1

Introduction to Information Theory

COPYRIGHTED MATERIAL

1.1. Introduction

Information theory was developed by Claude Shannon in the 1940s [SHA 48, SHA 59b]. This is a mathematical theory which introduced source coding and channel coding, two fundamental concepts of communication systems. This theory allows us to determine, depending on the sources' properties, the theoretical limits of lossless source coding (exact message reconstruction of the source) or lossly source coding (message reconstruction under a fidelity criterion). It also gives us the reachable rates for a given transmission channel due to channel coding.

In this chapter, after reviewing the basics of discrete and continuous probabilities in section 1.2, we will start by introducing the fundamental notions of information theory such as the entropy and average mutual information in section 1.3. We will then focus on the fundamental theorems of information theory for communication systems. We will state the lossly and lossless source coding theorem in sections 1.4 and 1.5, respectively. Then we will determine the theoretical limits of communication without error in a noisy channel. In section 1.5, we will introduce different channel models and finally in section 1.7, we will compute the capacity of these channels and state the channel coding theorem.

1.2. Review of probabilities

Probability theory is a mathematical domain that describes and models random processes. In this section, we present a summary of this theory. We recommend for further reading the books of Papoulis and Pillai [PAP 02] and R. Durrett [DUR 10].

Let X be an experiment or an observation that can be repeated under similar circumstances several times. At each repetition, the result of this observation is an event denoted as x , which can take several possible outcomes. The set of these values is denoted as $\mathcal{A}_X$.

The result $X = x$ of this observation is not known before it takes place. X is consequently called a random variable. It is modeled by the frequency of appearance of all the outcomes.

Two classes of random variables can be distinguished as follows:

– discrete random variables, when the set of outcomes is discrete;

– continuous random variables, when their distribution functions are continuous.

1.2.1. *Discrete random variables*

A discrete random variable X takes its values in a discrete set, called its alphabet $\mathcal{A}_X$. This alphabet may be infinite (for instance, if $\mathcal{A}_X = \mathbb{N}$) or finite with a size n, if $\mathcal{A}_X = \{x_1, x_2, \ldots, x_n\}$. Each outcome is associated with an probability of occurrence $P_X = \{p_1, p_2, \ldots, p_n\}$:

$$Pr(X = x_i) = p_i \quad p_i \geq 0 \quad \text{and} \quad \sum_{x_i \in \mathcal{A}_X} p_i = 1 \qquad [1.1]$$

For discrete random variables, the probability density $f_X(x)$ is defined by:

$$f_X(x) = \sum_{x_i \in \mathcal{A}} \delta(x - x_i) p_i \qquad [1.2]$$

where $\delta(u)$ is the Dirac function.

1.2.1.1. *Joint probability*

Let X and Y be two discrete random variables of which respective set of possible outcomes is $\mathcal{A}_X = \{x_1, x_2, \ldots, x_n\}$ and $\mathcal{A}_Y = \{y_1, y_2, \ldots, y_m\}$.

$Pr(X = x_i, Y = y_j)$ is called the joint probability of the events $X = x_i$ and $Y = y_j$. Of course, the following property is verified:

$$\sum_{x_i \in A_x} \sum_{y_j \in \mathcal{A}_y} Pr(X = x_i, Y = y_j) = 1 \qquad [1.3]$$

1.2.1.2. *Marginal probability*

The probability $Pr(X = x_i)$ can be computed from the set of joint probabilities $Pr(X = x_i, Y = y_j)$:

$$Pr(X = x_i) = \sum_{y_j \in \mathcal{A}_y} Pr(X = x_i, Y = y_j) \qquad [1.4]$$

1.2.1.3. *Conditional probability*

$$Pr(X = x_i | Y = y_j) = \frac{Pr(X = x_i, Y = y_j)}{Pr(Y = y_j)} \qquad [1.5]$$

Similarly, we can write as:

$$Pr(Y = y_j | X = x_i) = \frac{Pr(X = x_i, Y = y_j)}{Pr(X = x_i)} \qquad [1.6]$$

As a consequence, the following relation stands:

$$\begin{aligned} Pr(Y = y_j, X = x_i) &= Pr(X = x_i | Y = y_j) Pr(Y = y_j) \\ &= Pr(Y = y_j | X = x_i) Pr(X = x_i) \end{aligned} \qquad [1.7]$$

which can be further developed to

$$Pr(Y = y_j | X = x_i) = \frac{Pr(X = x_i | Y = y_j) Pr(Y = y_j)}{Pr(X = x_i)}$$

$$= \frac{Pr(X = x_i|Y = y_j)Pr(Y = y_j)}{\sum_{y_k \in \mathcal{A}_y} Pr(X = x_i, Y = y_k)}$$

$$= \frac{Pr(X = x_i|Y = y_j)Pr(Y = y_j)}{\sum_{y_k \in \mathcal{A}_y} Pr(X = x_i|Y = y_k)Pr(Y = y_k)}$$

Equation [1.30] is called the Bayes law. From this equation, we can see that $Pr(X = x_i|Y = y_j)$ is the *a posteriori* probability, whereas $Pr(Y = y_k)$ is the *a priori* probability.

1.2.1.4. *Independence*

If two discrete random variables X and Y are independent, then

$$Pr(X,Y) = Pr(X)Pr(Y) \qquad [1.8]$$

and

$$Pr(X|Y) = Pr(X) \qquad [1.9]$$

1.2.2. *Continuous random variables*

The random variable X is continuous if its cumulative distribution function $F_X(x)$ is continuous. $F_X(x)$ is related to the probability density in the following way:

$$f_X(x) = \frac{dF_X(x)}{dx} \quad \Leftrightarrow \quad F_X(x) = \int_{-\infty}^{x} f_X(u)du \qquad [1.10]$$

The random variable mean is defined as:

$$m_X = E[X] = \int_{-\infty}^{\infty} x f_X(x)dx \qquad [1.11]$$

Its N^{th} moment is equal to:

$$E[X^N] = \int_{-\infty}^{\infty} x^N f_X(x)dx \qquad [1.12]$$

1.2.3. *Jensen's inequality*

Let us first recall that a function $f(x)$ is convex if, for any x, y and $0 < \lambda < 1$, the following inequality stands:

$$\lambda f(x) + (1-\lambda) f(y) \geq f(\lambda x + (1-\lambda) y) \qquad [1.13]$$

Let f be a convex function, $(x_1, \ldots, x_n)$ a real n-tuple belonging to the definition set of f and $(p_1, \ldots, p_n)$ a real positive n-tuple such that $\sum_{i=1}^{n} p_i = 1$. Then:

$$f\left(\sum_{i=1}^{n} p_i x_i\right) \leq \sum_{i=1}^{n} p_i f\left(x_i\right) \qquad [1.14]$$

Jensen's inequality is obtained by interpreting the p_i terms as probabilities: if $f(x)$ is convex for any real discrete random variable X, then:

$$f\left(E[X]\right) \leq E\left[f(X)\right] \qquad [1.15]$$

1.2.4. *Random signals*

The signals used in digital communications depend on time t.

Signal $x(t)$ is deterministic if the function $t \mapsto x(t)$ is perfectly known. If, however, the values taken by $x(t)$ are unknown, the signal follows a random process. At time t, the random variable is denoted by $X(t)$, and an outcome of this random variable is denoted as $x(t)$. The set of all signal values $x(t)$, for any t in the definition domain, is a given outcome of the random process X.

A random process is defined by its probability density and its statistical moments. The probability density is equal to:

$$f_X(x,t) = \lim_{\Delta x \to 0} \frac{Pr\left(x \leq X(t) \leq x + \Delta x\right)}{\Delta x} \qquad [1.16]$$

The random process is stationary if its probability density is independent of time: $f_X(x,t) = f_X(x)\ \forall t$. As a consequence, all of its statistical properties

are independent of t. Its probability density can thus be obtained from equation [1.10] in the following way:

$$f_X(x) = \lim_{\Delta X \to 0} \frac{F_{X+\Delta X}(x) - F_X(x)}{\Delta X} \qquad [1.17]$$

$m_x(t)$, the mean of the random variable $x(t)$ from the random process X, is defined as:

$$m_x(t) = E\left[x(t)\right] \qquad [1.18]$$

The autocorrelation function $R_{xx}(\tau)$ of a random variable is:

$$R_{xx}(t_1, t_2) = E\left[x(t_1)x^*(t_2)\right] \qquad [1.19]$$

The random process X is second-order stationary or wide-sense stationary if, for any random signal $x(t)$:

1) its mean $m_x(t)$ is independent of t;

2) its autocorrelation function verifies $R_{xx}(t_1, t_2) = R_{xx}(t_1 + t, t_2 + t)\ \forall t$.

Then it can simply be denoted as:

$$R_{xx}(\tau) = E\left[x(t)x^*(t - \tau)\right] \qquad [1.20]$$

In that case, the power spectrum density $\gamma_{xx}(f)$ is obtained by applying the Fourier transform on the autocorrelation function:

$$\begin{aligned} \gamma_{xx}(f) &= TF\left[R_{xx}\right](f) \\ &= \int_{-\infty}^{+\infty} R_{xx}(\tau)e^{-j2\pi f\tau}d\tau \end{aligned} \qquad [1.21]$$

Reciprocally, the autocorrelation function $R_{xx}(\tau)$ is determined from the power spectrum density as follows:

$$\begin{aligned} R_{xx}(\tau) &= TF^{-1}\left[\gamma_{xx}\right](\tau) \\ &= \int_{-\infty}^{+\infty} \gamma_{xx}(f)e^{+j2\pi f\tau}df \end{aligned} \qquad [1.22]$$

Generally, the mean and autocorrelation function of a stationary random process are estimated from a set of outcomes of signal $X(t)$. When the mean over time tends to the random process' mean, the random process is ergodic. Only one outcome of the random process X is required to evaluate its mean and autocorrelation function. Most random processes that are considered in digital communications are second-order stationary and ergodic.

For discrete signals (for instance, signals that have been sampled from a continuous random signal $x(t)$ at frequency $\frac{1}{T_e}$) $x_n = x(nT_e)$, the autocorrelation function $R_{xx}(\tau)$ is only defined at discrete times $\tau = nT_e$, and the power spectrum density becomes:

$$\begin{aligned}\gamma_{xx}(f) &= TF\left[R_{xx}\right](f) \\ &= \sum_{n=-\infty}^{+\infty} R_{xx}(nT_e)e^{-j2\pi fnT_e}\end{aligned} \qquad [1.23]$$

1.3. Entropy and mutual information

1.3.1. *Comments on the concept of information*

The quantitative notion of information associated with a message exchanged between a source and a receiver in the usual language is linked, for instance, to the veracity of the message, the *a priori* knowledge of the message by the receiver or the receiver's understanding (where a problem of language can occur, etc.).

All these considerations are a matter of semantic and are not taken into account by information theory. In information theory, we will only retain a part of the general concept of information: the quantitative measure of information is a measure of the uncertainty associated with an event. This notion of information is fundamental for the study of communication systems.

1.3.2. *A logarithmic measure of information*

A measure of the information associated with the event $X = x_i$ denoted as $h(x_i)$ should satisfy the following properties [SHA 48]:

– $h(x_i)$ should be continuous for $p(X = x_i)$ between 0 and 1;

– $h(x_i) = \infty$ if $Pr(X = x_i) = 0$;

– $h(x_i) = 0$ if $Pr(X = x_i) = 1$: a certain event brings no information;

– $h(x_i) > h(y_j)$ if $Pr(Y = y_j) > Pr(X = x_i)$: more an event is uncertain, more information it will bring;

– $h(x_i) + h(y_j) = h(x_i, y_j)$, if the events $Y = y_j$ and $X = x_i$ are independent: the realization of two independent events bring a quantity of information equal to the sum of the quantity of information of these two events $h(x_i)$ and $h(y_j)$.

In order to satisfy the above properties, the quantity of information $h(x_i)$ associated with the realization of the event $X = x_i$ should be equal to the logarithm of the inverse of the probability $Pr(X = x_i)$. Using this definition, a high probability event will carry less quantity of information than a low probability event. When the binary logarithm is used[1], the unit $h(x_i)$ is the Shannon (Sh). When the natural logarithm is used, the unit is the natural unit (Nat). In this book, we will consider binary logarithms. Consequently, we have the following relation:

$$h(x_i) = \log_2 \frac{1}{Pr(X = x_i)} = -\log_2 Pr(X = x_i) = -\log_2 p_i \qquad [1.24]$$

EXAMPLE 1.1.– Let a discrete source generate bits (0 or 1) with $Pr(X = 0) = Pr(X = 1) = \frac{1}{2}$. The quantity of information associated with the realization of the event $X = 0$ or $X = 1$ is equal to:

$$h(0) = h(1) = -\log_2 \frac{1}{2} = 1 \text{ Sh} \qquad [1.25]$$

If the source is generating a sequence composed of n independent bits, we have 2^n different sequences. Each of these sequences can appear with the probability $\frac{1}{2^n}$. The quantity of information associated with the realization of a specific sequence is equal to:

$$h(\text{sequence of } n \text{ bits}) = -\log_2 \frac{1}{2^n} = n \text{ Sh} \qquad [1.26]$$

1 $\log_2 x = \ln x / \ln 2$.

Let us consider the realization of two events $X = x_i$ and $Y = x_j$. The associated quantity of information is:

$$h(x_i, y_j) = \log_2 \frac{1}{Pr(X = x_i, Y = y_j)} = -\log_2 Pr(X = x_i, Y = y_j) \quad [1.27]$$

where $Pr(X = x_i, Y = y_j)$ is the joint probability of the two events.

The quantity of information associated with the realization of the event $X = x_i$ conditionally to the event $Y = y_j$ is as follows:

$$h(x_i|y_j) = \log_2 \frac{1}{Pr(X = x_i|Y = y_j)} = -\log_2 Pr(X = x_i|Y = y_j) \quad [1.28]$$

From relation [1.7], we deduce:

$$h(x_i, y_j) = h(x_i|y_j) + h(y_j) = h(y_j|x_i) + h(x_i) \quad [1.29]$$

or also:

$$h(x_i, y_j) = h(x_i|y_j) + h(y_j) = h(y_j|x_i) + h(x_i) \quad [1.30]$$

EXAMPLE 1.2.– A card is randomly drawn from a standard deck of 32 cards (4 colors: heart, spade, diamond, club – 8 values: 7, 8, 9, 10, Jack, Queen, King and Ace). Let x be the event "the drawn card is the club ace" and y be the event "the drawn card is a club". We can compute $h(x)$, $h(y)$ and $h(x|y)$. Since we have:

$$Pr(X = x) = \frac{1}{32} \quad \text{and} \quad Pr(Y = y) = \frac{1}{4} \quad [1.31]$$

we obtain:

$$h(x) = -\log_2 \frac{1}{32} = 5 \text{ Sh} \quad \text{and} \quad h(y) = -\log_2 \frac{1}{4} = 2 \text{ Sh} \quad [1.32]$$

$$Pr(X = x|Y = y) = \frac{Pr(X = x, Y = y)}{Pr(Y = y)} = \frac{1/32}{1/4} = \frac{1}{8} \quad [1.33]$$

$$h(x|y) = -\log_2 Pr(X = x|Y = y) = -\log_2 \frac{1}{8} = 3 \text{ Sh} \quad [1.34]$$

1.3.3. *Mutual information*

We define the mutual information as the quantity of information that the realization of the event $Y = y_j$ gives about the event $X = x_i$. In other words, the mutual information is the difference between the quantity of information associated with the realization of the event $X = x_i$ and the quantity of information associated with the the realization of the event $X = x_i$ conditionally to the event $Y = y_j$. This quantity of information is given by:

$$\begin{aligned} i(x_i; y_j) &= h(x_i) - h(x_i|y_j) \\ &= \log_2 \frac{Pr(X = x_i|Y = y_j)}{Pr(X = x_i)} \end{aligned} \quad [1.35]$$

If the two events are independent, we have $Pr(X = x_i|Y = y_j) = Pr(X = x_i)$ and consequently $i(x_i; y_j) = 0$. On the opposite, it the event $X = x_i$ is equivalent to the event $Y = y_j$, then we have $Pr(X = x_i|Y = y_j) = 1$ and $i(x_i; y_j) = h(x_i)$.

Since we have the following relation:

$$\frac{Pr(X = x_i|Y = y_j)}{Pr(X = x_i)} = \frac{Pr(X = x_i, Y = y_j)}{Pr(X = x_i)Pr(Y = y_j)} = \frac{Pr(Y = y_j|X = x_i)}{Pr(Y = y_j)}$$

The quantity of information that the realization of the event $Y = y_j$ gives about the event $X = x_i$ is the same as the information that the realization of the event $X = x_i$ gives about the event $Y = y_j$.

$$i(x_i; y_j) = i(y_j; x_i) \quad [1.36]$$

We also have the following relations:

$$\begin{aligned} i(x_i; y_j) &= h(x_i) - h(x_i|y_j) \\ &= h(x_i) + h(y_j) - h(x_i, y_j) \\ &= h(y_j) - h(y_j|x_i) \end{aligned}$$

Compared to $h(x_i)$, the mutual information $i(x_i; y_j)$ can be negative.

EXAMPLE 1.3.– (cont.) Compute $i(x;y)$:

$$\begin{aligned} i(x;y) &= h(x) - h(x|y) \\ &= 5 \text{ Sh} - 3 \text{ Sh} = 2 \text{ Sh} \end{aligned} \quad [1.37]$$

The quantity of information that the realization of the event "the drawn card is a club" gives about the event "the drawn card is a club ace" is equal to 2 Sh.

We will see in section 1.7 that the mutual information is important for communications when we associate X with the input of the channel transmission and Y to the output of the channel transmission.

1.3.4. *Entropy and average mutual information*

After having considered individual events, we will now compute the entropy of a source described with the random variable X with sample space $\mathcal{A}_X = \{x_1, x_2, \ldots, x_n\}$ and associated probabilities $\mathcal{P}_X = \{p_1, p_2, \ldots, p_n\}$. n is the size of the sample space. The average quantity of information or entropy of the source is the mean of the quantity of information associated with each possible realization of the event $X = x_i$:

$$\begin{aligned} H(X) &= \sum_{i=1}^{n} p_i h(x_i) \\ &= \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} \\ &= -\sum_{i=1}^{n} p_i \log_2 p_i \quad \text{in Sh/symbol} \end{aligned} \quad [1.38]$$

$H(X)$ is a measure of the uncertainty on X.

The entropy $H(X)$ has the following properties:

$$H(X) \geq 0 \quad [1.39]$$

$$H(X) \leq \log_2 n \quad [1.40]$$

$$H(X) = H_{MAX}(X) = \log_2 n \quad \text{if} \quad p_i = \frac{1}{n} \quad \forall i \quad [1.41]$$

The entropy is maximum when all the probabilities p_i are the same.

EXAMPLE 1.4.– Let a source with 2 states x_0 and x_1 with $p_0 = p$ and $p_1 = 1 - p$. The entropy of this source is the following:

$$\begin{aligned} H(X) &= -p \log_2 p - (1-p) \log_2 (1-p) \\ &\equiv H_2(p) \end{aligned} \qquad [1.42]$$

The function $H_2(p)$ defined previously will be often used in this chapter to simplify the notations. It is given in Figure 1.1.

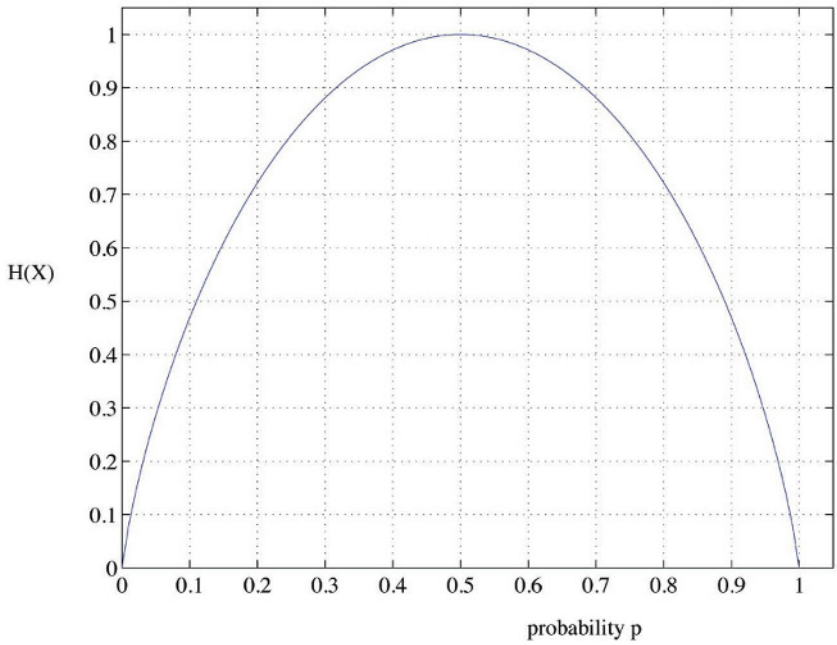


Figure 1.1. *Entropy of a binary source*

The entropy is maximum (1 Sh/bit) when $p = 0.5$.

We define two random variables X and Y with state spaces $\mathcal{A}_X = \{x_1, x_2, \ldots, x_n\}$ and $\mathcal{A}_Y = \{y_1, y_2, \ldots, y_m\}$, respectively. The joint

entropy $H(X,Y)$ is defined as follows:

$$H(X,Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j)h(x_i, y_j)$$
$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j)\log_2 Pr(X = x_i, Y = y_j) \quad [1.43]$$

If the two random variables X and Y are independent, the joint entropy is equal to the sum of the entropies $H(X)$ and $H(Y)$.

We can also compute the conditional entropy $H(X/Y)$ corresponding to the average quantity of information of X given the observation Y from $h(x_i|y_j)$:

$$H(X|Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j)h(x_i|y_j)$$
$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j)\log_2 Pr(X = x_i|Y = y_j) \quad [1.44]$$

The relations [1.7] and [1.30] enable us to write the joint entropy as a function of the entropy and the conditional entropy:

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) \quad [1.45]$$

The uncertainty on X and Y is equal to the sum of the uncertainty on X and the uncertainty on Y given X.

The mutual information associated with the realization of an event can be extended to the random variable X and Y. The average mutual information

between the random variables X and Y is given by:

$$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j) i(x_i; y_j)$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j) \log_2 \frac{Pr(X = x_i | Y = y_j)}{Pr(X = x_i)}$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{m} Pr(X = x_i, Y = y_j) \log_2 \frac{Pr(X = x_i, Y = y_j)}{Pr(X = x_i) Pr(Y = y_j)} \quad [1.46]$$

Consequently, we have also the following relations:

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$
$$= H(X) - H(X|Y) = H(Y) - H(Y|X) \quad [1.47]$$

The average mutual information $I(X;Y)$ measures the average quantity of information on X (or reduction of average uncertainty) due to the observation of Y. Figure 1.2 shows graphically the relations between the different entropies and the average mutual information.

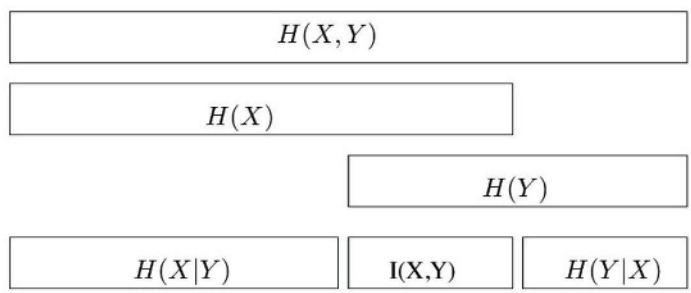


Figure 1.2. *Relations between entropies and average mutual information*

While $i(x_i; y_j)$ can be negative, we always have $I(X;Y) \geq 0$.

1.3.5. *Kullback–Leibler divergence*

Let X and Y be two random variables with state spaces $\mathcal{A}_X = \{x_1, x_2, \ldots, x_n\}$ and $\mathcal{A}_Y = \{y_1, y_2, \ldots, y_n\}$ and with associated probabilities $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ and $\mathcal{Q} = \{q_1, q_2, \ldots, q_n\}$, respectively.

We define the relative entropy or Kullback–Leibler divergence as follows:

$$D_{KL}(\mathcal{P}||\mathcal{Q}) = \sum_{i=1}^{n} p_i \log_2 \frac{p_i}{q_i} \qquad [1.48]$$

While Kullback–Leibler is often considered as a measure of distance between two probability densities, it is not strictly speaking a distance. For example, we generally have $D_{KL}(\mathcal{P}||\mathcal{Q}) \neq D_{KL}(\mathcal{Q}||\mathcal{P})$.

We can prove that $D_{KL}(\mathcal{P}||\mathcal{Q}) \geq 0$ and that $D_{KL}(\mathcal{P}||\mathcal{Q}) = 0$ if and only if $p_i = q_i \quad \forall i = 1 \ldots n$.

For continuous random variables P and Q with density probability $p(x)$ and $q(x)$, respectively, the Kullback–Leibner divergence is defined by the integral

$$D_{KL}(P||Q) = \int_{-\infty}^{\infty} p(x) \ln \frac{p(x)}{q(x)} dx \qquad [1.49]$$

1.3.6. *Differential entropy*

The differential entropy is a generalization of the entropy to the case of continuous random variables. Let a continuous random variable X be defined by the density probability $p(x)$. The differential entropy $H_D(X)$ of X is equal to:

$$H_D(X) = -\int_{-\infty}^{+\infty} p(x) \log_2 p(x) dx \qquad [1.50]$$

The differential entropy characterizes the quantity of information of the continuous random variable X.

Let us compute the differential entropy $H_D(X)$ of a random variable X with a centered Gaussian probability distribution of variance σ_x^2. We have:

$$H_D(X) = -\frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^{+\infty} \exp\left(\frac{-x^2}{2\sigma_x^2}\right) \log_2\left[\frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left(\frac{-x^2}{2\sigma_x^2}\right)\right] dx \quad [1.51]$$

$$= -\frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^{+\infty} \exp\left(\frac{-x^2}{2\sigma_x^2}\right)\left[\log_2\left(\frac{1}{\sqrt{2\pi\sigma_x^2}}\right) - \frac{x^2}{2\sigma_x^2}\log_2 e\right] dx \quad [1.52]$$

Since $\log_2\left(\frac{1}{\sqrt{2\pi\sigma_x^2}}\right)$ does not depend on x and

$$\frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^{+\infty} \exp\left(\frac{-x^2}{2\sigma_x^2}\right) = 1$$

We can extract the first term in the integral. Then we obtain:

$$H_D(X) = \log_2\left(\sqrt{2\pi\sigma_x^2}\right) + \frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^{+\infty} \frac{x^2}{2\sigma_x^2}\log_2 e \exp\left(\frac{-x^2}{2\sigma_x^2}\right) dx \quad [1.53]$$

By definition,

$$E[X^2] = \frac{1}{\sqrt{2\pi\sigma_x^2}} \int_{-\infty}^{+\infty} x^2 \exp\left(\frac{-x^2}{2\sigma_x^2}\right) dx = \sigma_x^2 \quad [1.54]$$

Finally, we have:

$$H_D(X) = \frac{\log_2 e}{2} + \log_2\left(\sqrt{2\pi\sigma_x^2}\right) = \frac{1}{2}\log_2 2\pi e\sigma_x^2 \quad [1.55]$$

1.3.7. *Typical and jointly typical sequences*

1.3.7.1. *Typical sequences*

The set of all sequences of random variable can be divided into two disjoint sets: the set of typical sequences and the set of non-typical sequences. Typical sequences are an important tool for the demonstration of the fundamental theorems of information theory.

Let us define a sequence of random variables $\mathbf{X} = (X_1, X_2, \ldots, X_N)$ independent and identically distributed (i.i.d) with state space $\mathcal{A}_X$ and $\mathbf{x}$ be a realization.

Since the variables X_i are independent, the terms $\log_2(Pr(X_i))$ are also independent and we have the following relation:

$$-\frac{1}{N}\log_2 Pr(\mathbf{X}=\mathbf{x}) = -\frac{1}{N}\sum_{i=1}^{N}\log_2 Pr(X_i = x_i) \qquad [1.56]$$

This relation converges to $H(X)$ when N is high enough. This property is called the asymptotic equipartition principle (AEP). Among the set of all the possible sequences $\mathcal{A}_X^N$, we define the typical sequences for which the probability of occurrence is close to $2^{-N(H(X)}$. The set of typical sequences $\mathcal{T}_\epsilon$ is described as follows:

$$\mathcal{T}_\epsilon = \left\{ \mathbf{x} \in \mathcal{A}_X^N : \left| \frac{1}{N}\log_2 Pr(\mathbf{X}=\mathbf{x}) - H(X) \right| < \epsilon \right\} \qquad [1.57]$$

From the relations [1.56] and [1.57], we can easily prove the following properties:

1) The probability that a sequence $\mathbf{x}$ is typical converge to 1 when $N \to \infty$.

2) The number of typical sequences $|\mathcal{T}_\epsilon|$ is upper bounded by:

$$|\mathcal{T}_\epsilon| \leq 2^{N(H(X)+\epsilon)} \qquad [1.58]$$

To summarize, for a sequence of random variables $\mathbf{X}$ with N large enough, the realizations $\mathbf{x}$ belong almost surely to the set $\mathcal{T}_\epsilon$ composed of around $2^{N(H(X))}$ sequences, each having an occurrence probability close to $2^{-N(H(X))}$.

In order to illustrate the typical sequences, we will consider a simple example. Let us consider a binary memoryless random variable X with occurrence probabilities $p_1 = \frac{2}{3}$ and $p_2 = \frac{1}{3}$. The entropy of X is equal to 0.9183 Sh/symb. For a vector of length N, we have $\binom{N}{n}$ sequences[2] composed of n symbols x_1 and $N - n$ symbols x_2 and of occurrence probability $Pr(\mathbf{x}) = p_1^n p_2^{N-n}$. In Figure 1.3, we have plotted the probability distribution of the sequences for $N = 100$ (continuous line) and the distribution of typical sequences set (dash line). We can see that for $N = 100$, the probability distribution is close enough to one of the set composed of 4.410^{27} typical sequences.

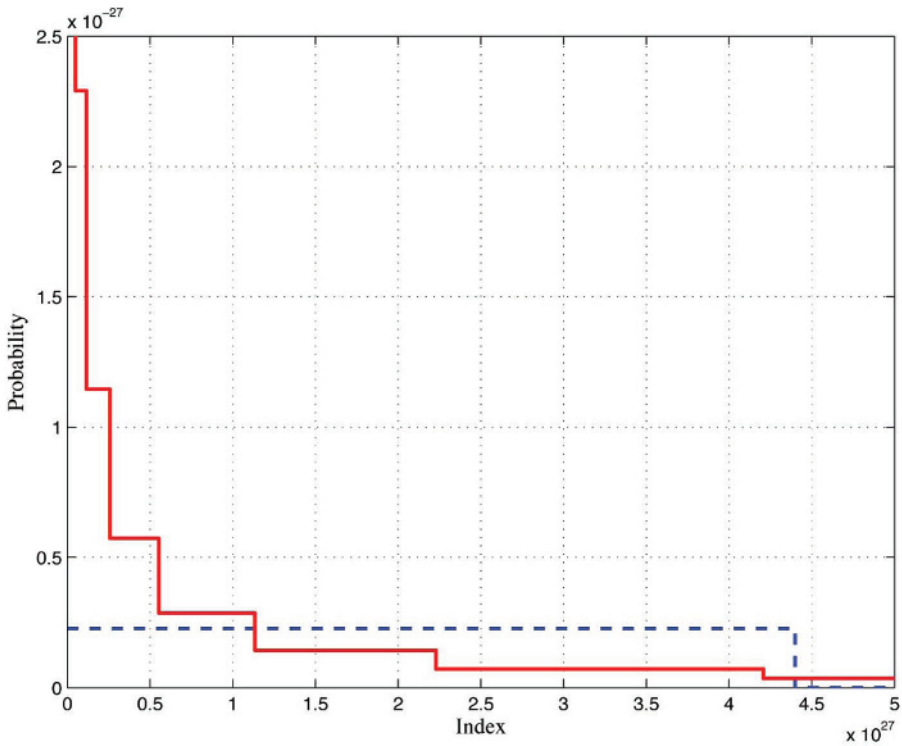


Figure 1.3. *Density probability and typical sequences set*

2 $\binom{n}{p} = \frac{n!}{p!(n-p)!}$ is the number of ways to choose without repetition p elements from a set of n elements.

1.3.7.2. *Jointly typical sequences*

The concept of typical sequences can be extended to the case of sequences of random variables couples. The set of jointly typical sequences $\mathcal{J}_\epsilon$ is described as follows:

$$\mathcal{J}_\epsilon = \left\{ \mathbf{x} \in \mathcal{A}_X^N : \left| \frac{1}{N} \log_2 Pr(\mathbf{X} = \mathbf{x}) - H(X) \right| < \epsilon \right. \\ \left| \frac{1}{N} \log_2 Pr(\mathbf{Y} = \mathbf{y}) - H(Y) \right| < \epsilon \\ \left. \left| \frac{1}{N} \log_2 Pr((\mathbf{X}, \mathbf{Y}) = (\mathbf{x}, \mathbf{y})) - H(X,Y) \right| < \epsilon \right\} \quad [1.59]$$

Let $(\mathbf{x}, \mathbf{y})$ be a sequence of random variables couples i.i.d. according to the following joint probability:

$$Pr(\mathbf{X} = \mathbf{x}, \mathbf{Y} = \mathbf{y}) = \prod_{i=1}^{N} Pr(X_i = x_i, Y_i = y_i) \quad [1.60]$$

We can easily prove the following properties:

– the probability that a sequence of couples $(\mathbf{x}, \mathbf{y})$ is jointly typical reaches 1 when $N \to \infty$;

– the number of sequences of couples that are jointly typical $|\mathcal{J}_\epsilon|$ is upper bounded by:

$$|\mathcal{J}_\epsilon| \leq 2^{N(H(X,Y)+\epsilon)}$$

– let $\mathbf{x}$ and $\mathbf{y}$ be two independent realizations of $\mathbf{X}$ and $\mathbf{Y}$ respectively, the probability that $(\mathbf{x}', \mathbf{y}')$ belongs to the set of jointly typical sequences of couples is:

$$Pr((\mathbf{x}', \mathbf{y}') \in \mathcal{J}_\epsilon) \leq 2^{-N(I(X;Y)-3\epsilon)} \quad [1.61]$$

The first two properties are obtained from the relations [1.56] and [1.59]. The proof of the third property is the following:

$$\begin{aligned} Pr((\mathbf{x}', \mathbf{y}') \in \mathcal{J}_\epsilon) &= \sum_{(\mathbf{x},\mathbf{y})\in\mathcal{J}_\epsilon} Pr(\mathbf{X} = \mathbf{x}) Pr(\mathbf{Y} = \mathbf{y}) \\ &\leq 2^{N(H(X,Y)+\epsilon)} 2^{-N(H(X)+\epsilon)} 2^{-N(H(Y)+\epsilon)} \\ &= 2^{-N(I(X;Y)-3\epsilon)} \end{aligned} \quad [1.62]$$

Since we have about $2^{N(H(X))}$ typical sequences $\mathbf{x}$, $2^{N(H(Y))}$ typical sequences $\mathbf{y}$ and only $2^{N(H(X,Y))}$ jointly typical sequences of couples, the probability to choose a jointly typical sequence of couples among the set of couples of typical sequences independently selected is approximately equal to:

$$\frac{2^{N(H(X,Y))}}{2^{N(H(X))} 2^{N(H(Y))}} = 2^{-N(I(X;Y))} \quad [1.63]$$

1.4. Lossless source coding theorems

1.4.1. *Introduction*

Source coding is divided into two classes: lossless source coding and lossy source coding. We will first study lossless source coding also called entropy coding. The aim of lossless source coding is to describe the digital sequence delivered by the source with the shortest sequence of symbols with the ability to reconstruct it by the source decoder.

As in most of the classical books on digital communications, in this chapter, we will study the techniques of source coding by ignoring the effect of the transmission channel and using Shannon's paradigm. Consequently, we assume that the output of the source coder is directly connected to the input of the source decoder as shown in Figure 1.4.

1.4.2. *Entropy and source redundancy*

We consider a discrete and stationary source the output symbols of which are Q-ary symbols (the size of the alphabet is equal to Q). The output of this

source is described by the random variable X. Consequently, the entropy $H(X)$ is the average quantity of information per symbol at the output of the source.

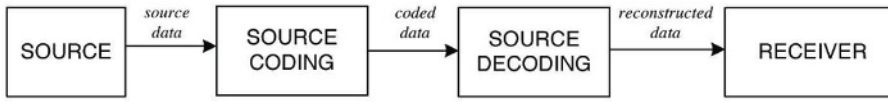


Figure 1.4. *Block diagram of the studied chain for source coding*

A discrete source is memoryless if the output symbols are de-correlated. Otherwise, we will say that the source is with memory.

If the source is memoryless, $H(X)$ can be computed as previously:

$$H(X) = -\sum_{i=1}^{Q} p_i \log_2 p_i \qquad \text{in Sh/symbol} \qquad [1.64]$$

The entropy $H(X)$ is maximum if the symbols are equiprobable. For Q-ary symbols, the maximum entropy is $H_{MAX} = \log_2 Q$.

If the source is with memory, then the entropy per symbol $H(X)$ can be computed by:

$$H(X) = \lim_{J \to \infty} \frac{1}{J} H_J(X) \qquad [1.65]$$

where $H_J(X)$ is the entropy per group of J symbols.

The redundancy of the source R_{red} characterizes the difference between the quantity of information of the source and the quantity of a source with equiprobable symbols. We have:

$$R_{red} = 1 - \frac{H(X)}{H_{MAX}(X)} \qquad [1.66]$$

The range of R_{red} is between 0 (the source symbols are independent and equiprobable) and 1 (the entropy of this source is zero).

1.4.3. *Fundamental theorem of source coding*

The fundamental theorem of source coding stated by Shannon [SHA 48] is the following:

THEOREM 1.1.– Let $\epsilon > 0$, for all stationary source with entropy per symbol $H(X)$, there is a binary source coding method that associates with each message $\mathbf{x}$ of length N a binary word of average length NR_{moy} such that:

$$H(X) \leq R_{moy} < H(X) + \epsilon \qquad [1.67]$$

Consequently, we can associate, on average $NH(X)$ bits, with each message $\mathbf{x}$.

PROOF.– We have seen previously that the typical sequences allow us to divide the set of sequences of random variables into two disjoint sets. The total set of the $|\mathcal{A}_X|^N$ sequences $\mathbf{x}$ can be divided into two sets: the set $\mathcal{T}_\epsilon$ of typical sequences with $| \leq |\mathcal{T}_\epsilon 2^{N(H(X)+\epsilon)}$ and the set $\mathcal{T}_\epsilon^c$ of the non-typical sequences.

In order to distinguish these two sets, we can add a prefix "0" for the typical sequences and "1" for the non-typical sequences. So, the typical sequences can be encoded using $N(H(X) + \epsilon) + 2$ bits (the additional bit takes into account the fact that $N(H(X) + \epsilon)$ is not necessarily an integer). The non-typical sequences can be encoded using at most $N \log_2 |\mathcal{A}_X| + 2$ bits.

We can bound the rate or average bits per realization R_{moy} as follows:

$$\begin{aligned} R_{moy} &= E\left[\frac{1}{N} l(\mathbf{X})\right] \\ &= \frac{1}{N} \sum_{\mathbf{x}} l(\mathbf{x}) Pr(\mathbf{X} = \mathbf{x}) \\ &= \frac{1}{N} \sum_{\mathbf{x} \in \mathcal{T}_\epsilon} l(\mathbf{x}) Pr(\mathbf{X} = \mathbf{x}) + \frac{1}{N} \sum_{\mathbf{x} \in \mathcal{T}_\epsilon^c} l(\mathbf{x}) Pr(\mathbf{X} = \mathbf{x}) \end{aligned}$$

$$\leq \frac{1}{N}\sum_{\mathbf{x}\in\mathcal{T}_\epsilon}(N(H(X)+\epsilon)+2)Pr(\mathbf{X}=\mathbf{x}) + \frac{1}{N}\sum_{\mathbf{x}\in\mathcal{T}_\epsilon^c}(N\log_2|\mathcal{A}_X|+2)Pr(\mathbf{X}=\mathbf{x})$$

$$\leq H(X)+\epsilon+\epsilon\log_2|\mathcal{A}_X|+\frac{2}{N}$$

$$= H(X)+\epsilon' \qquad [1.68]$$

$\epsilon' = \epsilon\log_2|\mathcal{A}_X| + \frac{2}{N}$ can be as small as we want by choosing a high value for N.

1.4.4. *Lossless source coding*

1.4.4.1. *Introduction*

From a general point of view, the source coder associates with each message delivered by the source a word composed of q-ary symbols while trying to minimize the average number of these symbols. A message, depending on the context, will be a Q-ary symbol from the source or a set of J Q-ary symbols.

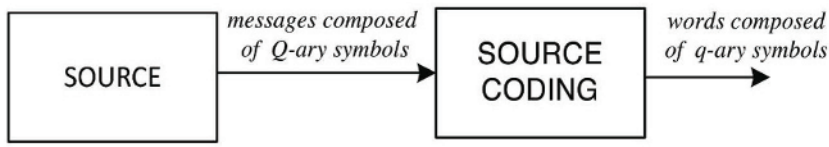


Figure 1.5. *Source coding*

We will restrict ourselves to the case where the symbols at the output of the source coder are bits ($q = 2$). The generalization to other alphabet sizes is possible without any particular difficulties.

The source coding should satisfy the two following criteria:

– unique coding: each message should be coded with a different word;

– unique decoding: each word should be distinguished without ambiguity. This criterion can be obtained using:

- coding by fixed length word,

- coding using a distinguishable separable symbol (Morse system for example),

- coding with words of variable length.

Since the source coding with a separable symbol is a suboptimal and obsolete solution, later in this chapter, we will focus only on variable and fixed length source coding.

A source code is instantaneous if no word is the beginning of another. This condition called prefix condition is important to facilitate the decoding.

1.4.4.2. *Variable length coding*

EXAMPLE 1.5.– Let a discrete source generating four different messages a_1, a_2, a_3 and a_4 with their respective probabilities $Pr(a_1) = \frac{1}{2}$, $Pr(a_2) = \frac{1}{4}$ and $Pr(a_3) = Pr(a_4) = \frac{1}{8}$. One word is associated with each message as described in Table 1.1.

Message	*Word*
a_1	1
a_2	00
a_3	01
a_4	10

Table 1.1. *Variable length code of example 1*

We can check that this source code satisfies the criterion of unique coding but it does not allow a unique decoding. Indeed, for example, it is not possible to decode the message $a_1, a_2, a_1, \ldots$ etc. coded by the sequence 1001. At the receiver, we have no way to decide if the transmitted message was a_1, a_2, a_1 or a_4, a_3. Consequently, this code is unusable.

EXAMPLE 1.6.– One word is associated with each message as described in Table 1.2.

We can check that this source code satisfies both unique coding and decoding. However, this code is not instantaneous. Indeed, the message a_3 is

the beginning of the message a_4. After the sequence 11, it is necessary to determine the parity of the number of zeros in order to be able to decode the rest of the transmitted message. Consequently, the decoding is more complex.

Message	*Word*
a_1	00
a_2	10
a_3	11
a_4	110

Table 1.2. *Variable length code of example 2*

EXAMPLE 1.7.– One word is associated with each message as described in Table 1.3.

Message	*Word*
a_1	0
a_2	10
a_3	110
a_4	111

Table 1.3. *Variable length code of example 3*

This source code satisfies both the unique coding and decoding. It is instantaneous as we can check on Figure 1.6 that shows the tree associated with this source code.

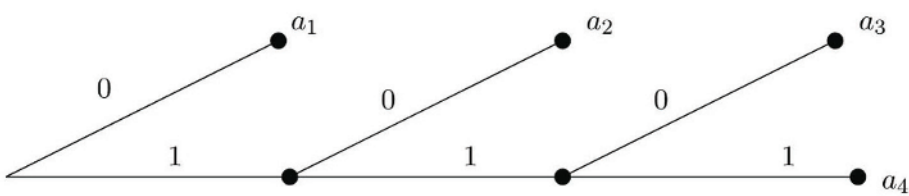


Figure 1.6. *Tree associated with the source code of example 3*

1.4.4.3. *Kraft inequality*

THEOREM 1.2.– An instantaneous code composed of Q binary words of length $\{n_1, n_2, \ldots, n_Q\}$, respectively, with $n_1 \leq n_2 \leq \cdots \leq n_Q$ should satisfy the following inequality:

$$\sum_{i=1}^{Q} 2^{-n_i} \leq 1 \qquad [1.69]$$

PROOF.– An instantaneous code can be graphically represented using a complete binary tree of depth n_Q. Each leaf of the final tree is associated with one of the source message. The word is the label sequence of the path going from the tree root to the leaf.

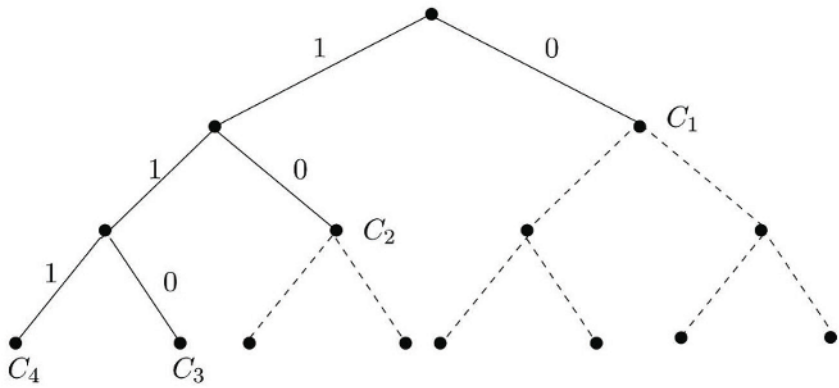


Figure 1.7. *Kraft inequality*

A complete tree is composed of 2^{n_Q} leaves. Let us choose a node of degree n_1 as the leaf associated with the first word C_1; this choice eliminates $2^{n_Q - n_1}$ leaves. Among the remaining nodes, we choose a node of degree n_2 as the leaf associated with the second word C_2. This choice eliminates $2^{n_Q - n_2}$ leaves. We continue this procedure until the last word. The necessary condition to guarantee an instantaneous decoding is the following:

$$\sum_{i=1}^{Q} 2^{n_Q - n_i} \leq 2^{n_Q}$$

By dividing the two terms by 2^{n_Q}, we obtain the Kraft inequality.

1.4.4.4. *Fundamental theorem of source coding*

We consider first a memoryless source with entropy per symbol $H(X)$. We will prove that, for this source, it is possible to build an instantaneous code for which the average length of the words R_{moy} satisfy the following inequality:

$$H(X) \leq R_{moy} < H(X) + 1 \qquad [1.70]$$

with

$$R_{moy} = \sum_{i=1}^{Q} p_i n_i \qquad [1.71]$$

PROOF.– We choose n_i the length of the word associated with the i^{th} message as follows:

$$n_i = \lceil h(x_i) \rceil = \lceil -\log_2 p_i \rceil \qquad [1.72]$$

$\lceil x \rceil$ is the smallest integer not less than x.

Let us verify that such a source code is instantaneous or, equivalently, that it satisfies the Kraft inequality:

$$\sum_{i=1}^{Q} 2^{-n_i} = \sum_{i=1}^{Q} 2^{-\lceil -\log_2 p_i \rceil} \leq \sum_{i=1}^{Q} 2^{\log_2 p_i} = \sum_{i=1}^{Q} p_i = 1 \qquad [1.73]$$

since $\lceil -\log_2 p_i \rceil \geq -\log_2 p_i$.

Consequently, we have:

$$\begin{aligned} R_{moy} &= \sum_{i=1}^{Q} p_i n_i = \sum_{i=1}^{Q} p_i \lceil -\log_2 p_i \rceil < \sum_{i=1}^{Q} p_i (-\log_2 p_i + 1) \\ &= H(X) + 1 \end{aligned} \qquad [1.74]$$

The fundamental theorem of source coding can be expressed as follows:

THEOREM 1.3.– For all stationary sources with entropy per symbol $H(X)$, there is a source coder that can encode the message into binary words with average length R_{moy} as close as possible to $H(X)$.

$$H(X) \leq R_{moy} < H(X) + \epsilon \qquad [1.75]$$

We consider again a memoryless source with entropy per symbol $H(X)$. By grouping the symbols of this source into a message composed of J symbols, we obtain a new source that can also be encoded using an instantaneous code. The length of the words of this new code R_{Jmoy} satisfies the following inequality:

$$JH(X) \leq R_{Jmoy} < JH(X) + 1 \qquad [1.76]$$

Dividing the terms by J, we obtain:

$$H(X) \leq R_{moy} < H(X) + \frac{1}{J} \qquad [1.77]$$

R_{moy} is the average number of bits associated with a symbol of the source $R_{moy} = \frac{R_{Jmoy}}{J}$. By increasing J, R_{moy} can reach asymptotically $H(X)$:

$$H(X) \leq R_{moy} < H(X) + \epsilon \qquad [1.78]$$

This result can be directly generalized to the case of sources with memory.

1.4.4.5. *Entropy rate*

We consider a stationary and discrete source X with entropy per symbol $H(X)$ Sh/symbol generating D_S symbols per second. We define the entropy rate D_I as follows:

$$D_I = H(X)D_S \qquad \text{in Sh/s} \qquad [1.79]$$

The binary data rate at the output of the coder D'_B is the product of the symbol rate D_S by the average number of bits per symbol R_{moy}:

$$D'_B = D_S.R_{moy} \qquad \text{in bit/s} \qquad [1.80]$$

At the output of the binary source encoder, we define $H'(X)$, the entropy per bit, as follows:

$$H'(X) = \frac{H(X)}{R_{moy}} \quad \text{in Sh/bit} \qquad [1.81]$$

The entropy rate D'_I at the output of the source coder is then given by:

$$D'_I = H'(X).D'_B = D_I \quad \text{in Sh/s} \qquad [1.82]$$

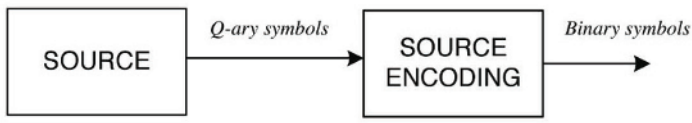
As expected, the entropy rate is not changed by the source coding. From the theorem of source coding, we have:

$$R_{moy} \geq H(X) \qquad [1.83]$$

Multiplying the two terms by D_S, we obtain:

$$D'_B \geq D_S.H(X) = D_I \qquad [1.84]$$

Consequently, D_I, the entropy rate of the source, is the lower bound on the binary data rate obtained after source coding. In case of equality, one bit will carry the quantity of information of one Shannon. If the redundancy of the output sequence is not zero, then one bit will carry less than one Shannon.



D_S	symb/s	$D'_B = D_S.R_{moy}$	bit/s
$H(X)$	sh/symb	$H'(X) = H(X) / R_{moy}$	sh/bit
$D_I = H(X).D_S$	sh/s	$D'_I = H'(X).D'_B = D_I$	sh/s

Figure 1.8. *Entropy rate*

1.5. Theorem for lossy source coding

1.5.1. *Introduction*

We will now study lossy channel coding. When the source generates a continuous and real signal, after sampling we have real samples. Compared to the previous section, the size of the state space is infinite and it is not possible to describe the source precisely using a finite number of bits. The aim of lossy source coding is to minimize a fidelity criterion such as the mean square error or a subjective quality under a binary rate constraint, or to minimize the binary rate under a given fidelity criterion. While mean square error is not always the best criterion, it is still the most used and we will consider it in this section. In the next chapter, we will study different practical solutions to implement lossy source coding such as scalar quantization with or without prediction, vector quantization, transform coding, etc.

In this section, we will introduce the concept of distortion and the distortion rate function. Then we will give the fundamental theorem for the lossy source coding.

1.5.2. *Definitions*

As previously mentioned, we will assume that the output of the source coder is directly connected to the input of the source decoder. The lossy source coder associates a binary word of length R bits with each sequence $\mathbf{x} \in \mathcal{X}$ and the source decoder associates a sequence $\tilde{\mathbf{x}} \in \tilde{\mathcal{X}}^N$ with each of the 2^R possible binary words. The sequence $\tilde{\mathbf{x}}$ is named as quantized or estimated sequence $\tilde{\mathbf{x}}$.

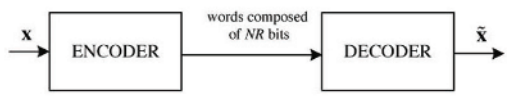


Figure 1.9. *Block diagram of the coder-decoder*

DEFINITION 1.1.– *The distortion per dimension between the sequences* $\mathbf{x}$ *and* $\tilde{\mathbf{x}}$ *of dimension* N *is defined by:*

$$\frac{1}{N}||\mathbf{x} - \tilde{\mathbf{x}}||^2 \qquad [1.85]$$

DEFINITION 1.2.– *The average distortion per dimension of the coder-decoder is defined by:*

$$D_N = \frac{1}{N} \int_{\mathbf{x}} ||\mathbf{x} - \tilde{\mathbf{x}}||^2 f(\mathbf{x}) d\mathbf{x} \qquad [1.86]$$

where $f(\mathbf{x})$ *is the density probability of* $\mathbf{x}$.

DEFINITION 1.3.– *A pair* (R, D) *is said to be achievable if there is a coder-decoder such that:*

$$\lim_{N \to \infty} D_N \leq D \qquad [1.87]$$

In his famous 1959 paper [SHA 59b], Shannon introduced the rate-distortion function which allows us to express the maximum theoretical rate under a given distortion constraint.

DEFINITION 1.4.– *For a given memoryless source, the rate distortion function* $R(D)$ *is defined as follows:*

$$R(D) = \min_{p(\tilde{x}|x)} \{I(X; \tilde{X}) | E[(X - \tilde{X})^2] \leq D\} \qquad [1.88]$$

1.5.3. *Lossly source coding theorem*

THEOREM 1.4.– The minimum number of bits per dimension R allowing to describe a sequence of real samples with a given average distortion D should be higher or equal to $R(D)$.

$$R \geq R(D) \qquad \text{in bits} \qquad [1.89]$$

The proof of this theorem [COV 91] is based on the jointly typical sequences.

If the source is Gaussian, it can be proved that the following relation is always true:

$$R(D) = \begin{cases} \frac{1}{2} \log_2 \frac{\sigma_x^2}{D} & 0 \leq D \leq \sigma_x^2 \\ 0 & D > \sigma^2 \end{cases} \qquad [1.90]$$

where σ_x^2 is the source variance. By introducing the distortion rate function $D(R)$, the relation [1.90] can also be written as:

$$D(R) = \sigma_x^2 2^{-2R} \qquad [1.91]$$

Like for the lossless source theorem, this theorem gives only a theoretical limit. For example, a simple uniform quantization does not generally allow us to reach this limit. Indeed, in the above theorem, it is assumed that the dimension N of the vector to be coded $\mathbf{x}$ tends to infinity. The rate-distortion can be generalized to the case of sources with memory.

In Figure 1.10, we have plotted the distortion-rate given by the relation [1.91] for $\sigma_x^2 = 1$.

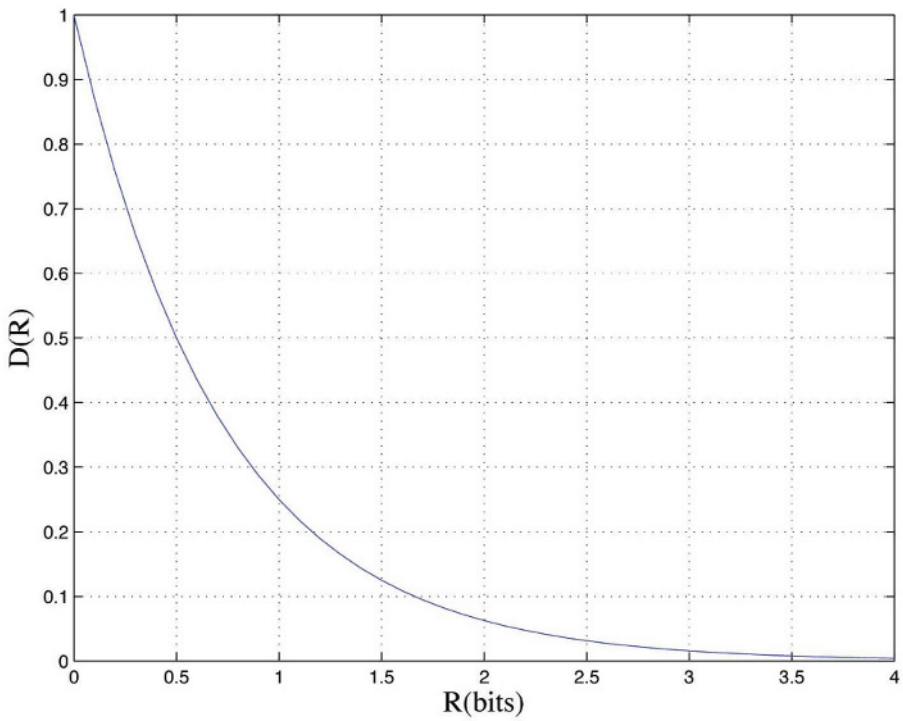


Figure 1.10. *Shannon distortion-rate for a Gaussian source of unitary variance*

In Figure 1.11, we have shown the optimal values y_i obtained using an uniform quantization (illustrated by "*") and a non-uniform quantization (illustrated by "o") for $L = 8$ and a Gaussian source.

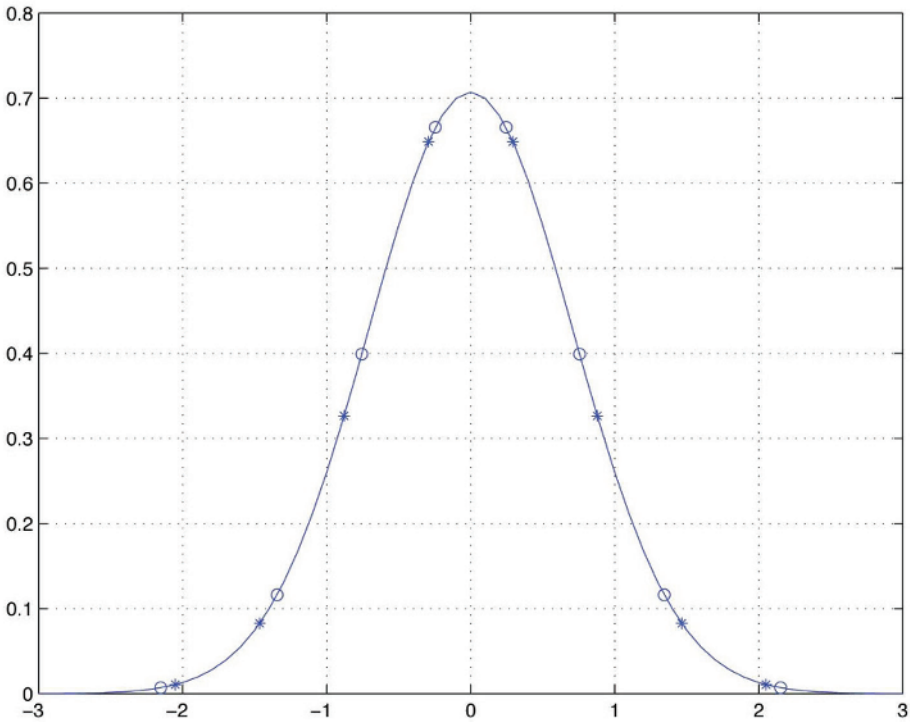


Figure 1.11. *Uniform and non-uniform quantization $L = 8$ for a Gaussian source with variance $\sigma_x = 1$*

In this simple case ($R = 3$ bits/sample and $\sigma_x = 1$), the average distortions of the uniform and non-uniform quantizations are -14.27 dB and -14.62 dB, respectively. The Shannon distortion-rate, in that case, is $10 \log_{10} 2^{-6} = -18.06$ dB. Since the probabilities associated with each interval are not the same, we can apply a lossy source coding after the quantization in order to reduce the binary data rate. This lossy source coding brings an additional gain of 2 dB. However, in order to reach the Shannon theoretical limit, we will have to perform vector quantization which means that we will have to combine several samples together. These different techniques will be developed in Chapter 2.

1.6. Transmission channel models

1.6.1. *Binary symmetric channel*

The binary symmetric channel is the simplest transmission channel since the input and the output of the channel is binary and it is defined using a single parameter.

This channel can be described using a graph as shown in Figure 1.12 on which we list the possible values of the input and output. The labels on the branches are the conditional probabilities $Pr(Y = y|X = x)$.

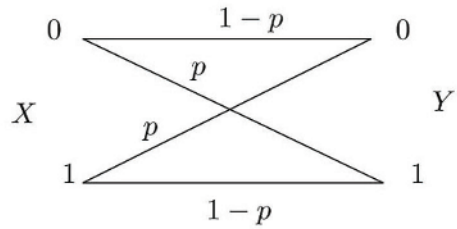


Figure 1.12. *Binary symmetric channel*

This channel is characterized by the four following conditional probabilities:

$$\begin{aligned} &Pr(Y = 0|X = 1) = Pr(Y = 1|X = 0) = p \\ &Pr(Y = 0|X = 0) = Pr(Y = 1|X = 1) = 1 - p \end{aligned} \qquad [1.92]$$

p is often called the inversion probability. We define also the probabilities associated with the input bits also called *a priori* probabilities $Pr(X = 0) = q$ and $Pr(X = 1) = 1 - q$.

The error probability for this channel can be easily calculated as follows:

$$\begin{aligned} P_e &= Pr(X = 0, Y = 1) + Pr(X = 1, Y = 0) \\ &= Pr(X = 0)Pr(Y = 1|X = 0) + Pr(X = 1)Pr(Y = 0|X = 1) \\ &= qp + (1 - q)p = p \end{aligned} \qquad [1.93]$$

The binary symmetric channel is memoryless: let $\mathbf{x}$ and $\mathbf{y}$ be respectively the input and output sequences composed of n bits: $\mathbf{x} = [x_0, x_1, \ldots, x_{n-1}]$, and $\mathbf{y} = [y_0, y_1, \ldots, y_{n-1}]$. Since the channel is memoryless, we have the following relation:

$$\begin{aligned} &Pr(Y_0 = y_0, \ldots, Y_{n-1} = y_{n-1} | X_0 = x_0, \ldots, X_{n-1} = x_{n-1}) \\ &\quad = \prod_{i=0}^{n-1} Pr(Y = y_i | X = x_i) \end{aligned}$$

The joint conditional probability is the product of the n conditional probabilities $Pr(Y = y_i | X = x_i)$.

Using the Bayes rule, we can compute the probabilities $Pr(X, Y)$, $Pr(Y)$ and $Pr(X|Y)$ from $Pr(Y|X)$ and $Pr(X)$ as given in Table 1.4.

$Pr(X,Y)$	$Y=0$	$Y=1$
$X=0$	$q(1-p)$	qp
$X=1$	$(1-q)p$	$(1-q)(1-p)$

$Pr(Y)$	
$Y=0$	$q(1-p)+(1-q)p$
$Y=1$	$qp+(1-q)(1-p)$

$Pr(X\|Y)$	$Y=0$	$Y=1$
$X=0$	$\frac{q(1-p)}{q(1-p)+(1-q)p}$	$\frac{qp}{qp+(1-q)(1-p)}$
$X=1$	$\frac{(1-q)p}{q(1-p)+(1-q)p}$	$\frac{(1-q)(1-p)}{qp+(1-q)(1-p)}$

Table 1.4. *Probabilities $Pr(X, Y)$, $Pr(Y)$ and $Pr(X|Y)$ for the binary symmetric channel*

From $Pr(Y|X)$, we can compute the conditional entropy $H(Y|X)$. We have:

$$\begin{aligned} H(Y|X) &= -p \log_2(p) - (1-p) \log_2(1-p) \\ &= H_2(p) \end{aligned} \qquad [1.94]$$

If $q = 0.5$, we also have $H(X|Y) = H_2(p)$.

In Figure 1.13, we have plotted the curves $H(X|Y) = f(q)$ for a binary symmetric channel with p =0.1, 0.2 and 0.5.

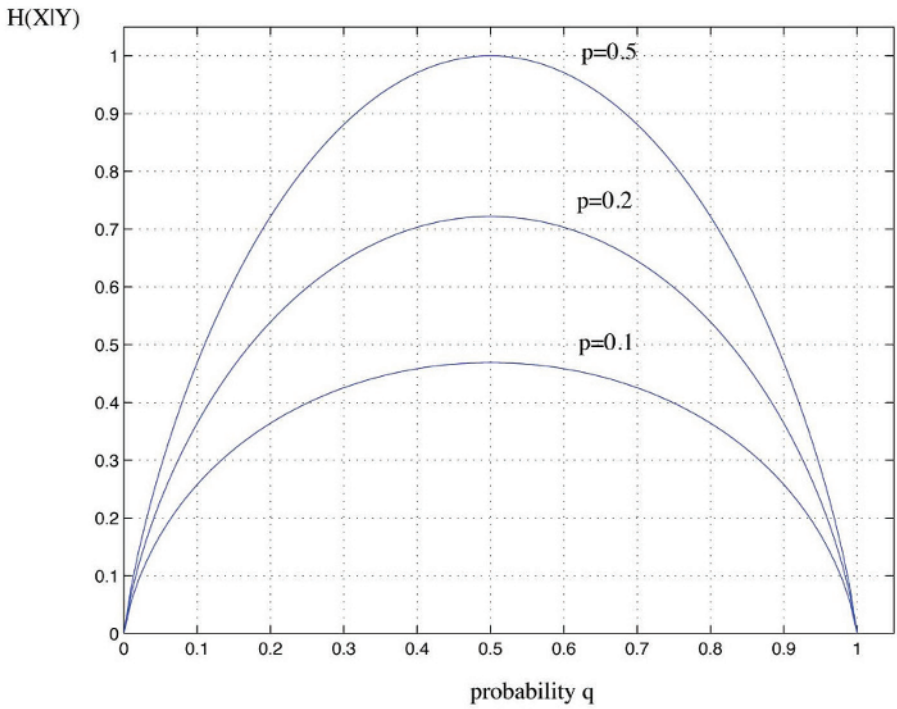


Figure 1.13. *Conditional entropy $H(X|Y)$ versus q and p*

1.6.2. *Discrete channels without memory*

The binary symmetric channel is a specific case of the class of the discrete channels without memory. The input symbols of the discrete channels are M-ary symbols and the output symbols are L-ary symbols. They are described using a set of LM conditional probabilities $Pr(Y = y_j|X = x_i) = p_{ij}$ and $Pr(X = x_i) = q_i$. As in the binary case, we can easily show that conditional probabilities satisfy the following relation:

$$\sum_{j=1}^{L} Pr(Y = y_j|X = x_i) = 1 \quad \text{for } i = 1, 2, \ldots, M \qquad [1.95]$$

These channels are described using a graph as shown in Figure 1.14.

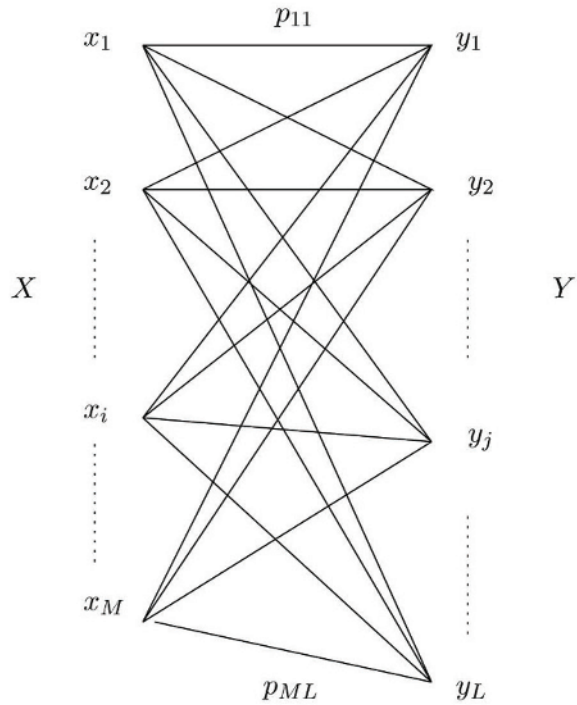


Figure 1.14. *Discrete channel without memory*

The symbol error probability P_e in this channel is given by:

$$\begin{aligned} P_e &= \sum_{i=1}^{M} \sum_{\substack{j=1 \\ j \neq i}}^{L} Pr(X = x_i, Y = y_j) \\ &= \sum_{i=1}^{M} Pr(X = x_i) \sum_{\substack{j=1 \\ j \neq i}}^{L} Pr(Y = y_j | X = x_i) \\ &= \sum_{i=1}^{M} Pr(X = x_i)(1 - p_{ii}) \end{aligned} \qquad [1.96]$$

1.6.3. *Binary erasure channel*

The binary erasure channel, introduced by Elias in 1955 [ELI 55], is a channel in which some bits can be lost or erased. Compared to the binary symmetric channel, we add an event $Y = \epsilon$ corresponding to the case where a transmitted bit has been erased. This channel is characterized by the following conditional probabilities:

$$\begin{aligned} Pr(Y = 0|X = 0) &= Pr(Y = 1|X = 1) = 1 - p \\ Pr(Y = \epsilon|X = 0) &= Pr(Y = \epsilon|X = 1) = p \\ Pr(Y = 0|X = 1) &= Pr(Y = 1|X = 0) = 0 \end{aligned} \quad [1.97]$$

p is the erasure probability. This transmission channel model is often used to model the packet loss in high level communication protocols. This channel is described by the diagram in Figure 1.15.

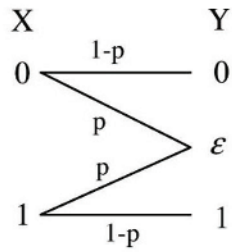


Figure 1.15. *Erasure channel*

Using the Bayes rule, we can compute $Pr(X, Y)$, $Pr(Y)$ and $Pr(X|Y)$ from $Pr(Y|X)$ and $Pr(X)$ as shown in Table 1.5.

The conditional entropy $H(X|Y)$ is equal to $pH_2(q)$.

1.6.4. *Additive white Gaussian noise channel*

The additive white Gaussian noise (AWGN) channel is the most important channel. It allows us to model the transmission channel for which the predominant noise is the thermal noise. We assume that the bandwidth of transmitted baseband signal is B and that the noise added to the transmitted

signal is stationary, white, Gaussian and with a unilateral power density spectrum N_0. The noise power N is equal to:

$$N = N_0 B \qquad [1.98]$$

$Pr(X,Y)$	$Y=0$	$Y=\epsilon$	$Y=1$
$X=0$	$q(1-p)$	qp	0
$X=1$	0	$(1-q)p$	$(1-q)(1-p)$

$Pr(Y)$	
$Y=0$	$q(1-p)$
$Y=\epsilon$	p
$Y=1$	$qp+(1-q)(1-p)$

$Pr(X\|Y)$	$Y=0$	$Y=\epsilon$	$Y=1$
$X=0$	1	q	0
$X=1$	0	$1-q$	1

Table 1.5. *Probabilities $Pr(X,Y)$, $Pr(Y)$ and $Pr(X|Y)$ for the erasure channel*

The sampling theorem says that $2BT$ samples are enough to represent a bandlimited signal ($f_{max} = B$) for a duration T. We will show in Volume 2 of this book [PIS 15] that the optimal demodulator is composed of a matched filter that will limit the noise bandwidth. After matched filtering and sampling, the relation between the input symbol s_i drawn from a discrete alphabet and the output symbol y_i at time i can be written for the AWGN channel as follows:

$$y_i = x_i + n_i \qquad [1.99]$$

n_i is the white noise sample with a centered Gaussian probability density:

$$p(n_i) = \frac{1}{\sqrt{\pi N_0}} \exp\left(-\frac{n_i^2}{N_0}\right) \qquad [1.100]$$

The variance σ_n^2 of the noise sample n_i is equal to:

$$\sigma_n^2 = \frac{N}{2B} = \frac{N_0}{2}$$

Consequently, the probability density of y_i conditionally to x_i is:

$$p(y_i|x_i) = \frac{1}{\sqrt{\pi N_0}} \exp\left\{-\frac{(y_i - x_i)^2}{N_0}\right\} \qquad [1.101]$$

1.7. Capacity of a transmission channel

1.7.1. *Introduction*

We would like to solve the following problem: let us assume that we transmit equiprobable bits $Pr(X = 0) = Pr(X = 1) = \frac{1}{2}$ with a binary rate of 1000 bits per second through a binary symmetric channel with parameter $p = 0.1$. What is the maximum information rate that can be transmitted? We can imagine that this rate is 900 Sh/s by substracting the number of errors per second. However, this is a not a good idea since we do not know the error positions. For example, when $p = 0.5$, we have on average 500 errors per second and no information is transmitted. In the following, we will answer this question.

1.7.2. *Capacity of a transmission channel*

We denote by X and Y the random variables associated with the input and the output of the channel, respectively.

DEFINITION 1.5.– *We define the capacity of a transmission channel as follows:*

$$C = \max I(X;Y) \qquad [1.102]$$

The capacity of a transmission channel is the maximum of average mutual information. The maximization is performed over all the possible sources. If the channel is memoryless, the maximization is done over the set of all possible distributions $p(x)$ of the input symbols x.

We first consider that the transmission channel is noiseless. In that case, the capacity is the average quantity of information that the input symbols can carry.

The capacity C is defined in Shannon/symbol. It is also possible to express the capacity in Shannon/second (we will refer to capacity per time unit instead of capacity per symbol). To distinguish it from the capacity per symbol, we will denote it by C'. We have:

$$C' = C \times D_s \quad \text{with} \quad D_s \quad \text{symbol rate of the source} \qquad [1.103]$$

When the channel is noiseless, the capacity C is equal to $\log_2 Q$. Indeed, the average quantity of information is maximized when the source entropy is maximized, that is to say, when all the Q-ary input symbols are equiprobable. Then we have:

$$C = H_{MAX}(X) = \log_2 Q \qquad [1.104]$$

When the channel is noisy, we have $C < H_{MAX}(X)$. In order to compute the capacity of a transmission channel, we have to calculate the average quantity of information that is lost in the channel. We have seen previously that $H(X|Y)$ is the measure of the residual uncertainty on X knowing Y. In order to perform a good transmission, it is desirable that this quantity is equal to zero or negligible.

$H(X|Y)$ corresponds to the average quantity of information lost in the channel. When the channel is noiseless, we have $H(X|Y) = H(X|X) = 0$ and consequently $C = H_{MAX}(X)$ corresponding to the relation [1.104].

When the channel is so noisy that X and Y are independent, we have $H(X|Y) = H(X)$. In that case, the capacity of information is zero, $C = 0$. These two cases are illustrated in Figures 1.16 and 1.17.

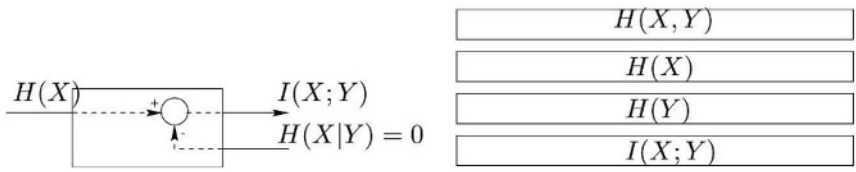


Figure 1.16. *Case* $C = H_{MAX}(X)$

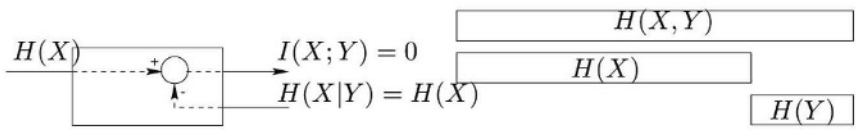


Figure 1.17. *Case* $C = 0$

When the source entropy is equal to $H_{MAX}(X)$, $H(X|Y)$ is only related to the transmission channel. If $H(X|Y)$ is non-negligible (case of a noisy

channel), it would not be possible to perform a transmission without errors by just connecting the source to the input of the transmission channel. We have to add an element called channel coder between the source and the transmission channel. Figure 1.18 illustrates the new communication chain including a channel coder, the noisy channel and the channel decoder.

Figure 1.18. *Communication system with channel coding*

For this new system, we can define the average mutual information $I(U;V) = H(U) - H(U|V)$. The role of channel coding is to make the average quantity of information $H(U|V)$ as low as desired. It is then possible to transmit through the noisy channel an average quantity of information $H(U)$ with the desired quality criterion. Of course, we have $H(U) < H(X)$ due to the redundancy added by the channel coding.

We will now state the fundamental theorem of channel coding.

1.7.3. *Fundamental theorem of channel coding*

There is a channel coding guaranteeing a communication with an error rate as low as desired under the condition that the average quantity of information entering the block channel coder-channel-channel decoder is less than the capacity C of the channel [SHA 48]:

$$H(U) < C \qquad [1.105]$$

Thus, the capacity of a transmission channel as defined in equation [1.102] is equal to the highest number of information bits that can be transmitted through the channel with an error rate as low as desired.

Multiplying the two terms of this inequality by D_s (the data rate of the source), we obtain an inequality between the maximum binary information rate D_b and the capacity per time unit C':

$$D_b < C' \qquad [1.106]$$

The proof of the fundamental theorem of channel coding is based on the principle of random coding and the properties of jointly typical sequences of couples. Shannon proposed to use the following channel coder and channel decoder to prove the theorem: the codewords associated with the information words are randomly generated among a set of 2^{NR} codewords. The decoding stage should verify if there exists a unique codeword jointly typical with the received word. If it exists, then the decoding is successful. In the opposite case (no codeword or many codewords satisfy the test), the decoding is a failure. Since the probability that another codeword is jointly typical with the received word is equal to $2^{-N(I(X;Y))}$, if we limit the number of codewords to $2^{N(I(X;Y))}$, we can guarantee with a high probability that there will be no confusion between the transmitted codeword and all other codewords. We will see later that the optimal decoding is to choose the closest codeword according to the Euclidian distance. However, the decoding scheme proposed by Shannon facilitates proof of the theorem.

The work of Shannon does not give us a practical solution (i.e. with a reasonable complexity) for the realization of the channel coder and the channel decoder. Since 1948, researchers have proposed practical error correcting codes and decoding algorithms to approach this theoretical limit. It is only in 1993, with the discovery of the so-called turbo codes [BER 93] and the rediscovery of the LDPC codes in 1995 [MAC 99], that it becomes possible to reach this limit within 1 dB.

1.7.4. *Capacity of the binary symmetric channel*

We have seen that the binary symmetric channel is described by the probability of error p. Since $H(Y|X) = H_2(p)$, the average mutual information $I(X;Y)$ of the binary symmetric channel is given by:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(Y) - H_2(p) \end{aligned} \qquad [1.107]$$

Since $H_2(p)$ is independent of q, in order to maximize $I(X;Y)$, it is necessary to maximize $H(Y)$. We have seen in equation [1.41] that to maximize $H(Y)$, we should have $Pr(Y = 0) = Pr(Y = 1) = 1/2$ i.e.

$Pr(X = 0) = Pr(X = 1) = q = 1/2$. Then the capacity of the binary symmetric channel is given by:

$$C = 1 - H_2(p) = 1 + p\log_2(p) + (1-p)\log_2(1-p) \qquad [1.108]$$

In Figure 1.19, we plot the curves $I(X;Y) = f(q)$ for a binary symmetric channel with $p = 0.0,\ 0.1,\ 0.2$ and 0.5. We can see on this figure that indeed the average mutual information is maximized when $Pr(X = 0) = Pr(X = 1) = q = 1/2$.

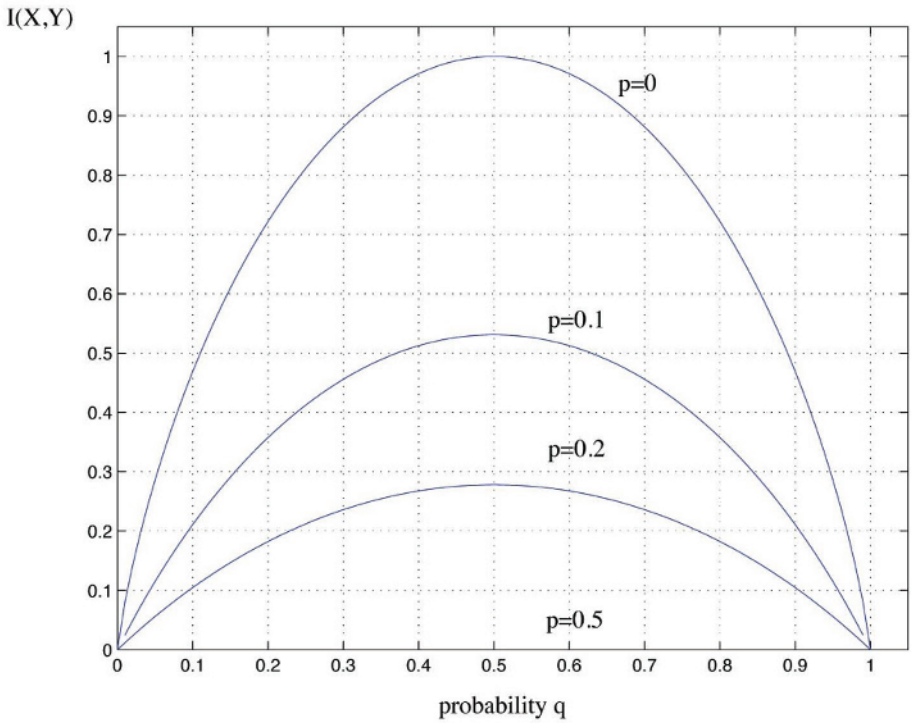


Figure 1.19. *Mutual information $I(X;Y)$ versus q and p*

In Figure 1.20, we plot the curve $C = f(p)$ for a binary symmetric channel with $q = 0.5$. As expected, the capacity is maximum when $p = 0$ and zero when $p = 0.5$.

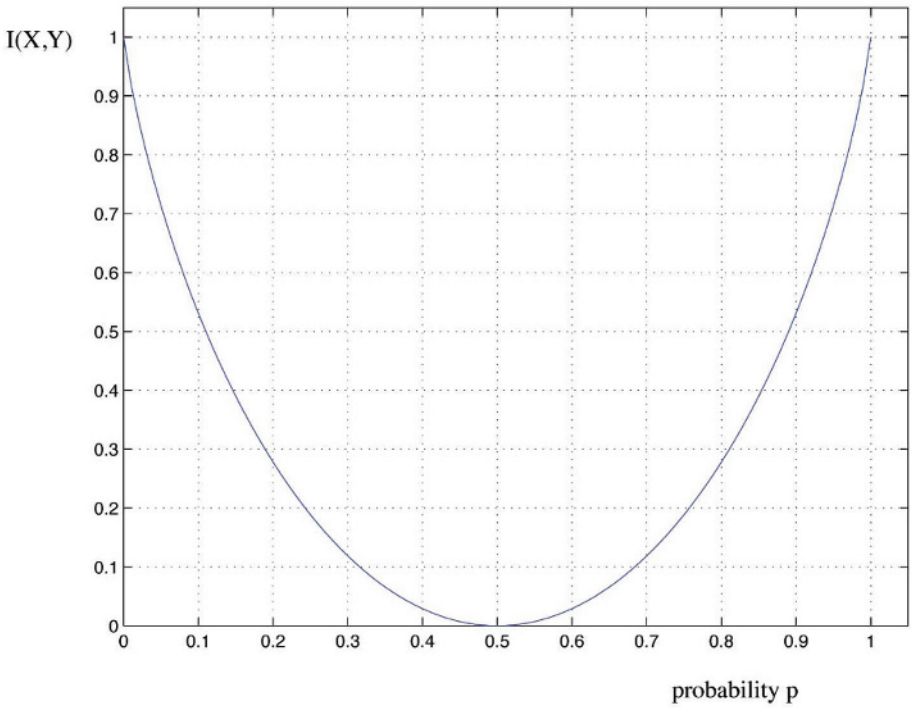


Figure 1.20. *Capacity of the binary symmetric channel versus* p

1.7.5. *Capacity of erasure channel*

For the erasure channel, we have seen that the conditional entropy $H(X|Y)$ is equal to $pH_2(q)$ and the average mutual information $I(X;Y)$ is the following:

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H_2(q) - pH_2(q) \\ &= (1-p)H_2(q) \end{aligned} \qquad [1.109]$$

The average mutual information is maximum for $q = 0.5$ i.e. $H_2(q) = 1$. Consequently, the capacity of this channel is:

$$C = 1 - p \qquad [1.110]$$

1.7.6. *Capacity of additive white Gaussian noise channel*

To determine the capacity of AWGN channel, we will first compute the average mutual information $I(X;Y)$.

We have introduced in section 1.6.4 the relation $y_i = x_i + n_i$ between the samples y_i at the output of the AWGN channel and the input samples x_i and noise samples n_i. The samples x_i, y_i and n_i can be seen as realizations of three random variables X, Y and Z. Consequently, the average mutual information can be written as follows:

$$I(X;Y) = \int\int p(x,y)\log_2 \frac{p(y|x)}{p(y)}dxdy \qquad [1.111]$$

$$\begin{aligned} &= H_D(Y) - H_D(Y|X) \\ &= H_D(Y) - H_D(X+Z|X) \\ &= H_D(Y) - H_D(Z|X) \\ &= H_D(Y) - H_D(Z) \end{aligned} \qquad [1.112]$$

since Z is the random variable associated with the noise and is independent of X.

In section 1.3.6, we have computed the differential entropy $H_D(X)$ of X, a Gaussian random variable with variance σ_x^2. From equation [1.55], we have:

$$\begin{aligned} H_D(X) &= \frac{1}{2}\log_2 2\pi e\sigma_x^2 \\ &= \frac{1}{2\ln 2} + \log_2\left(\sqrt{2\pi}\sigma_x\right) \end{aligned} \qquad [1.113]$$

It is possible to prove that the maximum of $I(X;Y)$ is reached when the density probability of X is Gaussian, centered, with variance σ_x^2. The noise variance of Z is equal to $\sigma_n^2 = \frac{N_0}{2}$.

Let us compute the variance of Y. We have:

$$\begin{aligned} E[Y^2] &= E[X+Z]^2 = E[X]^2 + 2E[XZ] + E[Z]^2 = E[X]^2 + E[Z]^2 \\ &= \sigma_x^2 + \frac{N_0}{2} \end{aligned} \qquad [1.114]$$

From [1.111] we can derive the capacity of the AWGN channel as:

$$\begin{aligned} C &= \max I(X;Y) \\ &= \log_2 \sqrt{\pi(2\sigma_x^2 + N_0)} - \log_2 \sqrt{\pi N_0} \\ &= \frac{1}{2}\log_2\left(1 + \frac{2\sigma_x^2}{N_0}\right) \qquad \text{in Shannon/symbol} \end{aligned} \qquad [1.115]$$

It should be noted that the capacity of the AWGN channel has been computed here under an average power constraint available at the transmitter. Other constraints, such as a peak power constraint, will give a different expression of the capacity.

When the noise is not white, the capacity will be obtained using the waterfilling technique that generalized the relation [1.115].

Let us introduce P as the average power of the signal $x(t)$. When considering a sampling frequency of $2B$, we have $2BT$ samples for a duration T. Then the power is derived as follows:

$$\begin{aligned} P &= \frac{1}{T}\int_0^T E[x^2(t)]dt \\ &= \frac{1}{T}\sum_{i=1}^{2BT} E[x_i^2] \\ &= \frac{1}{T}\sum_{i=1}^{2BT} \sigma_x^2 \\ &= 2B\sigma_x^2 \end{aligned} \qquad [1.116]$$

We finally obtain from [1.115], the classical relation of the capacity of the AWGN channel:

$$C = \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right) \qquad \text{in Shannon/symbol} \qquad [1.117]$$

The capacity C is the capacity per real symbol i.e. per dimension. Some authors expressed it in Shannon/dimension.

Figure 1.21 gives the curve of the capacity C of the AWGN channel versus the signal to noise ratio $SNR = \frac{P}{N}$. We can observe that for $SNR > 5dB$, the capacity C is well approximated by the linear function $C \approx \frac{1}{2}\log_2(SNR)$.

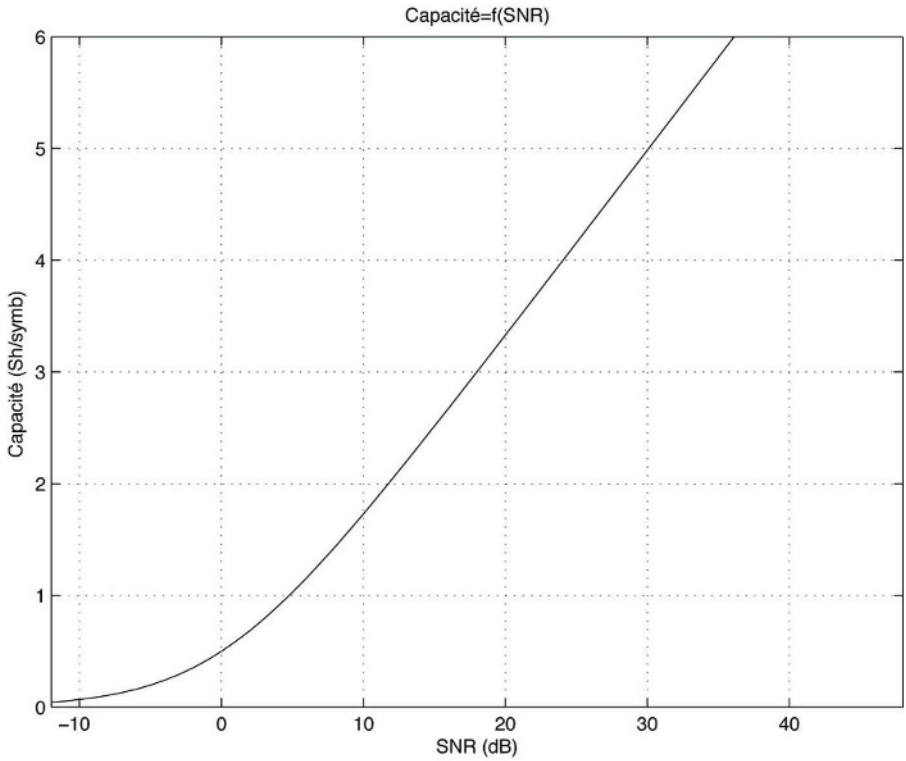


Figure 1.21. *Capacity of the additive white Gaussian noise channel*

When multiplying [1.117] by the sampling frequency $2B$, we finally obtain the expression of the capacity per time unit:

$$C' = B\log_2\left(1 + \frac{P}{N}\right) \qquad \text{in Shannon/s} \qquad [1.118]$$

where $N = BN_0$ the noise power.

When the signal to noise ratio is high, we can approximate the capacity of the AWGN channel as follows:

$$C' = B\log_2\left(1+\frac{P}{N}\right) \approx B\frac{\log_{10}(P/N)}{\log_{10}2} \approx \frac{B}{3}(P/N)_{dB}$$

1.7.7. *Graphical representation*

It is also possible to geometrically demonstrate that in order to ensure a transmission without error, the average quantity of information $H(U)$ should not be higher than $\frac{1}{2}\log_2\left(1+\frac{2\sigma_x^2}{\sigma_n^2}\right)$.

Let us recall the relation between the transmitted vector $\mathbf{x}$ and the received vector $\mathbf{y}$ of dimension D.

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \qquad [1.119]$$

$\mathbf{n} = (n_1, n_2, \ldots, n_D)$ is the noise vector composed of D independent Gaussian samples of variance $\sigma_n^2 = \frac{N_0}{2}$. The probability density of the vector $\mathbf{n}$ can be mathematically written as:

$$p(\mathbf{n}) = \frac{1}{(2\pi\sigma_n^2)^{D/2}}\exp\left(-\frac{\sum_{i=1}^{D} n_i^2}{2\sigma_n^2}\right) \qquad [1.120]$$

For D tending to infinity, we have shown in Appendix A that the noise vector[3] is concentrated at the surface of a D dimensions sphere with radius $\sqrt{D\sigma_n^2}$.

The transmitted vector $\mathbf{x}$ is randomly generated with a variance σ_x^2 per dimension and a Gaussian probability distribution in order to maximize the capacity:

$$p(\mathbf{x}) = \frac{1}{(2\pi\sigma_x^2)^{D/2}}\exp\left(-\frac{\sum_{i=1}^{D} x_i^2}{2\sigma_x^2}\right) \qquad [1.121]$$

3 norm of the noise vector = $\sqrt{\sum_{i=1}^{D} n_i^2}$.

For the same reason as above, the vector $\mathbf{x}$ is concentrated at the surface of a sphere of radius $\sqrt{D.\sigma_x^2}$. Since the power of the received signal is the sum $\sigma_x^2 + \sigma_n^2$, the vector associated with the received signal is on the surface of the D dimensions sphere with radius $\sqrt{D(\sigma_x^2 + \sigma_n^2)}$.

We wish to perform a transmission without error of an average quantity of information $H(U) = \frac{1}{D}\log_2 M$, where $M = 2^{DH(U)}$ is the number of possible transmitted signals. To meet this goal, all the spheres of noise should be disjoint. Consequently, the volume of the M spheres of noise must be less than the volume of the sphere of radius $\sqrt{D(\sigma_x^2 + \sigma_n^2)}$. Let us recall that the volume of a D dimensions sphere with radius r is given by:

$$V(r, D) = \frac{\pi^{D/2}}{\Gamma(D/2+1)} r^D \qquad [1.122]$$

where $\Gamma(.)$ is the factorial function[4].

As a consequence, we should have:

$$\text{number of distinguishable signals} = M \leq \frac{V(\sqrt{D(\sigma_x^2 + \sigma_n^2)}, D)}{V(\sqrt{D.\sigma_n^2}, D)} \qquad [1.123]$$

This idea is illustrated in Figure 1.22.

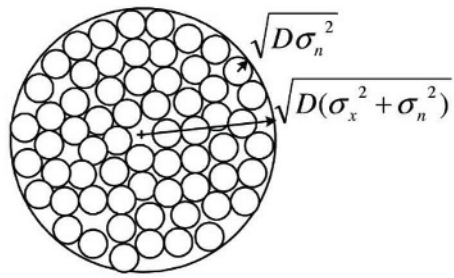


Figure 1.22. *Spheres of noise illustration*

4 the factorial function $\Gamma(.)$ is defined as follows:
– $\Gamma(n) = (n-1)!$ with $n \in \mathbb{N}^*$.
– $\Gamma(n+1/2) = \frac{(2n)!}{2^{2n}.n!}.\sqrt{\pi}$ with $n \in \mathbb{N}^*$.
– $\Gamma(1/2) = \sqrt{\pi}$.

The expression can be simplified as follows:

$$M \leq \frac{(D(\sigma_x^2 + \sigma_n^2))^{D/2}}{(D.\sigma_n^2)^{D/2}} \qquad [1.124]$$

Then we obtain the following inequality:

$$M \leq \left(\frac{\sigma_x^2 + \sigma_n^2}{\sigma_n^2} \right)^{D/2} \qquad [1.125]$$

This inequality can be rewritten as:

$$H(U) \leq \frac{1}{2} \log_2 \left(1 + \frac{\sigma_x^2}{\sigma_n^2} \right) \qquad [1.126]$$

Finally, since the capacity C is the highest possible value of the average information quantity $H(U)$, we find again the formula of the capacity of the AWGN channel:

$$C = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_x^2}{\sigma_n^2} \right) \qquad \text{in Sh/dim} \qquad [1.127]$$

When the bandwidth is limited, the dimension D is equal to $D = 2BT$ with B bandwidth of the system and T duration of the transmission. The noise power is equal to $N = N_0 B = 2B\sigma_n^2$ and the average power of the signal X is equal to $P = 2B\sigma_x^2$. Then the capacity C' per time unit is given by:

$$\begin{aligned} C' &= B \log_2 \left(1 + \frac{P}{N} \right) \\ &= B \log_2 \left(1 + \frac{P}{N_0 B} \right) \qquad \text{in Sh/sec} \end{aligned} \qquad [1.128]$$

Let E_b be the average energy per information bit and E_s be the average energy per symbol. We have:

$$P = \frac{E_s}{T_s} = \frac{E_b}{T_b} \qquad [1.129]$$

where T_s and T_b are the symbol and information bit duration respectively (assuming a M-ary modulation $M = 2^g$ and a code rate R we have $T_s = gRT_b$).

We have the following relation between the signal to noise ratio P/N and the ratio E_b/N_0:

$$\frac{P}{N} = \frac{E_s}{N_0 B T_s} = \frac{E_b}{N_0 B T_b} = \eta \frac{E_b}{N_0} \qquad [1.130]$$

η is the spectral efficiency in bits/sec/Hz:

$$\eta = \frac{D_b}{B} \quad \text{with} \quad D_b = \frac{1}{T_b} \quad \text{binary information rate} \qquad [1.131]$$

The spectral efficiency η is maximum when the bandwidth is minimum i.e. $B_{min} = 1/T_s$. We have:

$$\eta_{max} = \frac{1}{T_b B_{min}} = \frac{T_s}{T_b} \qquad [1.132]$$

When considering that the binary rate is equal to the channel capacity ($D_b = C'$), the spectral efficiency η_{max} can be also written as follows:

$$\eta_{max} = \frac{C'}{B} = \log_2\left(1 + \eta_{max}\frac{E_b}{N_0}\right) \qquad \text{in bits/sec/Hz} \qquad [1.133]$$

This equation can be also rewritten as:

$$\frac{E_b}{N_0} = \frac{2^{\eta_{max}} - 1}{\eta_{max}} \qquad [1.134]$$

The minimum value of E_b/N_0 for a communication without error is obtained when the maximum spectral efficiency tends to zero (the bandwidth tends to infinity). We then obtain:

$$\lim_{\eta_{max} \to 0} \frac{E_b}{N_0} = \ln 2 \quad \text{or} \quad \left.\frac{E_b}{N_0}\right|_{dB} = -1.59 \quad \text{dB} \qquad [1.135]$$

Figure 1.23 shows the curve of the maximum spectral efficiency versus E_b/N_0. We have also plotted the required ratio E_b/N_0 considering a bit error rate of 10^{-5} of systems such as digital modulation BPSK and QPSK without coding. These modulations will be studied in Volume 2 of this book [PIS 15]. The performance of these communication systems are at 9.5 dB and 7.75 dB, respectively, from the Shannon limit. Adding a convolutional code (133,171) of rate $R = 1/2$ to a system using BPSK modulation gives a 5.1 dB gain compared to a system without coding. The concatenation of this convolutional code and a Reed–Solomon code (255,223) proposed by Forney [FOR 66] allow us to be 2.5 dB from the Shannon limit. The last point is relative to the performance obtained using turbo codes *et al.* [BER 93]. We will study these error correcting codes in Chapters 3, 4 and 5.

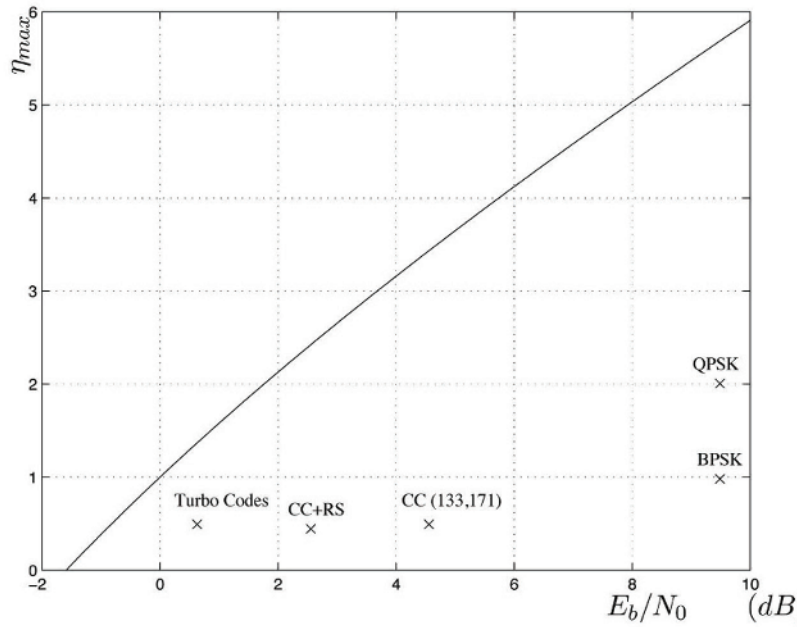


Figure 1.23. *Maximum spectral efficiency of an additive white Gaussian noise channel*

Figure 1.24 shows the maximum spectral efficiency for different digital modulations. Depending on the number of possible states M of these modulations, the spectral efficiency is always limited by $\log_2(M)$. These curves can be obtained numerically from the mathematical expression of the

average mutual information given by equation [1.111] by taking into account the distribution of y that is no more a Gaussian distribution but will depend on the considered modulation.

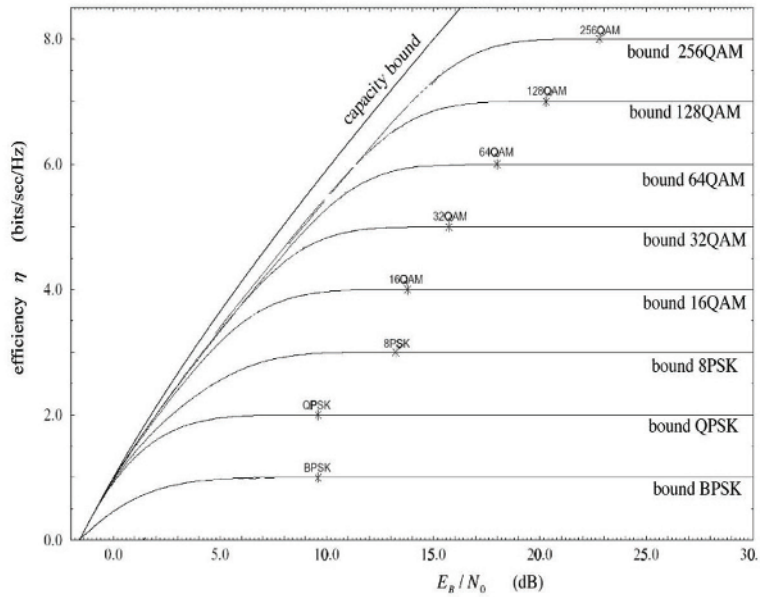


Figure 1.24. *Spectral efficiency versus* E_b/N_0

1.8. Exercises

1.8.1. *Exercise 1: calculation of the entropy for a discrete channel*

A source X can generate three different symbols a_1, a_2 and a_3 with the associated probabilities $\Pr(X = a_1) = 0.25$, $\Pr(X = a_2) = 0.5$ and $\Pr(X = a_3) = 0.25$

This source is connected to a discrete channel defined by the following conditional probabilities:

$$p_{ij} = \Pr(Y = a_j \,|X = a_i) = 0.05 \;\forall i, j \in \{1, 2, 3\} \;\; with \; i \neq j$$

$$p_{ii} = \Pr(Y = a_i \,|X = a_i) = 0.9 \;\forall i \in \{1, 2, 3\}$$

p_{ij} is the probability to receive a_j when we transmit a_i

1) Draw this transmission channel graphically.

2) Compute the probabilities $\Pr(Y = a_j)$ for $j \in \{1, 2, 3\}$ and the conditional probabilities $\Pr(X = a_i \,|Y = a_j)$.

3) Compute the entropies $H(X)$ and $H(Y)$, the joint entropy $H(X, Y)$ and the conditional entropy $H(Y|X)$.

4) Check that $H(X, Y) = H(Y|X) + H(X) = H(X|Y) + H(Y)$.

1.8.2. *Exercise 2: computation of the mutual information [BAT 97]*

We draw four cards randomly in a standard deck of 32 cards (4 colors: heart, spade, diamond, club – 8 values: 7, 8, 9, 10, Jack, Queen, King and Ace).

Let us define the following events:

– E1: the event "the hand contains no 7, 8, 9 and 10";

– E2: the event "the hand contains no Jack, Queen and King";

– E3: the event "the hand contains four cards of the same values".

1) Compute the information $h(E1)$, $h(E2)$ and $h(E3)$.

2) Compute the mutual information $i(E1; E2)$, $i(E1; E3)$

1.8.3. *Exercise 3: capacity of the additive white Gaussian noise channel*

Determine the capacity of the AWGN channel assuming that the signal power is 10 W, the bandwidth is 1 MHz and the noise spectrum density $\frac{1}{2}N_0$ is equal to 10^{-9} W/Hz

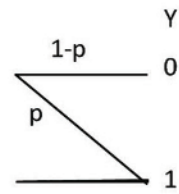
1.8.4. *Exercise 4: binary symmetric channel*

We consider a binary symmetric channel. The source X generates equiprobable bits $p(X = 0) = p(X = 1) = 0.5$.

Determine $H(Y)$,$H(X|Y)$ and $I(X; Y)$ in function of p. Achieve the numerical application for $p = 0.11$.

1.8.5. *Exercise 5: Z channel*

Let us define the Z channel as follows:



The source X generates equiprobable bits $p(X = 0) = p(X = 1) = 0.5$.

1) Determine $p(Y = y_i)$, $p(X = x_i, Y = y_j)$, $p(X = x_i|Y = y_j)$ in function of p.

2) Determine $H(X|Y)$ and $I(X;Y)$ in function of p. Achieve the numerical application for $p = 0.5$.

1.8.6. *Exercise 6: discrete channel*

Let us consider the discrete channel with input X and output Y with state space $A = \{0, 1, 2, 3, 4\}$ and conditional probabilities as follows:

$$Pr(Y = y_j|X = x_i) = \begin{cases} 0,5 & \text{if} \quad j = i \pm 1 \text{mod} 5 \\ 0 & \text{else} \end{cases}$$

1) Draw the channel graphically.

2) Compute $H(X|Y)$ and $I(X;Y)$ assuming that the input symbols are equiprobable.

3) Show that it is possible to transmit at the rate 1 bit/symb with a zero error probability.

4) Is it possible to increase the rate by grouping the symbols two by two?