HARDWARE AND DEVICE-TO-DEVICE COMMUNICATION SECURITY

Notes about that

Fabio Lorenzato

Contents

Part I

Wireless

Chapter 1

Digital Communication

This first section is all about how to convert and transmit some signal.

1.1 Introduction

The goal of communication is to transmit some kind of data form a sender to a receiver. In order to do so, the physical layer defines the means of transmitting a stream of **raw bits** over a physical data link, which connects those two nodes.
Data is transmitted in the form of **signals**, which are a physical representation of the data. The signal is transmitted over a **channel**, which is the transmission medium that connects the sender and receiver. This can be both wired or wireless.
Whereas with wired channels, checking the device connected to the channel is easier to implement, with wireless ones security is a major when travelling in the channel. This is for may reasons:

- No inherent protection is applied to the channel(it is replaced by a logical association)

  sending and receiving messages do not need physical access to the network infrastructure

- the communication is in broadcast, which is intrinsic of radio nature.

  Transmission can be overheard by anyone in range(which can be quite big, depending on the situation), and anyone can generate a transmission, for example by jamming nearby transmissions.

As a result:

- Eavesdropping is easy
- Injecting fake messages into the communication in easy
- replaying previously recorded messages is easy(*meaconing*). This is actually very dangerous for gps positioning, so it is also a security concern.
- illegitimate access to the network and its services is easy
- Denial of service attacks are easy, achieved by jamming the channel.

1.2 Digital Communication System

The digital communication system in characterized by three sections:

- the **user section**, which consist in the transmitter and the receiver, that want to communicate.
- the **interface section**, which is the interface to conveying the signal from the user to the analog channel. It also transforms bits to analog signal, compressing and encoding them, also associating bits to signal waveforms, to transform bits to analog signal.
- the **channel section**, which is the physical medium, that can only propagate analog waveforms. In the end, we want to transmit digital signal but we are forced to use analog ones.

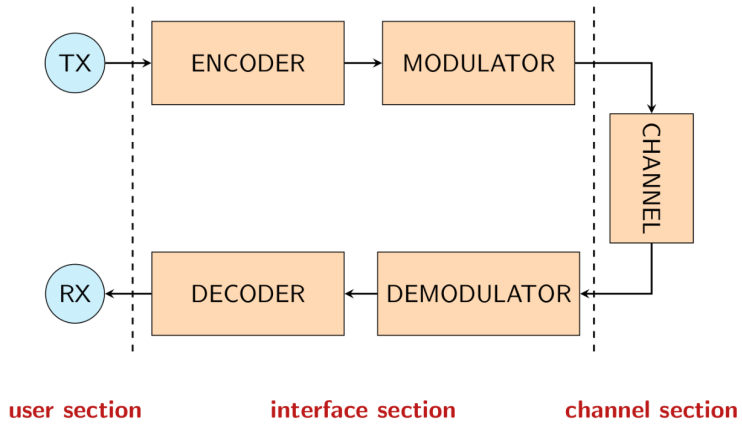

Figure 1.1: Digital Communication System

1.2.1 The transmitter chain

The transmitter chain is the part of the system that takes the digital signal, or an analog one converted to digital, and converts it to an analog signal, that can be transmitted over the channel.
It is basically composed by two parts. The first one being an **encoder**, which can limit the amount of bits transmitted(*source encoding*), and/or make the transmitted sequence more robust to errors(*channel encoding*).
The second one is the **modulator**, which is the part of the system that takes the digital signal and converts it to an analog one to transmit it over the channel.

1.2.2 The channel

The channel is the physical medium that transfers bits from interface to interface, from the sender to the receiver. Its operation is affected by different types of disturbances such as:

- frequency-domain distortion
- wireless fading

- additive noise
- impulsive noise
- interference from other frequency channels (interchannel interference)
- interference from the same frequency channel (cochannel interference)
- Intentional interference

1.2.3 The receiver chain

The receiver chain is the part of the system that takes the analog signal from the channel and converts it to a digital signal, that can be processed by the user.
It is composed by the dual counterpart of the transmitter chain, the **demodulator** and the **decoder**.
The demodulator takes the analog signal and converts it to a sequence of samples that can be processed by the decoder.
The decoder takes the sequence of samples and converts it to a digital signal. It implements *channel decoding*, to correct errors, and *source decoding*, to recover the original message.

1.3 Signal representation and Processing

> A **signal** is a (mathematical) function that conveys information about a phenomenon.

Basically, any quantity that varies over space or time can be used to represent a informations, allowing to describe the evolution of physical quantities over time(voltages, currents, ...).
Its mathematical representation is therefore a function of real variable (time) taking real or complex(more than one) values.
We will be mostly focused on Electromagnetic Signals (e.g. voltage), but the general concepts can be applied to any kind of signal

1.3.1 Energy of a signal

The energy of a signal is the integral of the squared modulus of the signal itself.

$$E(x) = \int_{-\infty}^{\infty} |x(t)|^2 dt \tag{1.1}$$

As we can see , the energy is a scalar value, and the whole function is made positive by the squared modulus.
A signal with a very large amplitude, over time, will have a very high energy, while a signal which assumes values close to zero will have a very low energy, being a very weak signal.
Furthermore, we can note that the more distant is the signal from the origin, the larger the energy.

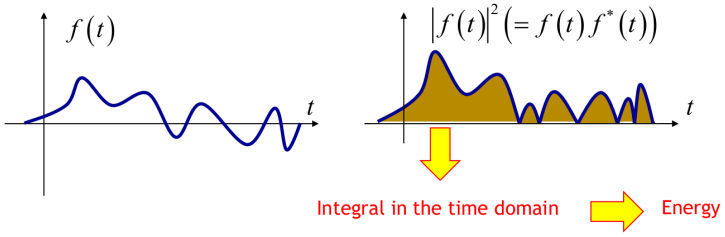

Figure 1.2: Energy of a signal

1.3.2 Power of a signal

When we refer to power we can refer to the **instantaneous power** of a signal, which is just the square module of a signal

$$P(x) = |x(t)|^2 \tag{1.2}$$

but much more commonly we refer to the average power of a signal, which is the time average of the instantaneous power of the whole signal.

$$P(x) = \lim_{a \to \infty} \frac{1}{2a} \int_{-a}^{a} |x(t)|^2 dt \tag{1.3}$$

This a again a scalar value.

1.3.3 Signal Representation

To analyze and process the signals, it is necessary to adequately represent them, and the definition of signals as "time functions" is NOT effective for many applications, for many reasons.
Generally, signals can become very complicated depending on our communication system, and we want different ways of representing them, to make them easier to process.
For instance, we can represent a signal as a sum of elementary signals, thanks to the scalar product of the signal with a basis of the space of signals.

The scalar product between signals is a scalar value, which is a measure of the similarity among signals.
If two function are quite similar we will get a large number. It it is zero, they are said to be orthogonal.

$$\langle x, y \rangle = \langle x(t), y(t) \rangle = \int_{-\infty}^{\infty} x(t) y^*(t) dt \tag{1.4}$$

So, if we have a set of elementary signals $w_1(t), w_2(t), \ldots, w_m(t)$, we write the signal $x(t)$ as a linear combination of the elementary signals:

$$x(t) = \sum_{i=1}^{m} \alpha_i w_i(t) \tag{1.5}$$

where α_i are the coefficients of the linear combination $\alpha_i = \langle x(t), w_i(t) \rangle$.

In a more down to hearth way, the coefficient α_i allows us to understand how much each individual signal is similar to any other elementary signal we are considering, and because the scalar product is higher for similar signals, we can understand how much each elementary signal is contributing to the whole signal.

Furthermore, by adjusting the coefficient, we are able to create a whole different signal using the same elementary signals.

A common example: In Phase and Quadrature components representation

Lets consider a very simple basis, or a set of elementary signals, which is actually more important that many other ones:

- the **in-phase** signal, which is a cosine function $w_1(t) = cos(2\pi f_o t)$
- the **quadrature** signal, which is a sine function $w_2(t) = sin(2\pi f_o t)$

where f_o is the frequency, in Hz, of the signal.
We can write any signal as a linear combination of these two signals, just by adjusting the coefficients:

$$x(t) = x_1 cos(2\pi f_o t) + x_2 sin(2\pi f_o t) \tag{1.6}$$

where x(t) is the signal we want to represent, and x_1 and x_2 are the coefficients of the linear combination.

A very simple representation of this complex signal is obtainable by representing each signal as an axes in a complex plane, for example in figure 1.3 the x-axis is the in-phase signal, and the y-axis is the quadrature signal.
Each signal can be represented as a point in the complex plane, because the distance from the origin signal(*axis*) is the amplitude of the signal. For example, choosing a point close to the x-axis, we are choosing a signal with a very low quadrature component, and a very high in-phase component.Furthermore, a set of those different points is called a *constellation*

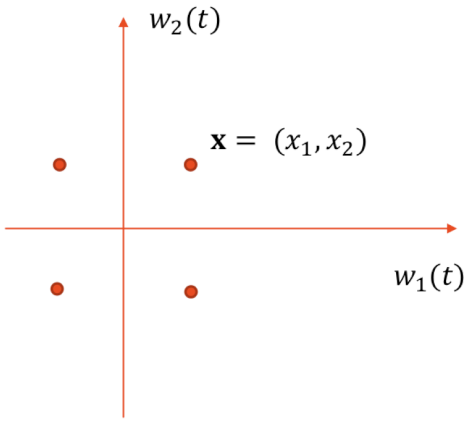

Figure 1.3: Some points that represent some signals in the I/Q representation

1.3.4 Fourier Analysis

Lets consider a signal with base the complex exponential functions

$$e^{j2\pi\frac{n}{T}t} = cos(2\pi\frac{n}{T}t) + jsin(2\pi\frac{n}{T}t) \tag{1.7}$$

It is actually characterized by a frequency $f_n = \frac{n}{T}$, where T is the period of the signal. The higher the frequency, the more oscillations we will have in the same time interval. In this function they have both the same frequency.

We can use that function as a basis to decompose a signal, again. This is because it is possible to generate an infinite set of functions

$$w_n(t) = \frac{1}{\sqrt{T}} e^{j\frac{2\pi}{T}nt} \tag{1.8}$$

with $-T/2 \leq t \leq T/2$, each associated with a frequency. That can be used ad a complete basis for all the signals limited in $[-T/2, T/2]$ or periodic.
For example, we can write a signal as a linear combination of these functions:

$$x(t) = \frac{1}{\sqrt{T}} \sum_{n=-\infty}^{\infty} c_n e^{j\frac{2\pi}{T}nt} \tag{1.9}$$

where c_n are the coefficients of the linear combination $c_n = \langle x(t), w_n(t) \rangle$.
Each one of those coefficients is a measure of how much each frequency f_n, of the n-th sinusoid(the shape of equation 1.7) is present in the signal $x(t)$.
Lets now take a look at picture 1.4. We can see that the coefficients are higher when the

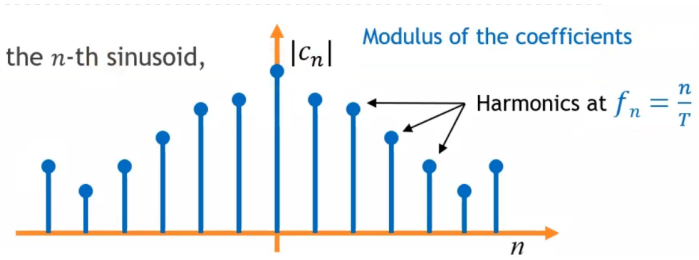

Figure 1.4: Plot of the coefficients of equation 1.9

frequence is very small, so the signal 1.9 is mostly composed by large components of low frequency.
This whole concept is called **Fourier Analysis**, or frequency analysis, which allows to decompose a signal into a set of frequencies.

> TLDR: I can build a signal trough a combination of frequency components.
> The coefficients of this frequency components are the measure of how much each frequency is present in the signal.

Now we just need to expand it to any signal and any frequency(a continuous frequency domain). By doing so we can derive the definition of the **Fourier Transform** of a signal

$x(t)$:

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt \tag{1.10}$$

where $X(f)$ is the Fourier Transform of the signal $x(t)$, and f is the frequency.
The Fourier transform is equivalent to a scalar product between the signal and the complex exponential function at a given frequency f. This means that each of the values of the Fourier Transform is a measure of how much the frequency f is present in the signal $x(t)$.
Furthermore, trough the inverse of equation 1.10

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft} df \tag{1.11}$$

we can write again a signal $x(t)$ as a linear combination of the complex exponential functions , which represents the frequency components of the signal, weighted by the Fourier Transform.

> The Fourier Transform $X(F)$ indicates the "weight" of each frequency component(sinusoidal component at a given frequency f) in the signal $x(t)$.
> The inverse Fourier Transform $x(t)$ tells us we can decompose any signal into frequency components(sinusoidal components at a given frequency f).

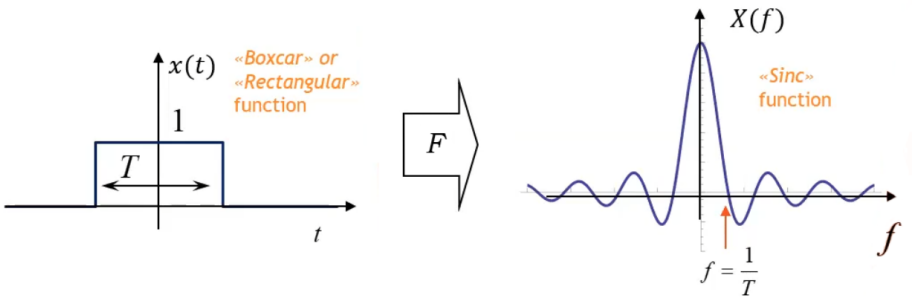

Figure 1.5: Fourier Transform of a square function

With that in mind, take a look at figure 1.5. It represents a rectangular signal (a signal that is 1 for a certain time, and 0 for the rest of the time), and its Fourier Transform, which tells us the frequency components of the signal.
From that, we can see that the Fourier Transform is mostly composed by low frequency components, because values closer to zero are higher. That is because in the constant part of the signal has a sinusoidal component that constant.

> To wrap it up, for each signal we have a **spectral representation**. And for each operation over a signal, there are equivalents effects in the frequency domain.
> Furthermore, a signal that has finite duration in time, has a infinite support in the frequency domain.

1.3.5 Bandwidth

The bandwidth is the **interval of frequencies** that a signal occupies.
If we consider a signal $x(t)$, we can define the bandwidth as the interval of frequencies where the Fourier Transform $X(f)$ is different from zero.
Signals have often infinite support over the frequency domain over a finite duration, but many of them are characterized by a quasi-null(finite) spectrum outside a certain interval of frequencies(the main lobes of the spectrum).
For this reason, we usually consider the bandwidth around half of the frequency spectrum of the signal, as shown in figure 1.6(for example 3dB bandwidth, or half power bandwidth).

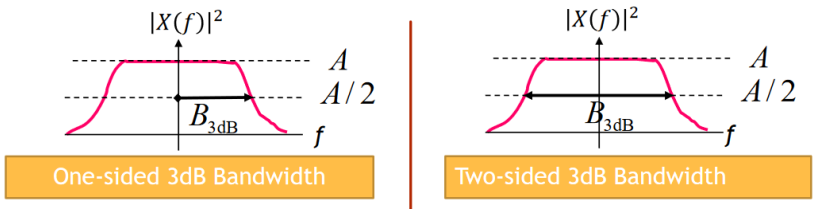

Figure 1.6: Bandwidth of a signal

Bandwidth in linear systems

A **system** is a set of operations applied to signals.
The relationship between the bandwidth of the input signal and the bandwidth of a system is usually very important. In fact, when a system is used to pass or remove particular frequencies of a signal, it can be regarded as a system.
We can associate a bandwidth to a system, specifically a **linear-time invariant** system, with a **frequency response** $H(f)$.This mean that we can associate a bandwidth to a system, making us able to compute a new bandwidth $Y(f)$ by combining together the bandwidth $X(f)$ of the input signal and the frequency response $H(f)$ of the system($Y(f) = X(f)H(f)$ in formulas).
This concept can be represented graphically very easily, like in figure 1.7. If the result of the combination of the input signal and the sequence of operation of the system is a signal with a bandwidth $Y(f)$. If the bandwidth of the linear system is larger than the origin signal, the signal pass trough smoothly($Y(f) \approx X(f)$).
However, if the bandwidth of the signal is larger than the bandwidth of the system, the signal will be cutted off($Y(f) \neq H(f)$).

1.3.6 Filters

A filter is a system used to model desired and undesired effects over a signal.
It is usually used to remove undesired frequency components from a signal, but overall can be used to:

- share the wireless medium

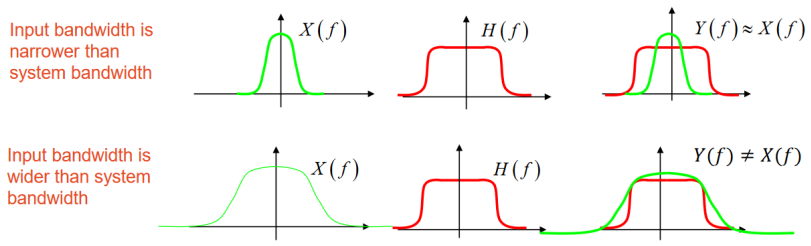

Figure 1.7: Bandwidth of a system

- model the spectrum of a signal over the channel
- mitigate undesired effects over a signal trough equalizers

1.3.7 Signal modulation

Signal modulation is the process of multiplying a signal by a sinusoidal function, resulting in a **frequency shift**.

$$y(t) = x(t) \cdot cos(2\pi f_0 t) \tag{1.12}$$

This is possible because

$$F(x(t) \cdot cos(2\pi f_0 t)) = \frac{1}{2}[X(f - f_0) + X(f + f_0)] \tag{1.13}$$

where X is the frequency domain representation.

We can see that as a result of the modulation, the spectrum of the signal is shifted around

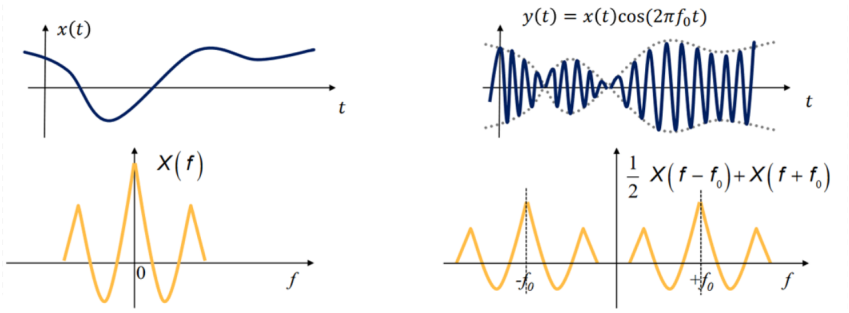

Figure 1.8: Graphical representation of the modulation

the frequency f_0, as shown in figure 1.8.

1.3.8 Signal demodulation

When modulating a signal, we alter it a bit, centering it around the frequency f_0, shifting the spectrum of the signal. The effect of this operation is not trivial.

To recover the original signal, we need to multiply the modulated signal by a sinusoidal function at the same frequency f_0 as the one used for the modulation. This allows us to shift the spectrum back to the original position.

This operation is called **demodulation**.
A given modulated signal $Y(f)$

$$Y(f) = \frac{A}{2}[X(f - f_0) + X(f + f_0)] \tag{1.14}$$

shown in figure 1.9 can be demodulated by multiplying it by the same sinusoidal function

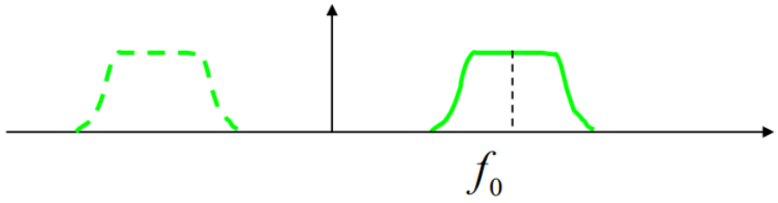

Figure 1.9: A modulated signal at frequency f_0

used for the modulation

$$Y'(f) = Y(f) \cdot cos(2\pi f_0 t) = \frac{A}{2}X(f) + \frac{A}{4}[X(f - 2f_0) + X(f + 2f_0)] \tag{1.15}$$

shown in figure 1.10
This doesn't allow us to recover the original spectrum of the signal. That's why we need

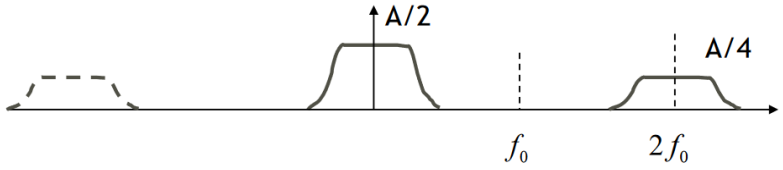

Figure 1.10: A demodulated signal at frequency f_0

to use a **low-pass filter** to remove the frequency components at $2f_0$ and its symmetrical counterpart, as shown in figure 1.11.

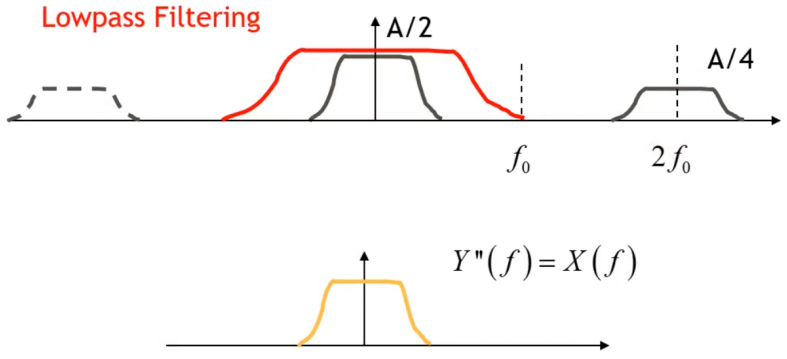

Figure 1.11: A demodulated signal at frequency f_0 after a low-pass filter

1.3.9 Frequency Multiplexing(FDM)

Modulation and demodulation allows multiple wireless communication systems to coexist at different frequencies.
For example, if i want to transmit different signals with overlapping bandwidths, i can simply modulate each signal at a different frequency, and then transmit them all together, as shown in figure 1.12.
Once received the signal, each of those signals can be demodulated by multiplying it by the same function at the same frequency used for the modulation.

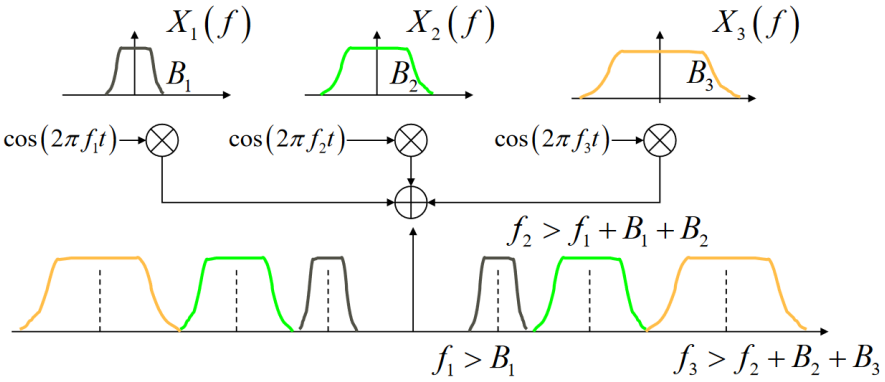

Figure 1.12: Frequency Multiplexing

1.3.10 Analog-to-Digital Conversion

We can now deal with signals, but we still have to convey information.
The informations can be both **analog** or **digital**. Usually, transmitting digital information is ideal, because it has some advantages, such as error detection and correction, and the possibility to compress the information. On the other hand, we still have to convert digital information to analog information to be transmitted over the channel, after converting it to a stream of bits.
Once the signal is received, it has to be converted back to digital information. To do so, first of all the signal it has to be sampled, which can be a lossless operation if the sampling frequency is high enough.
After the sampling, the sample has to be quantized, which is the process of converting the amplitude of the sample to a digital value at discrete times(because it is a continuous time function, which would require an infinite number of digits to represent). Each of those values is associated with a given amplitude, which is associated to a number, which eventually is converted into binary digits. We can also observe that quantization is a lossy operation by definition.
At the end of the fair, a sequence of bits is obtained, which can be transmitted over the channel.

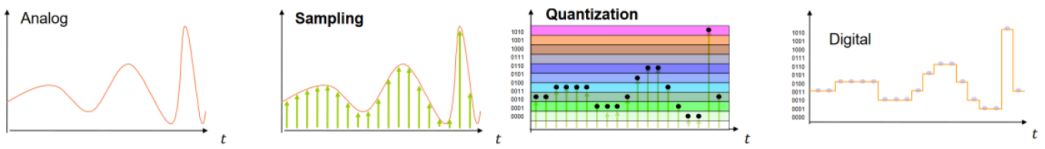

Figure 1.13: Analog-to-Digital Conversion

Sampling theorem

As previously stated, the sampling operation can be lossless if the sampling frequency is high enough. This is because of the **Nyquist sampling theorem**, which states that a signal can be perfectly reconstructed from its samples if the sampling frequency is at least twice the bandwidth of the signal.

$$f_c = \frac{1}{T_c} > 2B \rightarrow T_c < \frac{1}{2B} \tag{1.16}$$

where f_c is the sampling frequency, T_c is the sampling period, and B is the bandwidth.

1.4 Signal Transmission and Reception

Now that we know how a signal can be represented and processed, we can start to think how each component of a communication system can be designed.

1.4.1 Digital Modulations

The end goal is to have a reliable communication system, which can transmit and receive information. As such, a important design choose is the signal waveform to transmit.
The **modulator** is the component of the system that takes the digital information and modulates it to a signal that can be transmitted over the channel. The demodulator component just does the opposite, taking the signal and converting it back to digital information.

> **Modulation** is the process of varying one or more properties of a periodic waveform, called the **carrier**, with a modulating signal that typically contains information to be transmitted.

This process is necessary not only to cope with the analog channel, but also to allow multiple communication systems(which means different signals) to coexist in the same channel.

Generally, digital and analog modulations resort to basic modulation types:

- **Amplitude Modulation(AM)**, which changes the amplitude of the carrier
- **Frequency Modulation(FM)**, which changes the frequency of the carrier
- **Phase Modulation(PM)**, which changes the phase of the carrier

Amplitude Modulation(AM)

The amplitude modulation is the simplest form of modulation.
The amplitude of an high-carrier signal(like a cosine signal) is varied according to the instantaneous amplitude of the modulating message signal $m(t)$.

Frequency Modulation(FM)

In frequency modulation, the frequency of the carrier signal is varied by the modulating signal $m(t)$, while the amplitude of the carrier signal is kept constant.
This means that the as the amplitude of the information signal varies, the carrier frequency varies as well. For example, if the amplitude of the information signal increases, the frequency of the carrier signal increases as well.

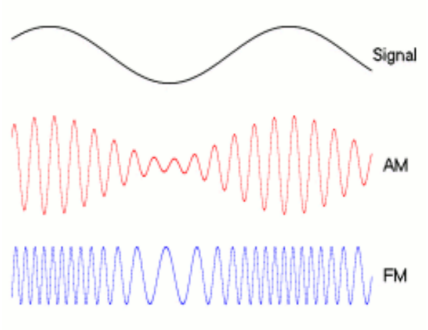

Figure 1.14: An example of a signal modulated in amplitude and frequency

Phase Modulation(PM)

Phase modulation is a form of modulation that encodes the signal $m(t)$ as a variation in the instantaneous phase of a carrier wave.
This means that the phase of a carrier is modulated to follow the changing in the signal amplitude of the message signal.

The peak amplitude and the frequency of the carrier signal are maintained constant, but as the amplitude of the message signal changes, the phase of the carrier changes correspondingly.

Analog-to-Digital modulations

Even if the world has turned to digital, transmitted signals are analog.
This means that the digital information has to be converted to an analog signal to be transmitted over the channel. But the receiver still need to understand the digital information from the received signal.
To be sure that the information can be recovered, the signal has to be modulated in a way that the receiver can understand the digital information. This can be done by varying some

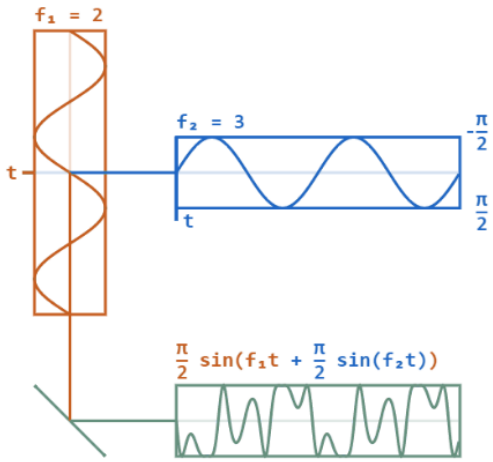

Figure 1.15: An example of a signal modulated in phase. The modulating wave(in blue) is modulating the phase of the carrier wave(in red), resulting in the PM signal(in green)

proprieties of the carrier signal, such as the amplitude, the frequency, or the phase, to represent the digital information.

The carrier signal is used to modulate the digital information, so we can distinguish between

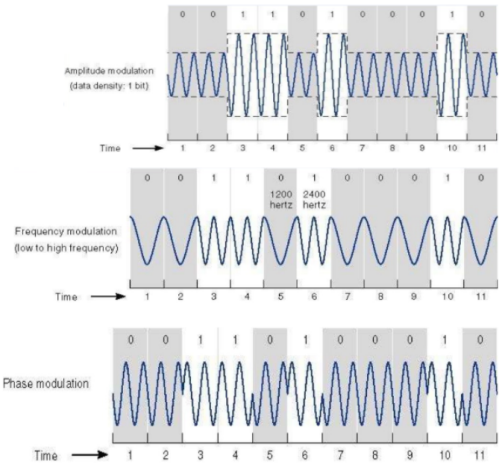

Figure 1.16: Some example of modulations used to represent digital information. From top to bottom: Amplitude Shift Keying, Frequency Shift Keying, Phase Shift Keying

different kinds of signals:

- the **the baseband signal**, which is the unmodulated signal, whose spectrum is centered around zero frequency
- the **passband signal**, which is the modulated signal, whose spectrum is centered around the carrier frequency

The baseband signal can be converted to a passband signal by multiplying it by a carrier signal with the desired frequency.

Baseband Signals

The simplest kind of digital modulation is the **Pulse Amplitude Modulation(PAM)**, which is a form of modulation where the message signal is encoded in the amplitude of a series of signal pulses.
For example, if we have a binary signal, we can encode the 0 as a low amplitude pulse $-A$, and the 1 as a high amplitude pulse A. The simplest pulse is a rectangular one, but other kind of pulses can be used.
If we have a binary PAM(2-PAM), the signal can be represented as:

- $s(t) = g(t) \rightarrow$ "1"
- $s(t) = -g(t) \rightarrow$ "0"

where $g(t)$ is the basic pulse shape.

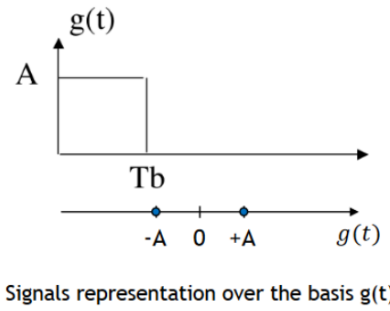

Figure 1.17: An example of a 2-PAM signal representation

M-ary PAM

WA 2-PAM signal can only represent 1 bit of information. To represent more bits, we can use M-ary PAM, where M is the number of different symbols that can be represented, while still using the same base signal.
For example, a 4-PAM signal can represent 2 bits of information by defining 4 levels of amplitude, and can be represented as:

- $s(t) = 3g(t) \rightarrow$ "00"
- $s(t) = g(t) \rightarrow$ "01"
- $s(t) = -g(t) \rightarrow$ "10"
- $s(t) = -3g(t) \rightarrow$ "11"

This definition can be generalized to:

$$s_i(t) = A_i g(t), \quad i = 1, 2, \ldots, M \tag{1.17}$$

allowing to represent $log_2(M)$ bits of information.

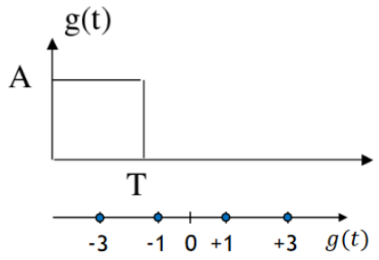

Figure 1.18: An example of a 4-PAM signal representation

Gray Coding

When using M-ary PAM, it is important to use a coding that minimizes the error probability. After all, Symbols that are close to each other in the signal space are more likely to be confused, so the choice of the number of symbols and the distance between them is important.

> **Gray coding** is a strategy to **mapping bits to symbols** that minimizes the probability of error.

Gray coding achieves 1-bit error correction, meaning that if a error is to occur, it will only affect 1 bit of the message with a high probability.

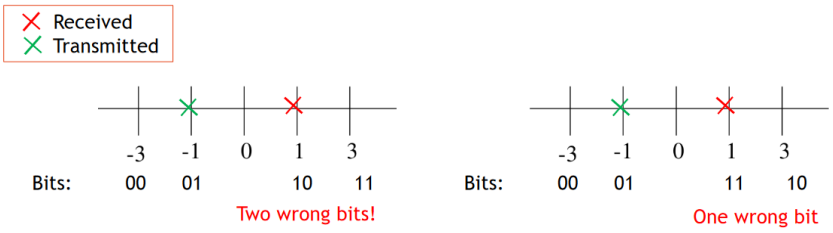

Figure 1.19: An example of a 4-PAM signal representation using Gray coding

Energy per bit

A measure of the energy efficiency of a modulation can be obtained by calculating the avarage energy per bit.
The energy per bit can be defined as

$$E_b = \frac{E_s}{log_2(M)} \tag{1.18}$$

where E_s is the energy of the signal, and M is the number of symbols, or in a more discursive way, the average energy per symbol divided by the number of bits carried by each symbol. The energy per symbol can be calculated as

$$E_s = \int_0^T (S_m(t))^2 dt = (A_m)^2 \int_0^T (g(t))^2 dt = (A_m)^2 E_g \tag{1.19}$$

where $S_m(t)$ is the modulated signal, A_m is the amplitude of the modulated signal, $g(t)$ is the base pulse, and E_g is the energy of the base pulse.

For example, the average energy per symbol for the 4-PAM of figure 1.18 is

$$E_s = \frac{3^2T + 1^2T + 1^2T + 3^2T}{4} = 5T \tag{1.20}$$

Bandpass Signals

As previously stated, to transmit a baseband signal $s(t)$ trough a passband channel, we have to modulate it at a certain frequency f_c, by multiplying it by a sinusoidal carrier signal with that frequency, otherwise it will be centered around zero frequency.

Bandwidth Occupancy

Part II

Hardware