{16} = \log_2 2^4 = 4\ \text{Sh}$$

(bit)

Self-information

Conditional information content

Self-information applies to 2 events A and B. Note that $P(A, B) = P(A)\,P(B|A)$. We get:

$$h(A, B) = -\log P(A, B) = -\log P(A) - \log P(B|A)$$

Note that $-\log P(B|A)$ is the information content of B that is not provided by A.

Definition 2. *Conditional information content of B given A is defined as:*

$$h(B|A) = -\log P(B|A),$$

that is: $h(B|A) = h(A, B) - h(A)$.

Exercise. Analyze and interpret the following cases: $A \subset B$, $A = B$, $A \cap B = \emptyset$.

A : with $P(A)$

$$h(A) = -\log_2 P(A) \qquad \text{Sh}$$

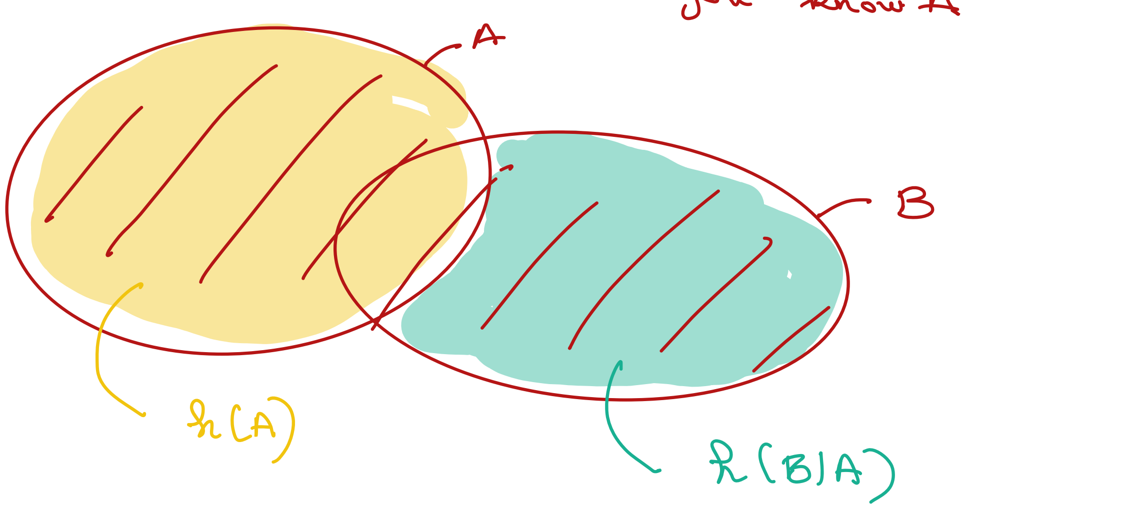
A, B : with $P(A,B)$ joint proba.

$$h(A,B) = -\log_2 P(A,B) \qquad \text{Sh}$$

extension : $P(A,B) = P(A)\,P(B \mid A)$

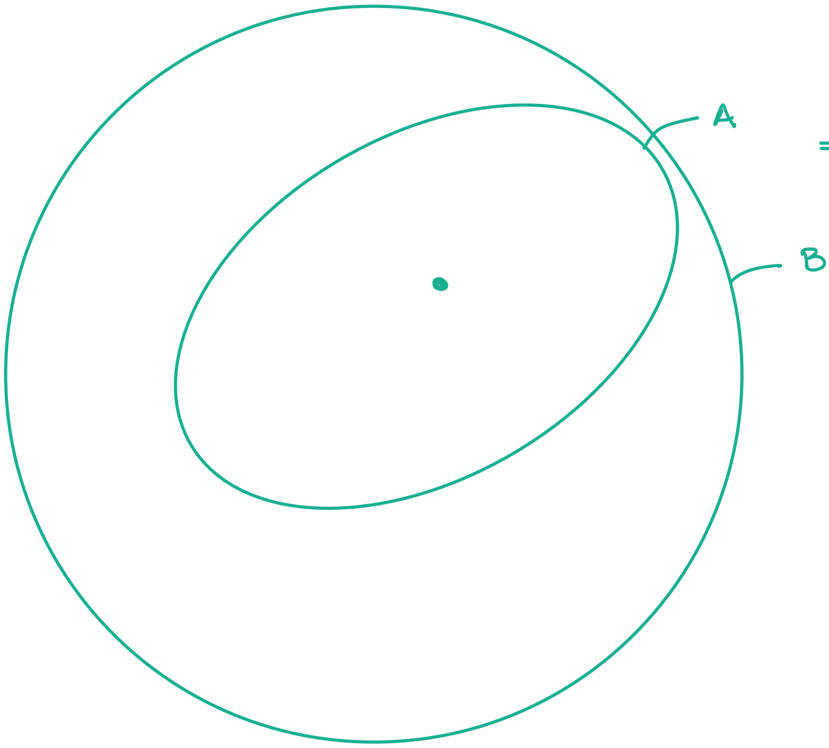
$$\begin{aligned} h(A,B) &= -\log_2 P(A,B) \\ &= -\log_2 \left[P(A)\,P(B \mid A)\right] \\ &= -\log_2 P(A) - \log_2 P(B \mid A) \\ &\triangleq \underbrace{h(A)}_{\text{Sh}} + \underbrace{h(B \mid A)}_{\text{Sh}} \end{aligned}$$

→ quantity of info provided by B given that you know A



Exercise. Analyze and interpret the following cases: $A \subset B$, $A = B$, $A \cap B = \emptyset$.

$\boxed{A \subset B}$



$A \subset B$

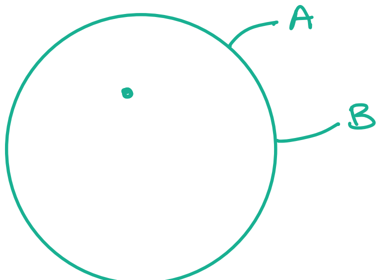
$\Rightarrow P(B|A) = 1$

$$h(A,B) = h(A) + h(B|A)$$

$$h(B|A) = -\log_2 P(B|A) = 0$$

$$\Rightarrow h(A,B) = h(A)$$

$\boxed{A = B}$



$P(A|B) = P(B|A) = 1$

$h(A,B) = h(A) = h(B)$

independent

$\boxed{A \cap B = \emptyset}$

$$P(A,B) = P(A)P(B)$$

$$\Rightarrow h(A,B) = h(A) + h(B)$$

because $P(A|B) = P(A)$
$P(B|A) = P(B)$

Self-information

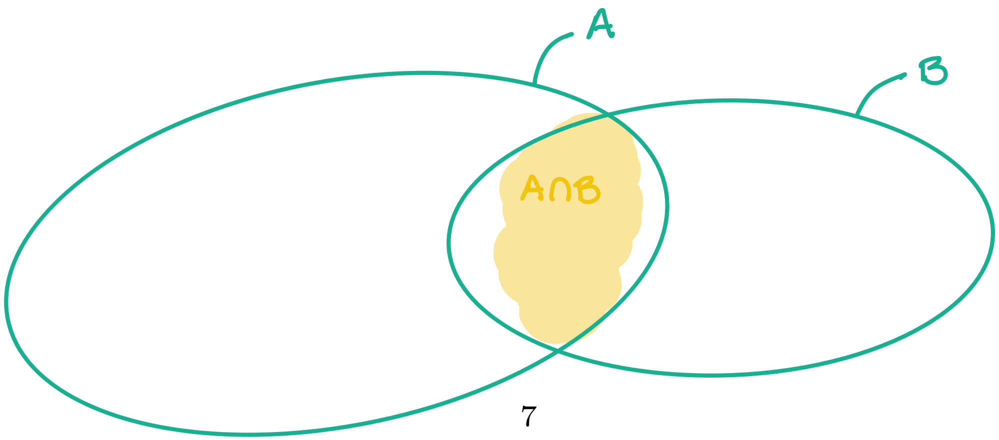
Mutual information content

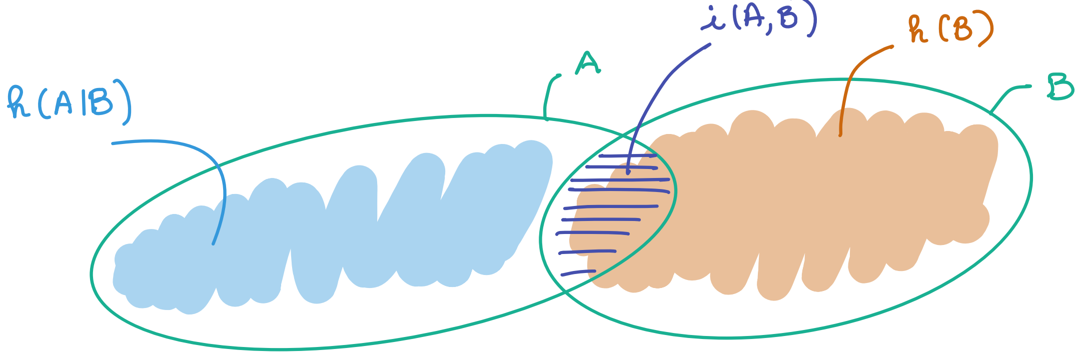
The definition of conditional information leads directly to another definition, that of mutual information, which measures information shared by two events.

Definition 3. *We call mutual information of A and B the following quantity:*

$$\boxed{i(A,B) = h(A) - h(A|B) = h(B) - h(B|A).}$$

Exercise. Analyze and interpret the following cases: $A \subset B$, $A = B$, $A \cap B = \emptyset$.



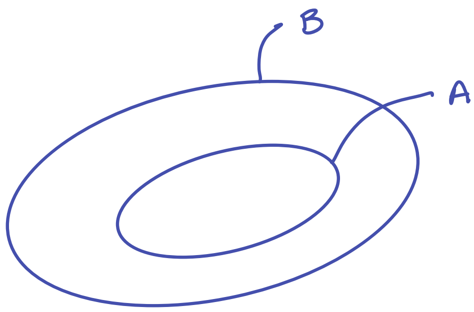


$$h(A) - h(A|B) \triangleq \underbrace{i(A,B)}_{} \triangleq h(B) - h(B|A)$$

↳ mutual information

" shared information "

Exercise. Analyze and interpret the following cases: $A \subset B$, $A = B$, $A \cap B = \emptyset$.



$P(B|A) = 1$

$h(B|A) = 0$

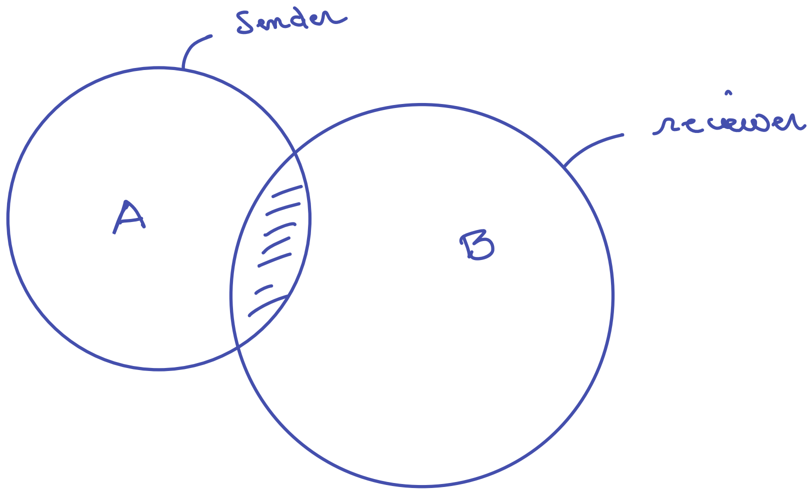
$i(A,B) = h(B)$

$\boxed{A = B}$ $\quad i(A,B) = h(A) = h(B)$

independent.

$\boxed{\cancel{A \cap B = \emptyset}}$

$h(A|B) = h(A) \Rightarrow i(A,B) = 0$



good telecommunication : max $i(S, R)$

Entropy of a random variable

Definition

Consider a memoryless stochastic source S with alphabet $\{s_1, \ldots, s_n\}$. Let p_i be the probability $P(S = s_i)$.

The entropy of S is the average amount of information produced by S:

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

Definition 4. *Let X be a random variable that takes its values in $\{x_1, \ldots, x_n\}$. Entropy of X is defined as follows:*

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

$$S = \{ s_1 , \dots , s_n \}$$ event, state, character

$$P(S = s_1) = p_1 \Rightarrow h(S = s_1) = -\log p_1 \text{ Sh}$$

$(\dots)$

$$P(S = s_n) = p_n \Rightarrow h(S = s_n) = -\log p_n \text{ Sh}$$

$$\underbrace{H(S)}_{\text{entropie}} = \sum_{i=1}^{n} p_i \, h(S = s_i) \quad \leftarrow \text{mean value } E\{\cdot\}$$

entropie $\rightarrow$ Sh / event or state or character.

$$H(S) = \sum_{i=1}^{n} -p_i \log_2 p_i \quad \text{Sh / event}$$

$$\boxed{H(S) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad \text{Sh / event / state}}$$

Alphabetical source : $a, b, c, \dots, z$
$\hookrightarrow P(S = a) = \dots$

$p \log p$ with $p = 1 \longrightarrow 0$

$p \log p$ with $p \to 0 \longrightarrow 0$

$$\boxed{\begin{array}{l} \text{if : } P(S = s_i) = 1 \\ \text{and } P(S = s_j) = 0 , \quad \forall j \neq i \\ \Longrightarrow H(S) = 0 \end{array}}$$

Entropy of a random variable

Example of a binary random variable

The entropy of a binary random variable is given by:

$$H(X) = -p \log p - (1-p)\log(1-p) \triangleq H_2(p).$$

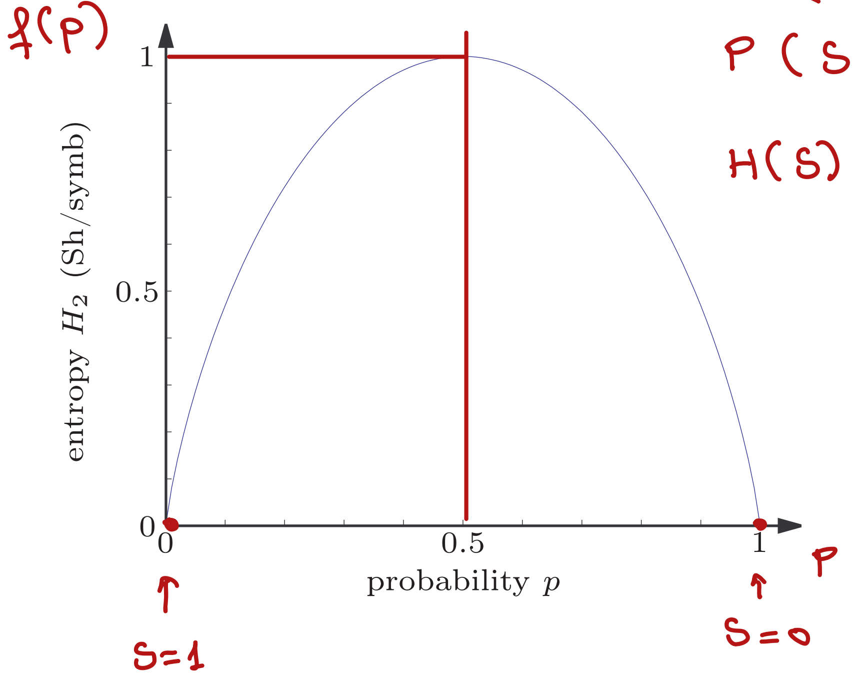
$H_2(p)$ is called the binary entropy function.

$P(S=0) = p$

$P(S=1) = 1-p$

$H(S) = -p \log_2 p - (1-p)\log_2(1-p)$

$= f(p)$



$$H(S) = 2 \times \left[-\frac{1}{2} \log \frac{1}{2} \right]$$

$$= 2 \times \frac{1}{2}$$

$$= 1 \quad \text{Sh} \; / \text{state} .$$

Entropy of a random variable

Notation and preliminary properties

Lemme 2 (Gibbs' inequality)**.** *Consider 2 discrete probability distributions with mass functions* $(p_1, \dots, p_n)$ *and* $(q_1, \dots, q_n)$*. We have:*

$\sum_i p_i = 1 \quad , \quad p_i \geq 0 \quad \forall i$

$\sum_i q_i = 1 \quad , \quad q_i \geq 0 \quad \forall i$

$$\sum_{i=1}^{n} p_i \log \frac{q_i}{p_i} \leq 0$$

Equality is achieved when $p_i = q_i$ *for all* i

Proof. The proof is carried out in the case of the neperian logarithm. Observe that $\ln x \leq x - 1$, with equality for $x = 1$. Let $x = \frac{q_i}{p_i}$. We have:

$$\sum_{i=1}^{n} p_i \ln \frac{q_i}{p_i} \leq \sum_{i=1}^{n} p_i \left(\frac{q_i}{p_i} - 1 \right) = 1 - 1 = 0.$$

We have : $\ln x \leq x - 1 \quad , \forall x > 0$

$q_i / p_i > 0$

$$\sum_{i=1}^{n} p_i \log \frac{q_i}{p_i} \leq 0$$

$$\sum_{i=1}^{n} p_i \log \overbrace{\frac{q_i}{p_i}}^{x} \leq \underbrace{\sum_{i=1}^{n} p_i \times \overbrace{\left(\frac{q_i}{p_i} - 1 \right)}^{x-1}}$$

$$\sum_{i=1}^{n} (q_i - p_i) = \sum_{i=1}^{n} q_i - \sum_{i=1}^{n} p_i = 1 - 1 = 0$$

if $p_i = q_i \quad , \forall i$

$$\Rightarrow \sum_i p_i \log \frac{q_i}{p_i} = 0$$

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

$$\sum_{i=1}^{n} p_i \log \frac{q_i}{p_i} \leq 0$$

$$\Rightarrow \sum_{i=1}^{n} \left[p_i \log q_i - p_i \log p_i \right] \leq 0$$

$$\Rightarrow \underbrace{- \sum_{i=1}^{n} p_i \log p_i}_{H(S)} + \sum_{i=1}^{n} p_i \log q_i \leq 0$$

We set $q_i = \frac{1}{n}$

$$H(S) - \log_2 n \underbrace{\sum_{i=1}^{n} p_i}_{1} \leq 0$$

$$\Rightarrow \boxed{H(S) \leq \log_2 n}$$

2 states : $n = 2$

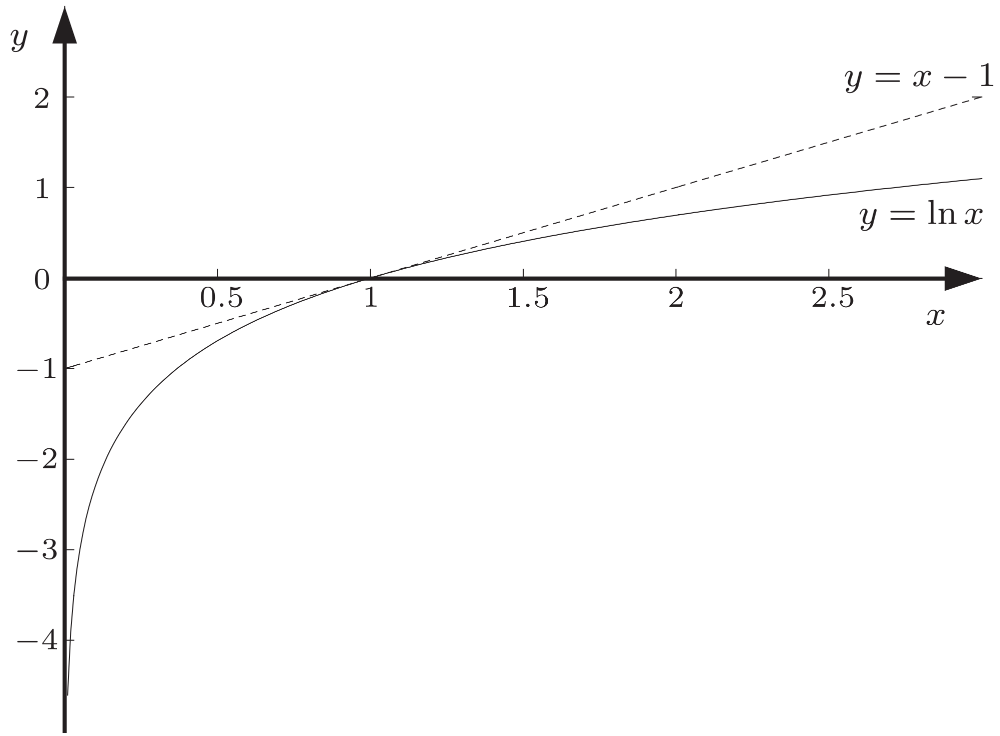
$H(S) \leq 1$ Sh

(see before)

$$H(S) = \log_2 n$$

if $p_i = q_i = \frac{1}{n}$, $\forall i = 1, \dots, n$

Graphical checking of inequality $\ln x \leq x - 1$



Entropy of a random variable

Properties

Property 1. *The entropy satisfies the following inequality:*

$$H_n(p_1, \ldots, p_n) \leq \log n,$$

Equality is achieved by the uniform distribution, that is, $p_i = \frac{1}{n}$ *for all* i*.*

Proof. Based on Gibbs' inequality, we set $q_i = \frac{1}{n}$.

Uncertainty about the outcome of an experiment is maximum when all possible outcomes are equiprobable.

Entropy of a random variable

Properties

Property 2. *The entropy increases as the number of possible outcomes increases.*

Proof. Let X be a discrete random variable with values in $\{x_1, \ldots, x_n\}$ and probabilities $(p_1, \ldots, p_n)$, respectively. Consider that state x_k is split into two substates x_{k_1} et x_{k_2}, with non-zero probabilities p_{k_1} et p_{k_2} such that $p_k = p_{k_1} + p_{k_2}$.

Entropy of the resulting random variable X' is given by:

$$\begin{aligned} H(X') &= H(X) + p_k \log p_k - p_{k_1} \log p_{k_1} - p_{k_2} \log p_{k_2} \\ &= H(X) + p_{k_1}(\log p_k - \log p_{k_1}) + p_{k_2}(\log p_k - \log p_{k_2}). \end{aligned}$$

The logarithmic function being strictly increasing, we have: $\log p_k > \log p_{k_i}$. This implies: $H(X') > H(X)$.

Interpretation. Second law of thermodynamics

Entropy of a random variable

Properties

Property 3. *The entropy H_n is a concave function of $p_1, \ldots, p_n$.*

Proof. Consider 2 discrete probability distributions $(p_1, \ldots, p_n)$ and $(q_1, \ldots, q_n)$. We need to prove that, for every λ in $[0, 1]$, we have:

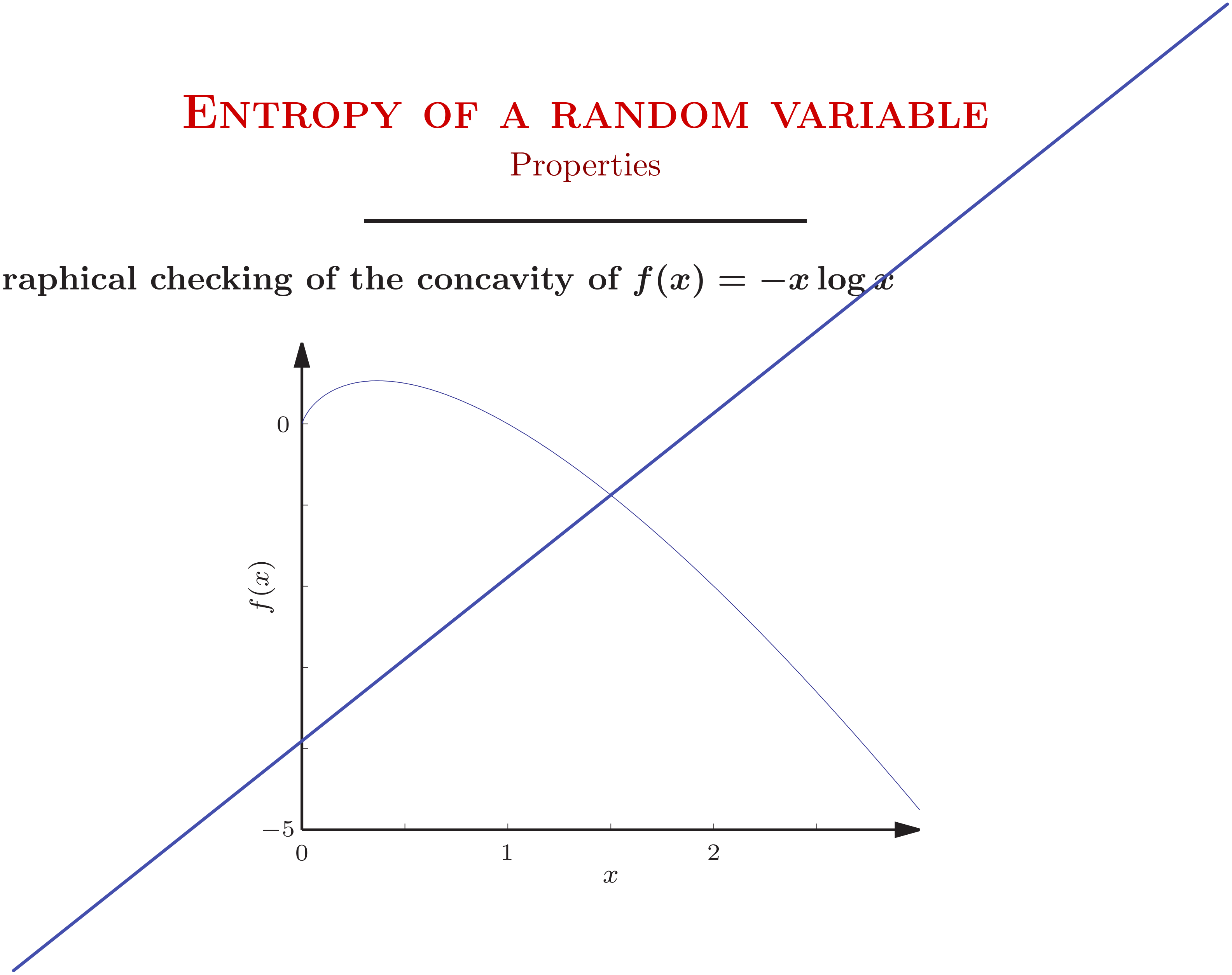
$$H_n(\lambda p_1 + (1-\lambda)q_1, \ldots, \lambda p_n + (1-\lambda)q_n) \geq \lambda H_n(p_1, \ldots, p_n) + (1-\lambda)H_n(q_1, \ldots, q_n).$$

By setting $f(x) = -x \log x$, we can write:

$$H_n(\lambda p_1 + (1-\lambda)q_1, \ldots, \lambda p_n + (1-\lambda)q_n) = \sum_{i=1}^{n} f(\lambda p_i + (1-\lambda)q_i).$$

The result is a direct consequence of the concavity of $f(\cdot)$ and Jensen's inequality.

Graphical checking of the concavity of $f(x) = -x \log x$



Entropy of a random variable

Properties

Concavity of H_n can be generalized to any number m of distributions.

Property 4. *Given* $\{(q_{1j}, \ldots, q_{nj})\}_{j=1}^{m}$ *a finite set of discrete probability distributions, the following inequality is satisfied:*

$$H_n(\sum_{j=1}^{m} \lambda_j \, q_{1j}, \ldots, \sum_{j=1}^{m} \lambda_j \, q_{mj}) \geq \sum_{j=1}^{m} \lambda_j \, H_n(q_{1j}, \ldots, q_{mj}),$$

where $\{\lambda_j\}_{j=1}^{m}$ *is any set of constants in* $[0, 1]$ *such that* $\sum_{j=1}^{m} \lambda_j = 1$*.*

Proof. As in the previous case, the demonstration of this inequality is based on the concavity of $f(x) = -x \log x$ and Jensen's inequality.

Pair of random variables

Joint entropy

Definition 5. *Let X and Y be two random variables with values in $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$, respectively. The joint entropy of X and Y is defined as:*

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

▷ The joint entropy is symmetric: $\underline{H(X,Y) = H(Y,X)}$ car $\mathbb{P}(X,Y) = \mathbb{P}(Y,X)$

Example. Case of two independent random variables

X	Y
x_1	y_1
$\vdots$	$\vdots$
x_n	$\vdots$
	y_m

$Z = (X, Y)$	
$x_1 \; y_1$	
$x_1 \; y_2$	
$\vdots$	
$x_1 \; y_m$	
$\vdots$	
$x_n \; y_m$	

$z_{ij} = (x_i, y_j)$

$n\,m$ states

$P(X = x_i, Y = y_j)$

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

$$= - \sum_{i=1}^{i=n} \sum_{j=1}^{m} P(Z = z_{ij}) \log_2 P(Z = z_{ij})$$

$$= - \sum_{i} \sum_{j} P(X = x_i, Y = y_j) \log_2 P(X = x_i, Y = y_j)$$

Sh / pair of states of X and Y

$$H(X,Y) \leq \overbrace{\log_2 (n.m)}^{\log_2 n + \log_2 m}$$

if X and Y indep. $H(X,Y) = \underset{\log n}{\underset{\wedge}{H(X)}} + \underset{\log m}{\underset{\wedge}{H(Y)}}$

Pair of random variables

Conditional entropy

Definition 6. *Let X and Y be two random variables with values in $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$, respectively. The conditional entropy of X given $Y = y_j$ is:*

$$H(X|Y = y_j) \triangleq -\sum_{i=1}^{n} P(X = x_i|Y = y_j) \log P(X = x_i|Y = y_j).$$

$H(X|Y = y_j)$ is the amount of information needed to describe the outcome of X given that we know that $Y = y_j$.

Definition 7. *The conditional entropy of X given Y is defined as:*

$$H(X|Y) \triangleq \sum_{j=1}^{m} P(Y = y_j)\, H(X|Y = y_j),$$

Example. Case of two independent random variables

$H(X \mid Y = y_j) \longrightarrow$ X : system

Y : fixed to y_j $\Big\} \to$ single system $X \mid Y = y_j$

$$H(X \mid Y = y_j) \triangleq - \sum_{i=1}^{n} P(X = x_i \mid Y = y_j) \log_2 P(X = x_i \mid Y = y_j)$$

Sh / state of X

fixed

<u>Rm</u> : $H(X \mid Y = y_j) \leq \log_2 n$

$$H(X \mid Y) \triangleq \underbrace{\sum_{j=1}^{m} P(Y = y_j) \overbrace{H(X \mid Y = y_j)}}_{\text{mean value over all } y_j}$$

$$\triangleq E_Y \, H(X \mid Y = y)$$

⚠ $H(X \mid Y) \neq H(Y \mid X)$

$$H(X|Y) \triangleq \sum_{j=1}^{m} P(Y = y_j)\, H(X|Y = y_j),$$

Example. Case of two independent random variables

X and Y independent

$$H(X|Y=y_j) = H(X)$$

because $P(X=x_i|Y=y_j) = P(X=x_i)$

$$\Rightarrow H(X|Y) = \sum_{j=1}^{m} P(Y=y_j)\, H(X)$$

$$= H(X) \underbrace{\sum_{j=1}^{m} P(Y=y_j)}_{1}$$

$$= H(X)$$

Pair of random variables

Relations between entropies

$$\boxed{H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y).}$$

These equalities can be obtained by first writing:

$$\log P(X = x, Y = y) = \log P(X = x|Y = y) + \log P(Y = y),$$

and then taking the expectation of each member.

Property 5 (chain rule)**.** *The joint entropy of n random variables can be evaluated using the following chain rule:*

$$H(X_1, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_1 \ldots X_{i-1}).$$

$$P(X=x_i, Y=y_j) = P(X=x_i)\, P(Y=y_j \mid X=x_i)$$

$- \log$

$$\underbrace{-\log P(X=x_i, Y=y_j)}_{h(X=x_i,\, Y=y_j)} = \underbrace{-\log P(X=x_i)}_{h(X=x_i)} \underbrace{- \log P(Y=y_j \mid X=x_i)}_{h(Y=y_j \mid X=x_i)}$$

$E_{xy}\{\cdot\}$

<u>Rm</u> : $h(A,B) = h(A) + h(B \mid A)$

$$A = (X = x_i)$$

$$B = (Y = y_j)$$

$$H(X) = E_x\{h(X=x)\}$$

$$H(X,Y) = E_{x,y}\{h(X=x, Y=y)\}$$

$$H(X,Y) = E_{xy}\{h(X=x)\} + E_{xy}\{h(Y=y \mid X=x)\}$$

$$= E_y\{E_x\{h(X=x)\}\} + E_y\{E_x\{h(Y=y \mid X=x)\}\}$$

$$= E_y\{H(X)\} + E_x\{H(Y \mid X=x)\}$$

$$= H(X) + H(Y \mid X)$$

$$\boxed{H(X,Y) = H(X) + H(Y \mid X)}$$

Pair of random variables

Relations between entropies

Each term of $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$ is positive. We can conclude that:

$$\boxed{\begin{aligned} H(X) &\leq H(X,Y) \\ H(Y) &\leq H(X,Y) \end{aligned}}$$

$$\underbrace{H(X,Y)}_{\geq 0} = \underbrace{H(X)}_{\geq 0} + \underbrace{H(Y|X)}_{\geq 0} \Rightarrow \boxed{\begin{aligned} H(X,Y) &\geq H(X) \\ H(X,Y) &\geq H(Y|X) \end{aligned}}$$

Pair of random variables

Relations between entropies

From the *generalized concavity* of the entropy, setting $q_{ij} = P(X = x_i|Y = y_j)$ and $\lambda_j = P(Y = y_j)$, we get the following inequality:

$$\boxed{H(X|Y) \leq H(X)}$$

Conditioning a random variable reduces its entropy. Without proof, this can be generalized as follows:

Property 6 (entropy decrease with conditioning)**.** *The entropy of a random variable decreases with successive conditionings, namely,*

$$H(X_1|X_2, \ldots, X_n) \leq \ldots \leq H(X_1|X_2, X_3) \leq H(X_1|X_2) \leq H(X_1),$$

where $X_1, \ldots, X_n$ denote n discrete random variables.

Pair of random variables

Relations between entropies

Consider X and Y two random variables, respectively with values in $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$. We have:

$$0 \overset{1}{\leq} H(X|Y) \overset{2}{\leq} H(X) \overset{3}{\leq} H(X,Y) \overset{4}{\leq} H(X) + H(Y) \overset{5}{\leq} 2H(X,Y).$$

1 : Entropie is positive (linear combination of $f(x) = -x \log x$) $1 \leq x \leq 1$

2 see previous slide (concavity) – not demonstrated.

3 $H(X,Y) = H(X) + H(Y|X) \Rightarrow H(X) \leq H(X,Y)$ because $H(Y|X) \geq 0$

4 $H(X,Y) \overset{3}{=} H(X) + H(Y|X)$ and $H(Y|X) \overset{2}{\leq} H(Y)$

$\leq H(X) + H(Y)$

5 3 applied to X and to Y $\quad H(X) \leq H(X,Y)$

$+ \quad H(Y) \leq H(X,Y)$

$\overline{H(X) + H(Y)} \leq 2\, H(X,Y)$.

Pair of random variables

Mutual information

Definition 8. *The mutual information of two random variables X and Y is defined as follows:*

$$\boxed{I(X,Y) \triangleq H(X) - H(X|Y)} = H(Y) - H(Y|X)$$

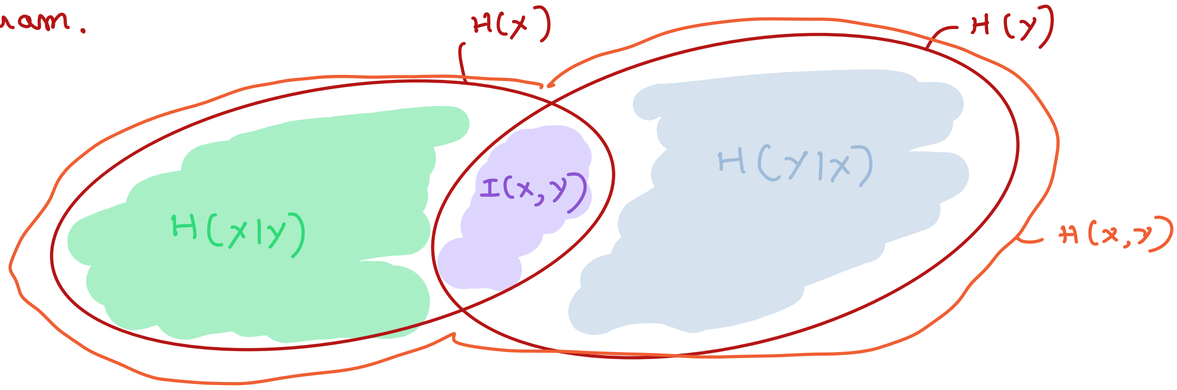
or, equivalently,

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

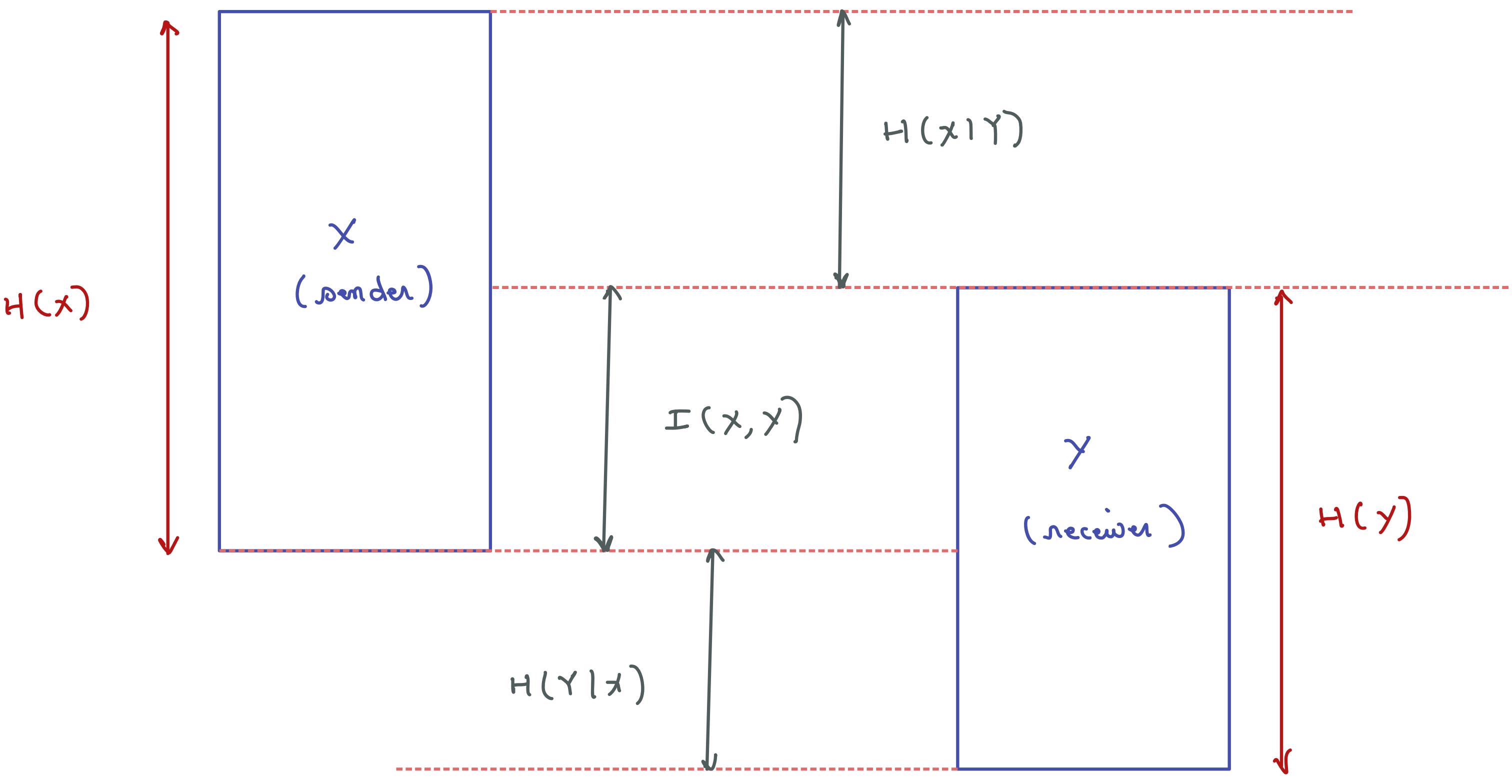
The mutual information quantifies the amount of information obtained about one random variable through observing the other random variable.

Exercise. Case of two independent random variables

Venn diagram.



$$H(x,y) = I(x,y) + H(x|y) + H(y|x)$$



Pair of random variables

Mutual information

In order to give a different interpretation of mutual information, the following definition is recalled beforehand.

Definition 9. *We call the Kullback-Leibler distance between two distributions* P_1 *and* P_2*, here supposed to be discrete, the following quantity:*

$$d(P_1, P_2) = \sum_{x \in X(\Omega)} P_1(X = x) \log \frac{P_1(X = x)}{P_2(X = x)}.$$

The mutual information corresponds to the Kullback-Leibler distance between the marginal distributions and the joint distribution of X and Y.

Pair of random variables

Venn diagram

A Venn diagram can be used to illustrate relationships among measures of information: entropy, joint entropy, conditional entropy and mutual information.