Wireless Security

Prof. Marco Mellia
Dr. Andrea Nardin

Course Outline

- **Course Outline**
  - **Review of basic concepts for digital communications**
  - Security at the physical layer
  - Global Navigation Satellite Systems (GNSS) and positioning
  - Security in WiFi Networks
  - Bluetooth security
  - Security of Cellular Networks - 3G/4G/5G Network Structure and Architectures
  - Security of Near Field Communications (NFCs) and RFIDs

Basic Concepts for Digital Communications

Andrea Nardin

Contents

- Review of basic concepts for digital communications
  - Introduction
  - Digital Communications Overview
  - Signals Representation and Processing
    - Signal representation
    - Frequency domain, filters, modulation
    - Sampling Theorem and Discrete Time Signals
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

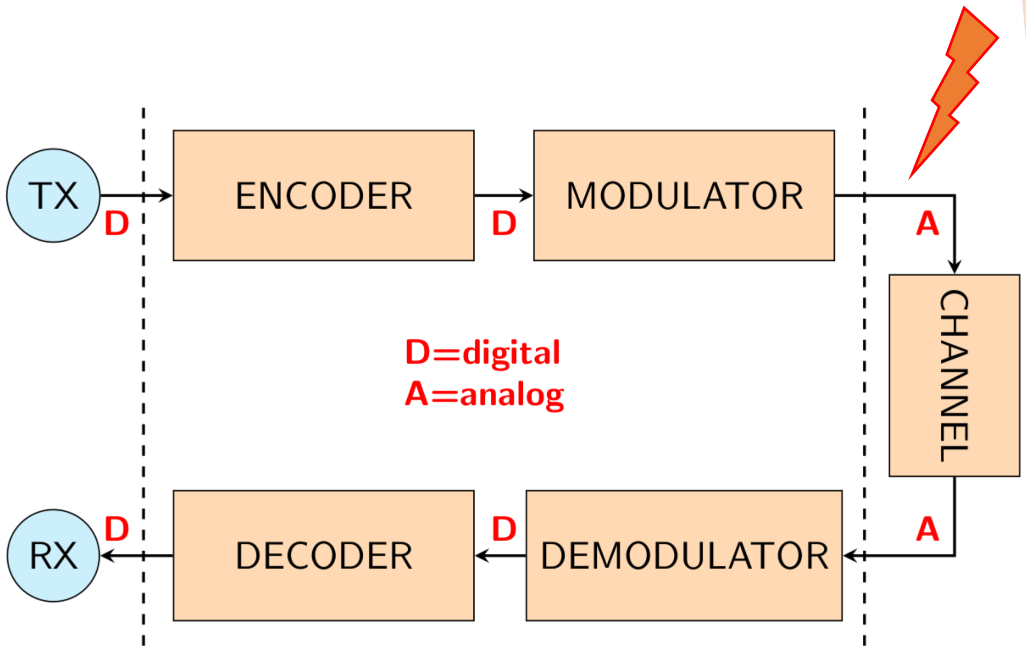
Contents

- Review of basic concepts for digital communications
  - **Introduction**
  - Digital Communications Overview
  - Signals Representation and Processing
    - Signal representation
    - Frequency domain, filters, modulation
    - Sampling Theorem and Discrete Time Signals
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

Wireless Channel and Security Threat

- The main study area of this part of the course is **security** at the ***physical layer***
- The *physical layer* defines the means of transmitting a stream of raw **bits** over a **physical data link** connecting network nodes
- The bitstream may be grouped into code words or symbols and converted to a physical **signal** that is transmitted over a **transmission medium**
- When signals are transmitted over the **wireless channel**, security is more of a concern

Security threat!



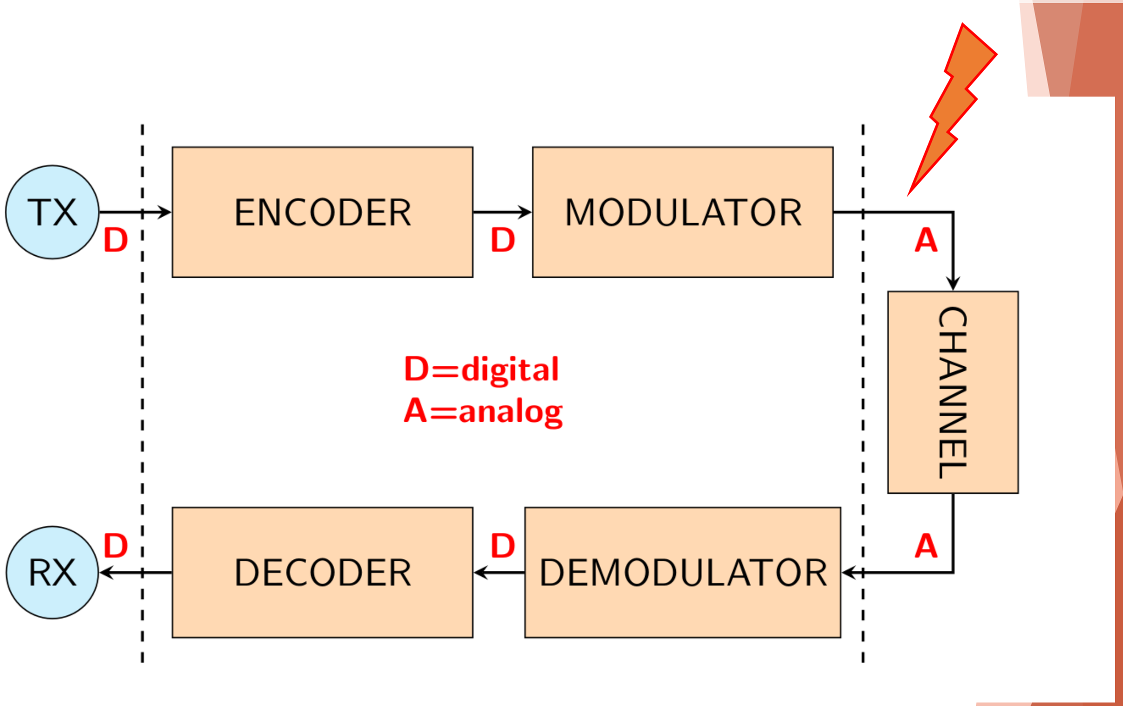
D=digital
A=analog

Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- Why?
  - No inherent physical protection
    - physical connections between devices are replaced by logical associations
    - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)

Security threat!

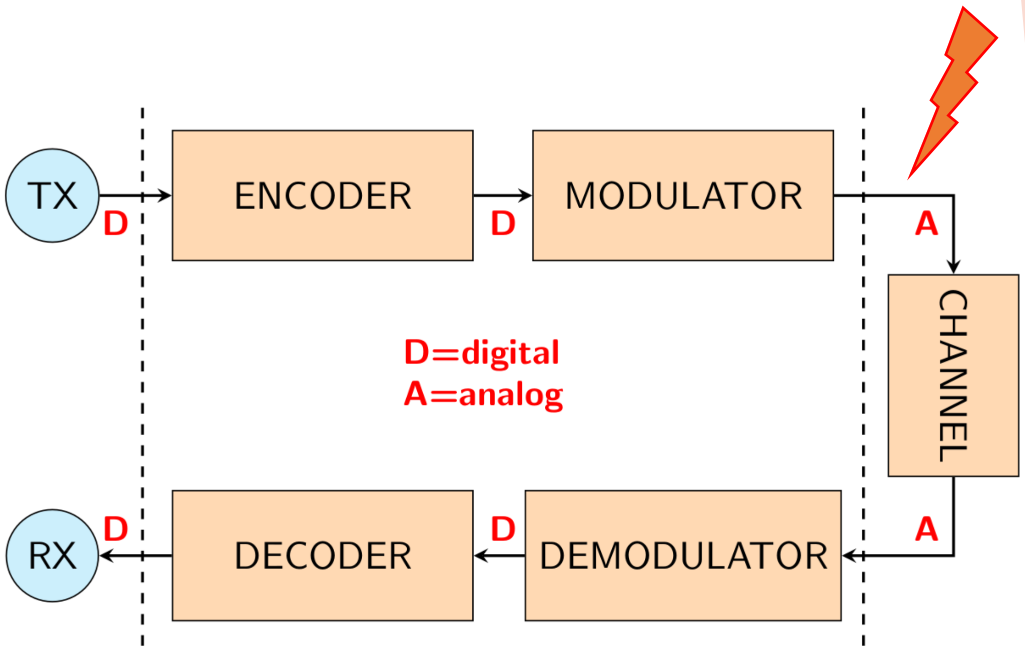


Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- Why?
  - Broadcast communications
    - wireless usually means radio, which has a broadcast nature
    - transmissions can be overheard by anyone in range
    - anyone can generate transmissions
      - received by other devices in range
      - interfere with other nearby transmissions and may prevent their correct reception (*jamming*)

Security threat!

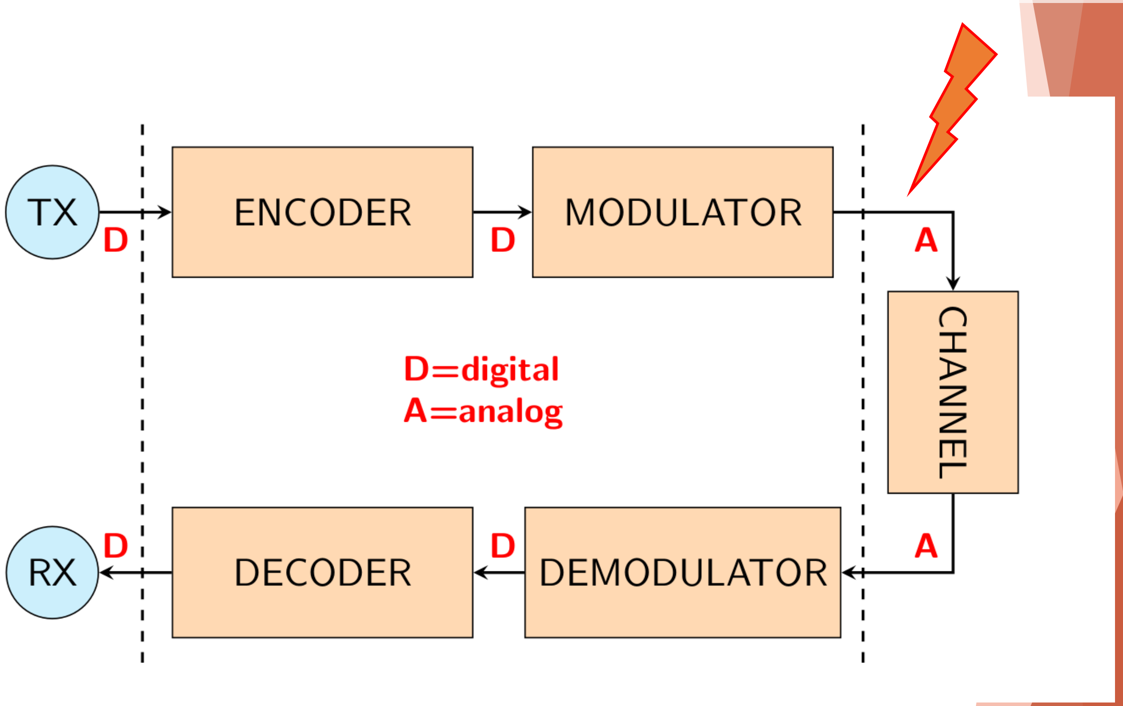


Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- As a result:
  - eavesdropping is easy
  - injecting bogus messages into the network is easy
  - replaying previously recorded messages is easy (e.g. *meaconing*)
  - illegitimate access to the network and its services is easy
  - denial of service is easily achieved by jamming

Security threat!

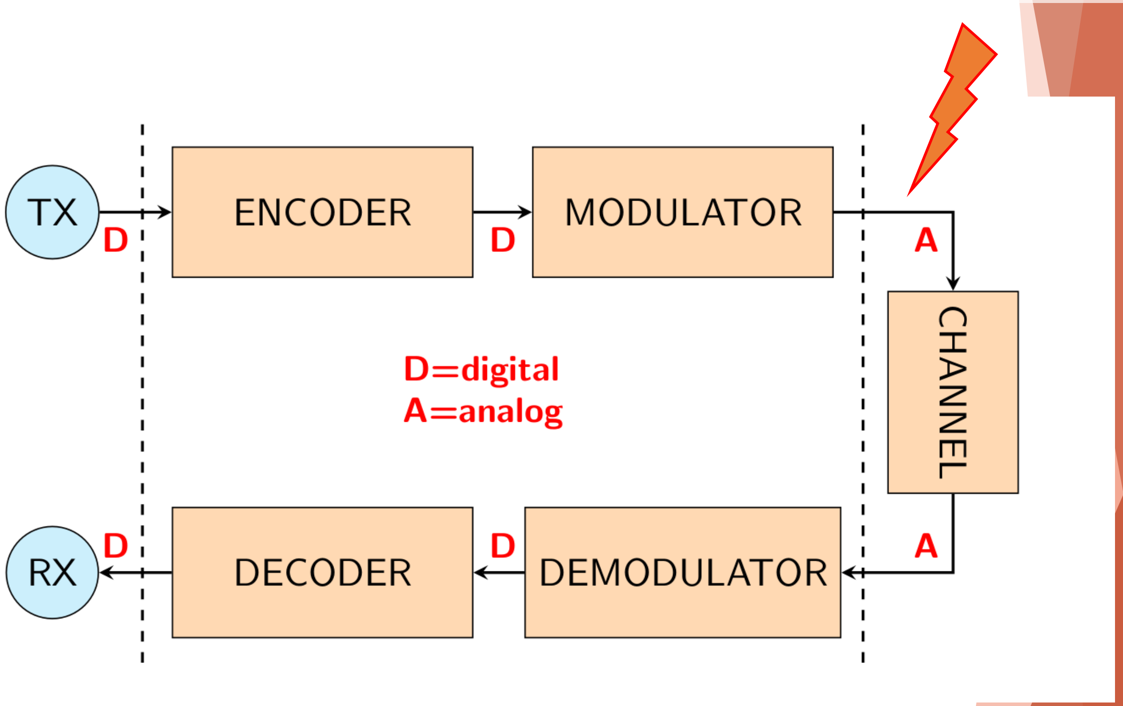


Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- To understand threats and identify countermeasures we must first dwell on the working principles of **digital communications**

Security threat!



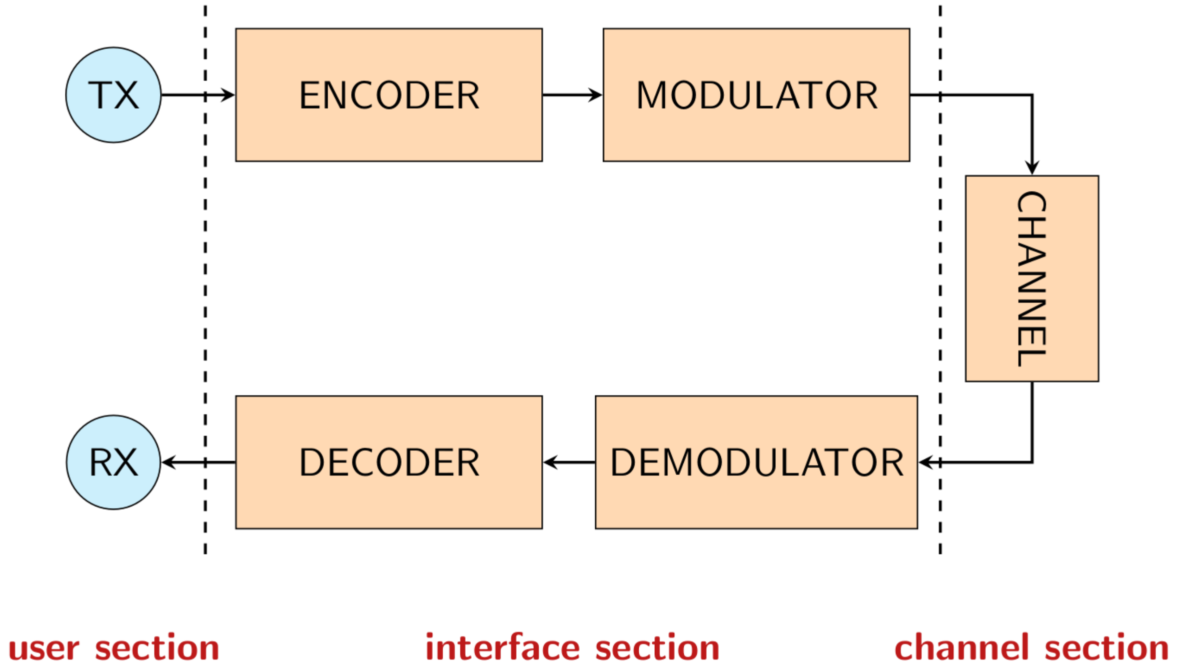
This will be our «reference map»

Contents

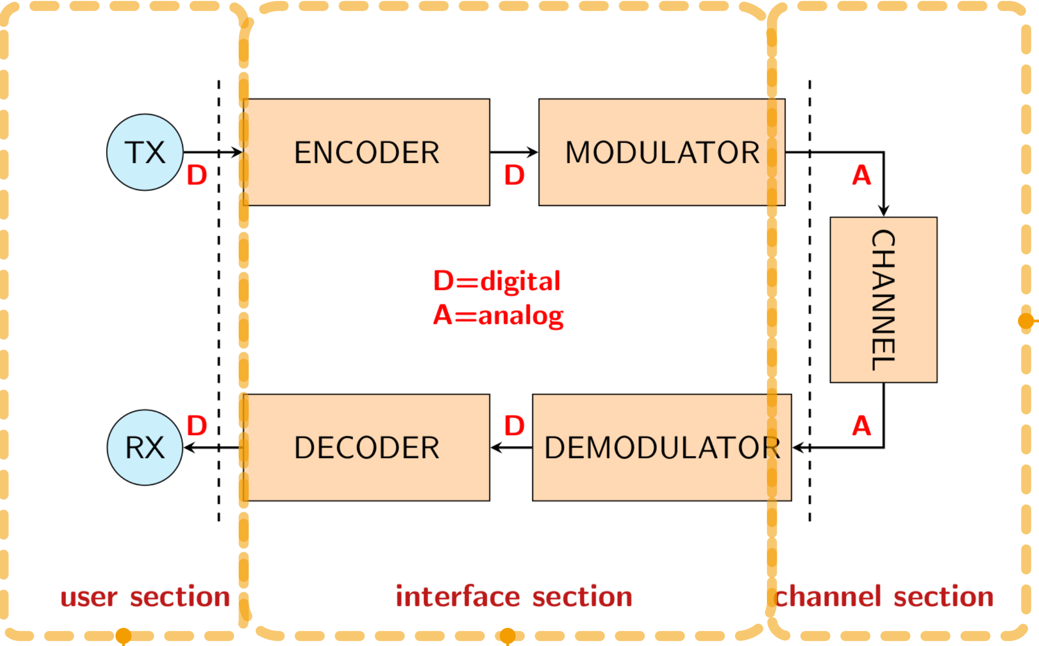
- Review of basic concepts for digital communications
  - Introduction
  - **Digital Communications Overview**
  - Signals Representation and Processing
    - Signal representation
    - Frequency domain, filters, modulation
    - Sampling Theorem and Discrete Time Signals
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

Digital Communication System: Overview

- To avoid getting lost on the working principles of **digital communications**, it is useful to characterize the general model of a digital communication system
- The model can be divided into three sections:
  - **The user section**
  - **The interface section**
  - **The channel section**

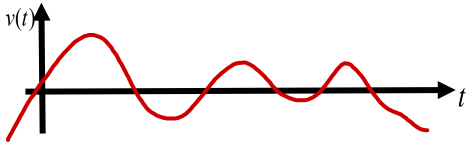


Digital Communication System: Overview



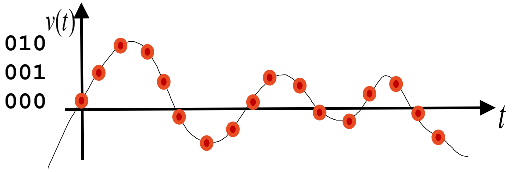
CHANNEL SECTION

- We can propagate **analog** waveforms
- What are **waveforms**/**signals**?
- How to generate them to
  - Convey information
  - Counteract channel impairments



USER SECTION

- Our goal is to **communicate** information from the TX to the RX
- Information is **digital** (or converted to digital)

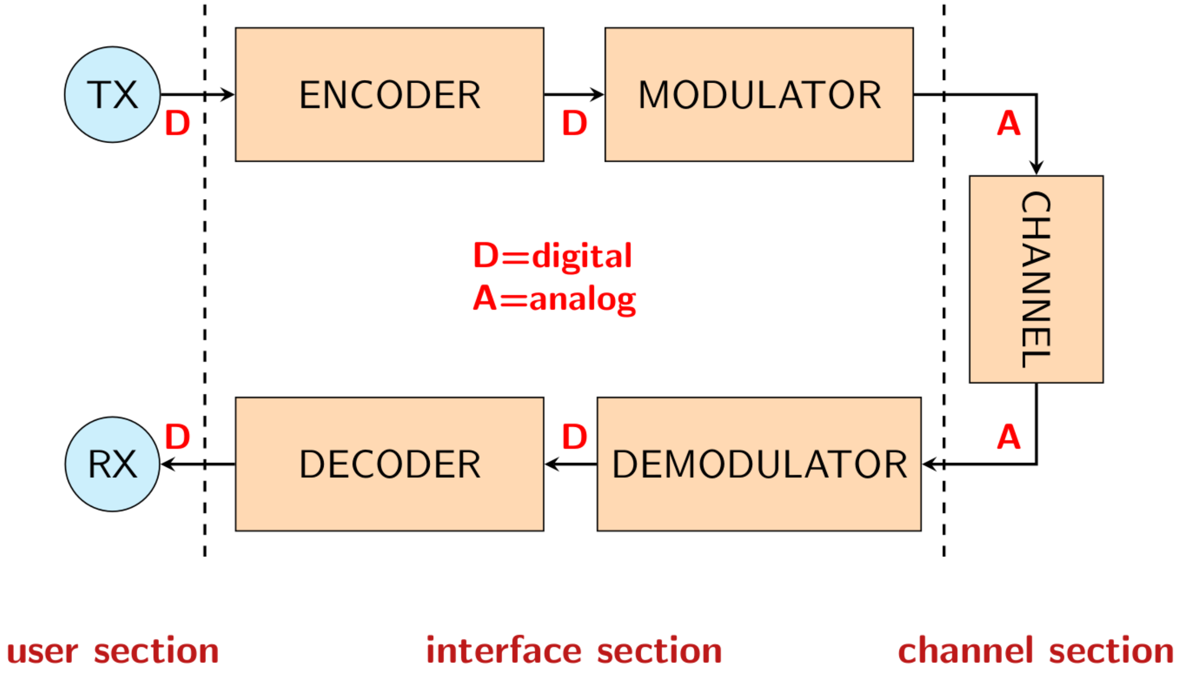


INTERFACE SECTION

- How to transform bits into signals?
  - **Compress** bits to save space (source encoding)
  - **Encode** bit sequences to make them more robust to errors (channel encoding)
  - **Associate** bits to signal waveforms (modulator)

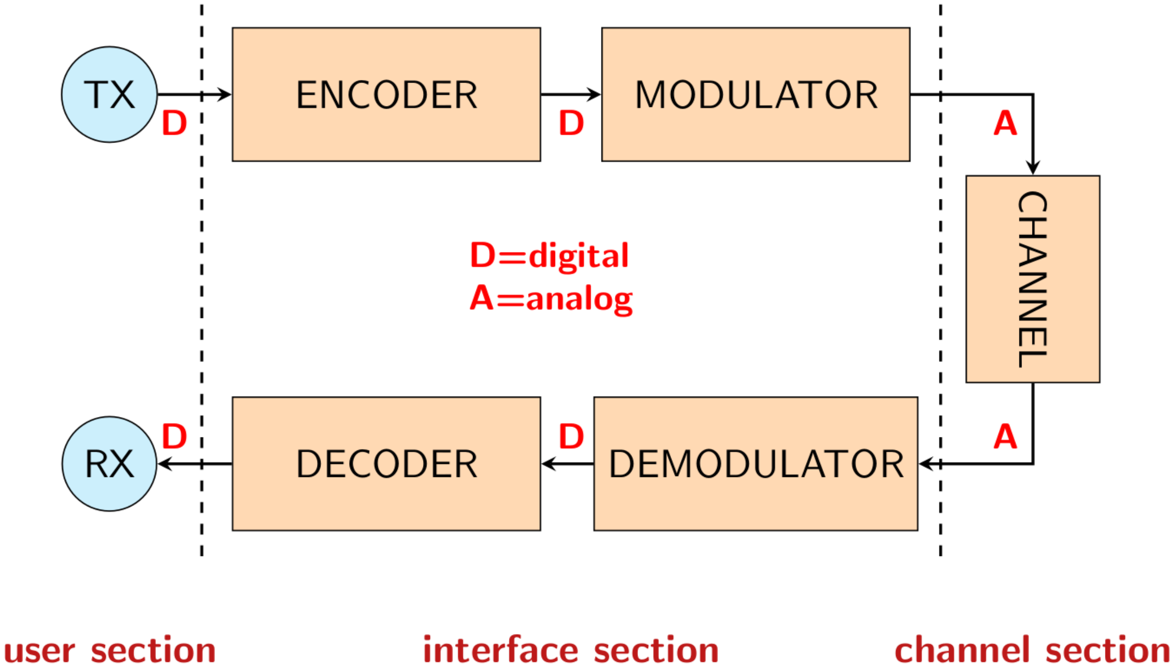
Digital Communication System: TX chain

- *Encoder*
  - Implements **source encoding** to limit the amount of transmitted data
  - Implements **channel encoding** to limit the effects of channel disturbances
- *Modulator*
  - **Converts** the digital signal into an analog signal to be transmitted over the channel



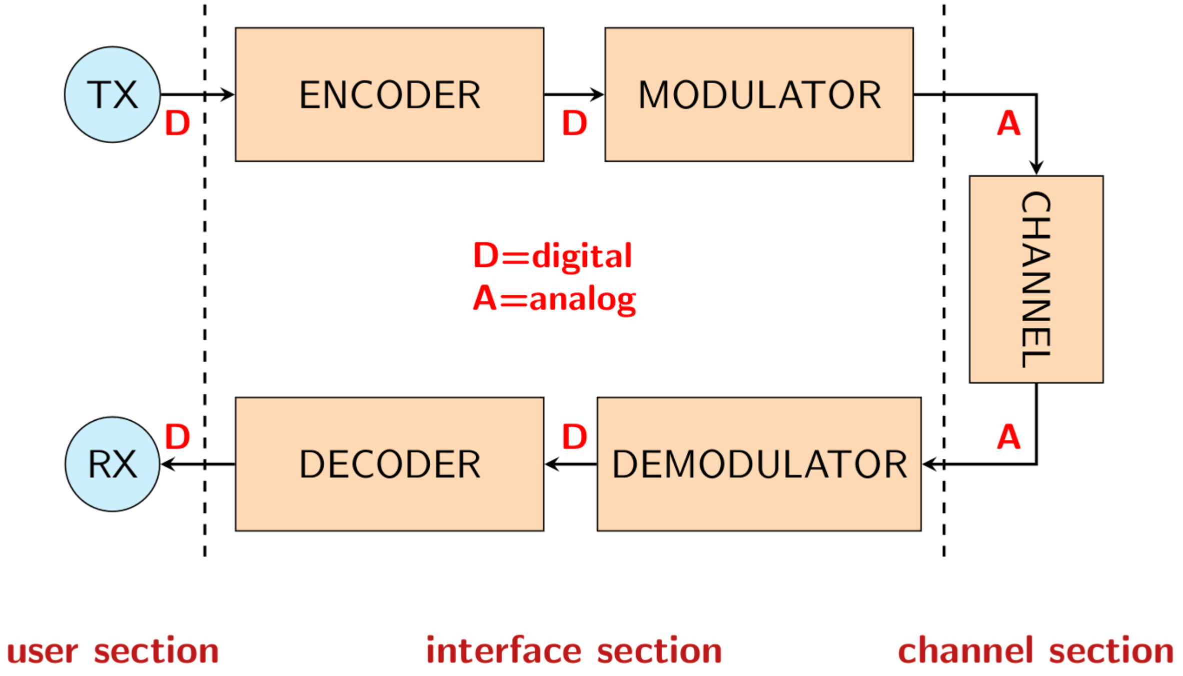
Digital Communication System: Channel

- *Channel*
  - The channel transfers an analog signal from the transmitter 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



Digital Communication System: RX chain

- *Demodulator*
  - Converts the received **analog signal** into a **sequence of samples** to be processed by the decoder
- *Decoder*
  - Implements **channel decoding** to limit the effect of channel errors and extract the information data
  - Implements **source decoding** to expand the compressed data back to their original form

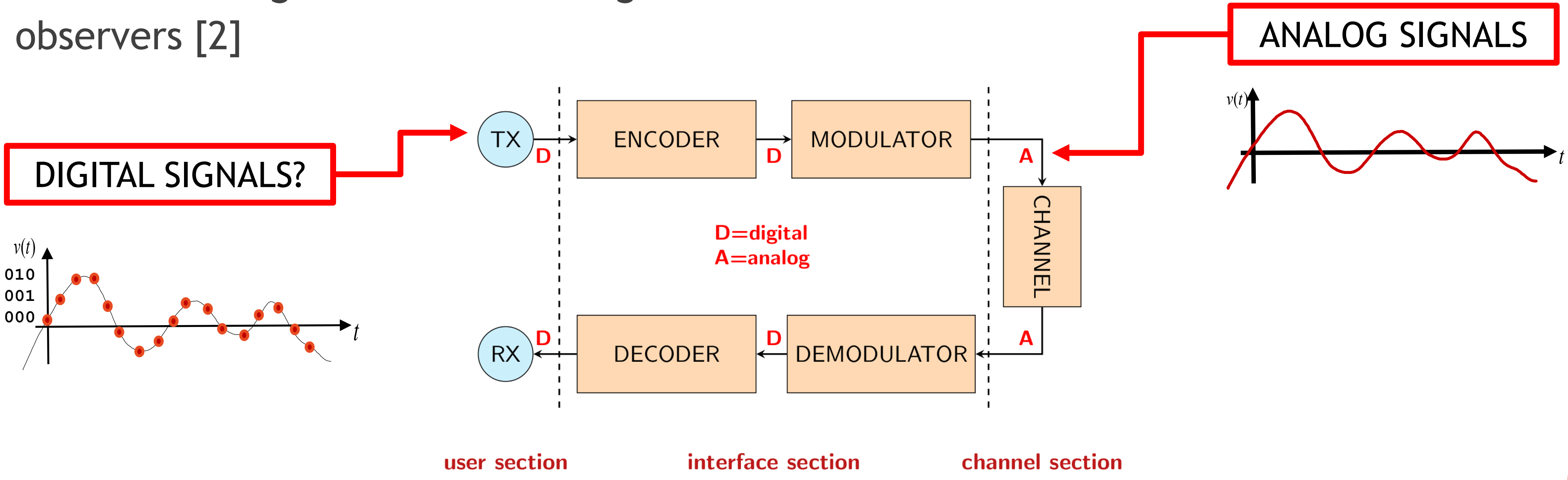


Contents

- Review of basic concepts for digital communications
  - Introduction
  - Digital Communications Overview
  - <u>**Signals Representation and Processing**</u>
    - <u>**Signal representation**</u>
    - Frequency domain, filters, modulation
    - Sampling Theorem and Discrete Time Signals
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

Signal Representation and Processing

- A *signal* is a function that conveys **information** about a phenomenon [1]
- Any quantity that can **vary over space or time** can be used as a signal to share messages between observers [2]



DIGITAL SIGNALS?

ANALOG SIGNALS

TX → ENCODER → MODULATOR → CHANNEL → DEMODULATOR → DECODER → RX

D=digital
A=analog

user section

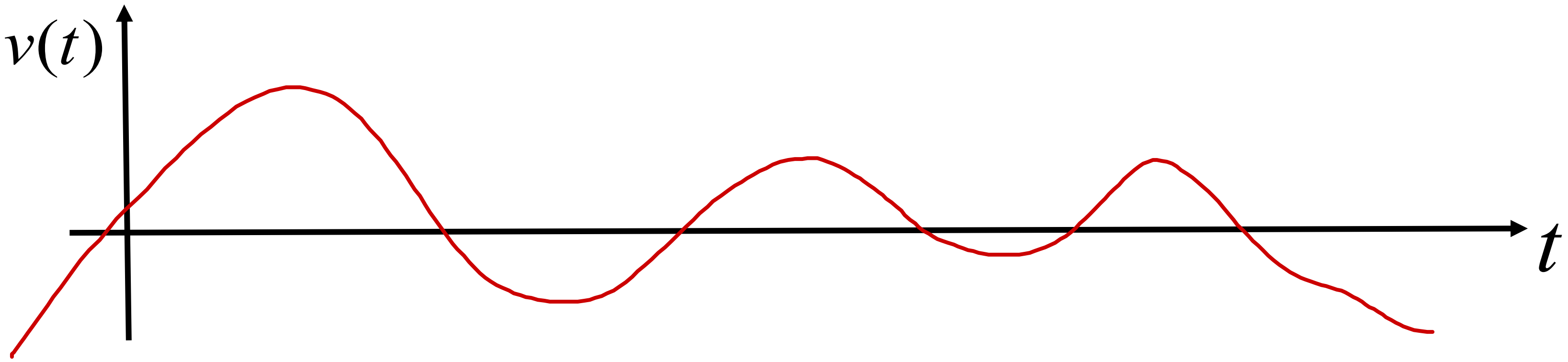
interface section

channel section

[1] Roland Priemer (1991). Introductory Signal Processing. World Scientific. p. 1. ISBN 978-9971509194
[2] Chakravorty, Pragnan (2018). "What Is a Signal? [Lecture Notes]". IEEE Signal Processing Magazine. 35 (5): 175–177. doi:10.1109/MSP.2018.2832195.

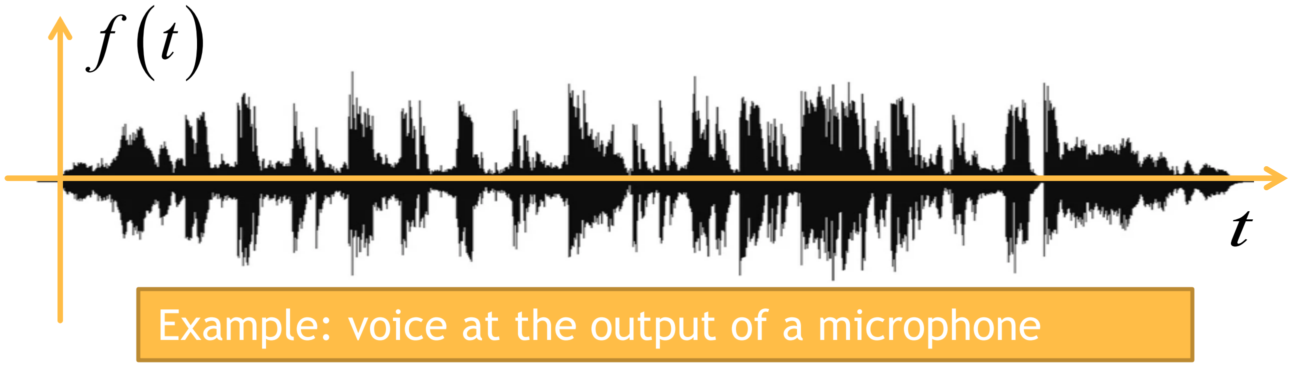
What is a Signal?

- A signal describes the evolution of physical quantities over **time** (voltages, currents, temperatures, etc.)
- Its mathematical representation is therefore a **function of real variable** (time) taking **real** or **complex** values

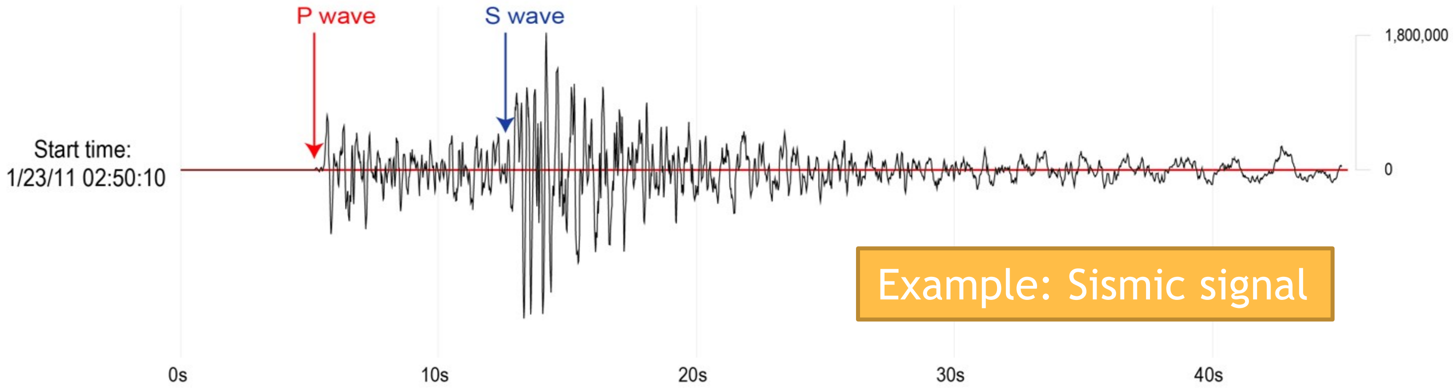


What is a Signal?

- We will be mostly focused on **Electromagnetic Signals** (e.g. voltage), but the general concepts can be applied to any kind of signal



Example: voice at the output of a microphone

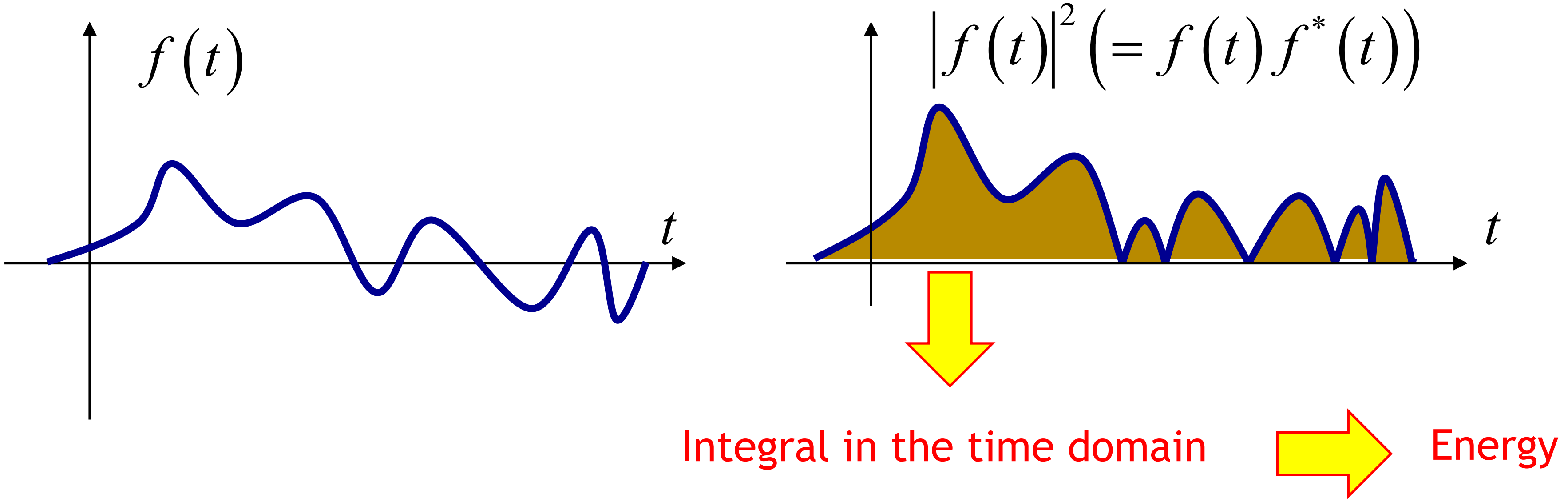


Example: Sismic signal

Energy of a Signal

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

$$\boxed{E\left(x\right) \triangleq \int_{-\infty}^{\infty} \left|x\left(t\right)\right|^{2} dt}$$


$f\left(t\right)$
t
$\left|f\left(t\right)\right|^{2}\left(=f\left(t\right)f^{*}\left(t\right)\right)$
t

Integral in the time domain ⇨ Energy

Power of a Signal

- Instantaneous power
  - It is a function of time that coincides with the squared module of the signal

$$P_{ist}(t) = |x(t)|^2$$

- Power (average)
  - Time average of the instantaneous power
  - We refer to this when we talk about power

$$\boxed{P(x) \triangleq \lim_{a \to \infty} \frac{1}{2a} \int_{-a}^{a} |x(t)|^2 \, dt}$$

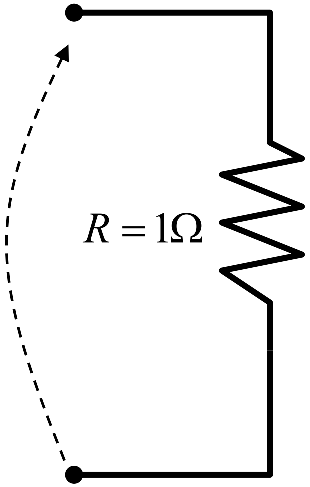
- Remark: Eenrgy and Average Power are associated with a real scalar number

Physical interpretation: resistor

- These concepts are related to the dual concepts seen in electronics classes
- Aside from a proportionality constant *R*, the previous definitions coincide with the physical definitions of **power** and **energy**

Voltage

$$f(t) = v(t)$$



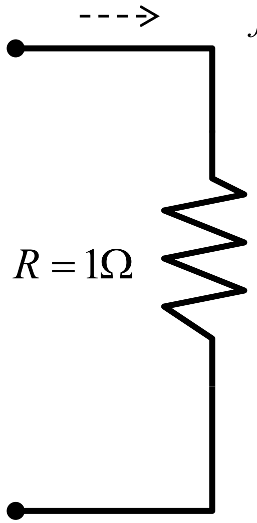
$$\Downarrow$$

$$P_{ist}(t) = \frac{v^2(t)}{R}$$

$$E = \frac{1}{R}\int_{-\infty}^{\infty} v^2(t)dt = E(f)$$

Current

$$f(t) = i(t)$$



$$\Downarrow$$

$$P_{ist}(t) = R \cdot i^2(t)$$

$$E = R\int_{-\infty}^{\infty} i^2(t)dt = E(f)$$

Signals Representation

- To analyze and process the signals, it is necessary to adequately represent them
- The definition of signals as "time functions" is NOT effective for many applications
- A signal can be represented as a **sum of elementary signals**
  - Thanks to the *scalar product* between signals

$$\left\langle \mathbf{x},\mathbf{y}\right\rangle = \left\langle x(t),y(t)\right\rangle \triangleq \int_{-\infty}^{\infty} x(t)\,y^{*}(t)\,dt \leftarrow$$

- The scalar product associates a (complex) **scalar number** to a pair of vectors or signals
- It is a measure of “similarity” among signals
- Two signals with zero scalar product are said to be **orthogonal**

  - Given a *complete orthonormal basis* for the signal x(t)

$$w_1(t) \quad w_2(t) \quad \cdots \quad w_M(t)$$

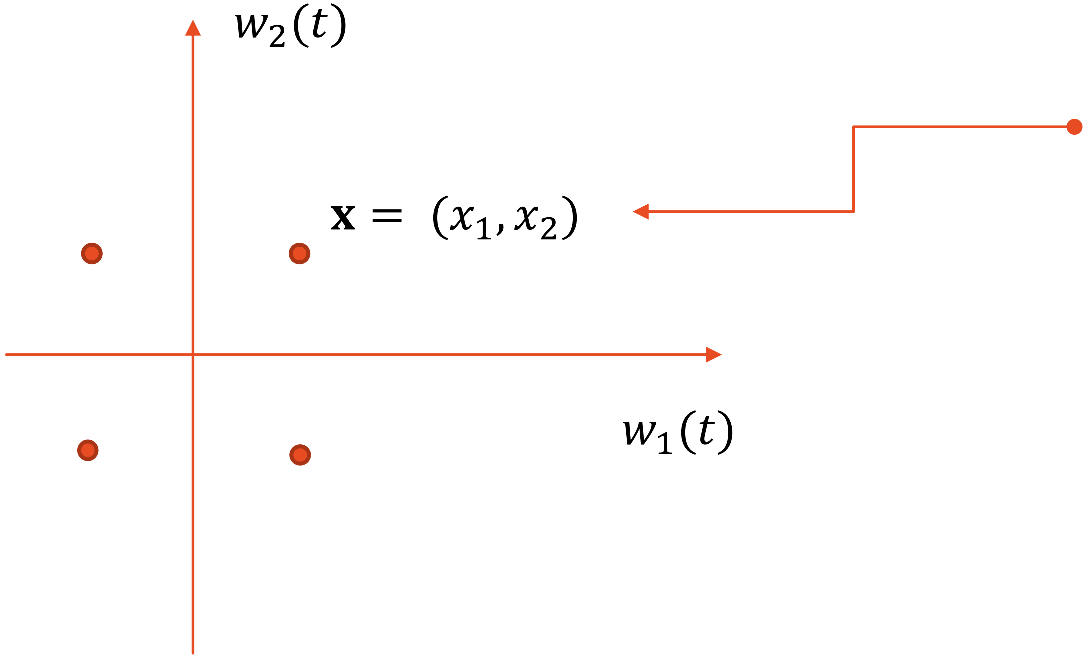
  - We can write the signal as a linear combination of basis functions

$$\boxed{x(t) = \sum_{i=1}^{M} \alpha_i\, w_i(t) \quad where: \quad \alpha_i = \langle x(t), w_i(t)\rangle = \int_{-\infty}^{+\infty} x(t)\cdot w_i^{*}(t)dt}$$

- This concept can be used
  - To associate signals with **vectors coefficients** (basis, modulations) $\mathbf{x} = (\alpha_1, \alpha_2, \ldots, \alpha_M)$
  - To associate signals with **frequency components** (spectral analysis)

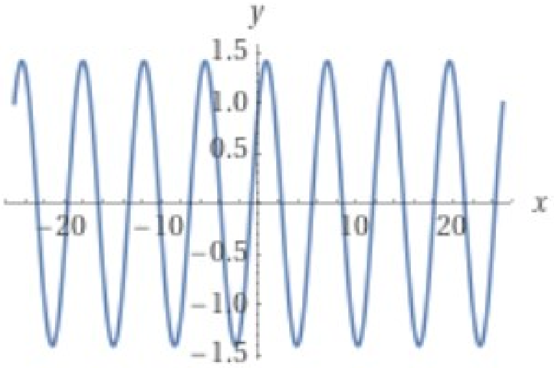
Signals Representation: I/Q Representation

- To associate signals with **vectors coefficients** (basis, modulations)
- Some basis are more important than others in practical applications:
  - $w_1\ (t) = \cos(2\pi f_0\ t)$ or *In-phase*
  - $w_2\ (t) = \sin(2\pi f_0\ t)$ or *Quadrature phase*



What is this signal?

$$x(t) = x_1 \cos(2\pi f_0 t) + x_2 \sin(2\pi f_0 t)$$



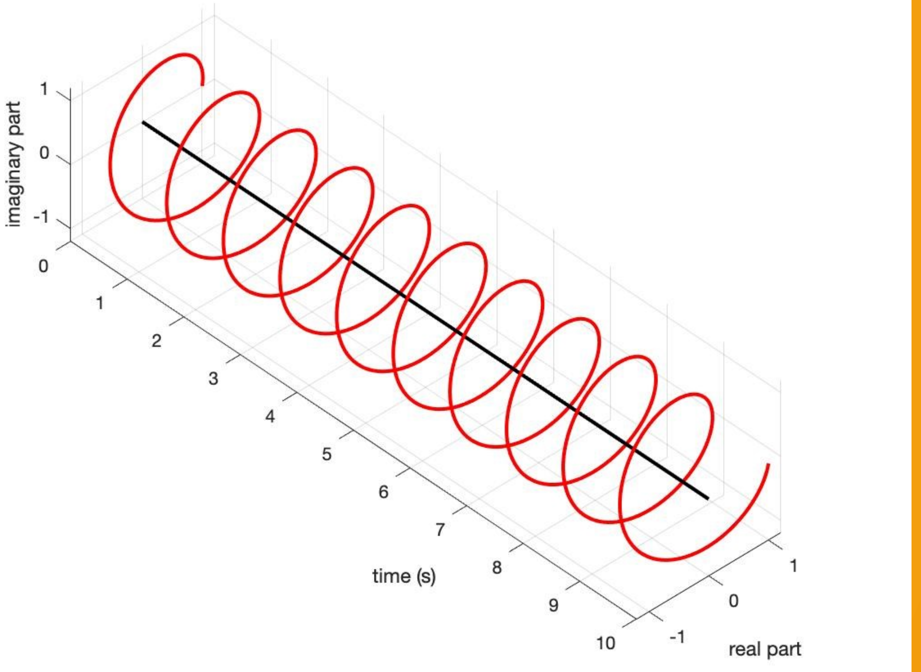
Contents

- Review of basic concepts for digital communications
  - Introduction
  - Digital Communications Overview
  - **Signals Representation and Processing**
    - Signal representation
    - **Frequency domain, filters, modulation**
    - Sampling Theorem and Discrete Time Signals
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

The Fourier Analysis

Euler's formula

- Let's consider the complex exponential $e^{j2\pi\frac{n}{T}t} = \cos\left(2\pi\frac{n}{T}t\right) + j\sin\left(2\pi\frac{n}{T}t\right)$
  - Made by complex sinusoidal signals with frequency $f_n = n/T$.



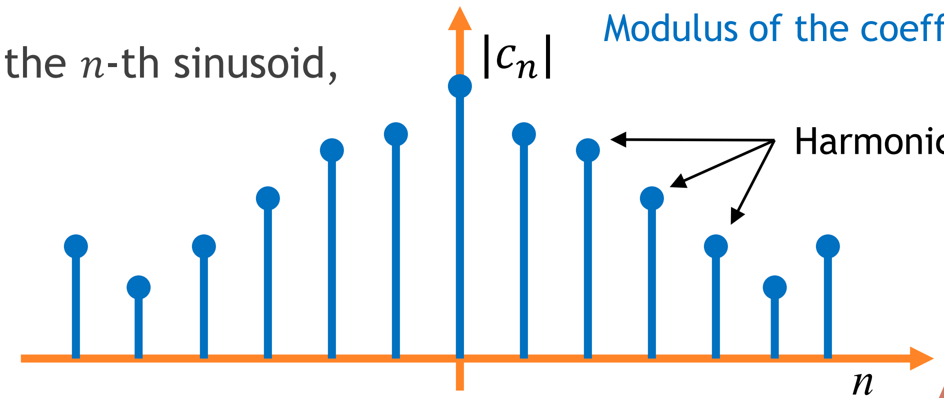
- It can be shown that this infinite set of functions

$$\boxed{w_n(t) = \frac{1}{\sqrt{T}} e^{j\frac{2\pi}{T}nt} \qquad -T/2 \le t \le T/2}$$

- Is a **complete basis** for all the signals limited in [-T/2,T/2] or periodic, i.e.

$$\boxed{x(t) = \frac{1}{\sqrt{T}} \sum_{n=-\infty}^{\infty} c_n e^{j\frac{2\pi}{T}nt}} \qquad c_n = \frac{1}{\sqrt{T}} \int_{-T/2}^{T/2} x(t) e^{-j\frac{2\pi}{T}nt} dt = \langle x(t), w_n(t) \rangle \qquad -\frac{T}{2} \le t \le \frac{T}{2}$$

  - Each coefficient c_n tells, for each frequency f_n of the n-th sinusoid, how much it «counts» in the signal $x(t)$



Modulus of the coefficients

Harmonics at $f_n = \frac{n}{T}$

The Fourier Analysis (cont’d)

- Extending the concept to **any signal** we get the *Fourier transform* of *x(t)*

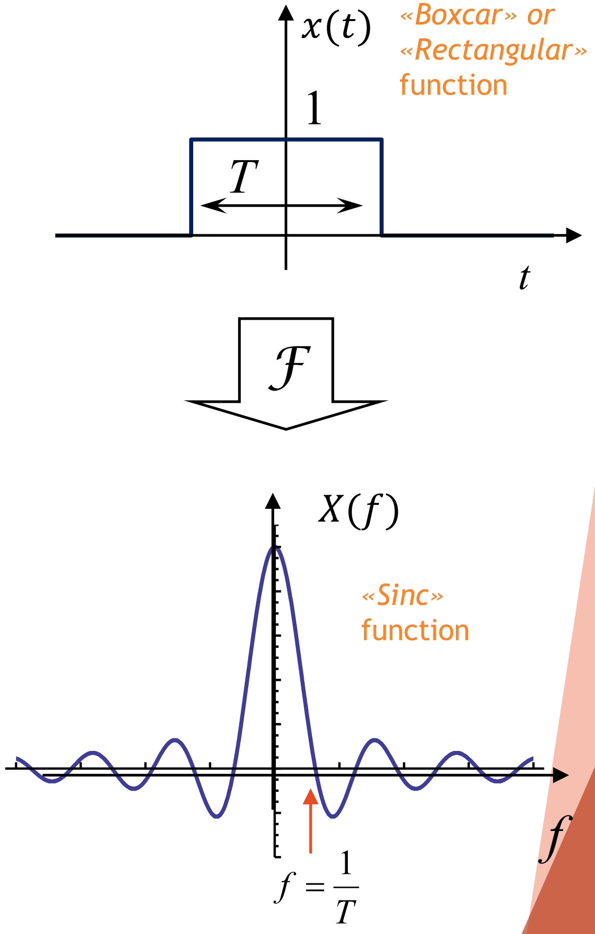
$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}\,dt$$

- And its *inverse*

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

- $X(f)$ indicates the "weight" (complex) of the **sinusoidal component** (complex) at frequency f for the generic signal $x(t)$
- The inverse F.t. tells us that we can decompose any signal into sinusoidal components at a given frequency *f*

- Important observations:
  - For each signal, we have a «***spectral***» **representation** (spectral analysis)
  - For each operation over a signal, there are equivalent **effects in the frequency domain**
  - **Finite duration** signals have **infinite support** in the frequency domain

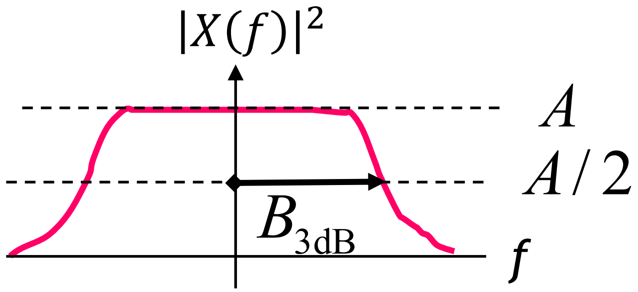


«Boxcar» or «Rectangular» function

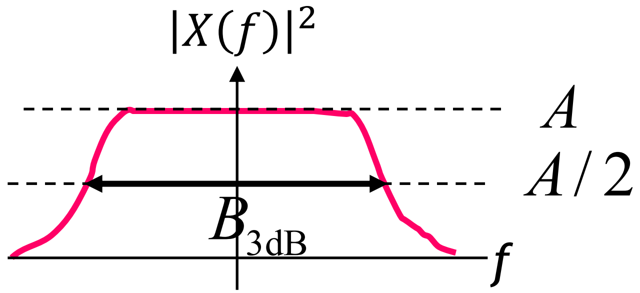
«Sinc» function

Bandwidth

- The bandwidth (or simply band) is the interval of frequencies occupied by a signal
- The definition of bandwidth as the support of the Fourier Transform of the signal is too restrictive.
  - Signals have often infinite support in frequency domain
  - But many systems are characterized by quasi-null frequency spectrum out of the main lobes
- Different definitions can be used but the most popular are related to the square of the modulus $|X(f)|$^2
  - E.g. 3dB Bandwidth



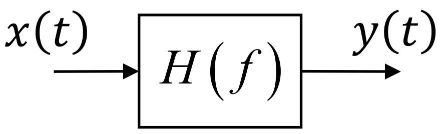
One-sided 3dB Bandwidth

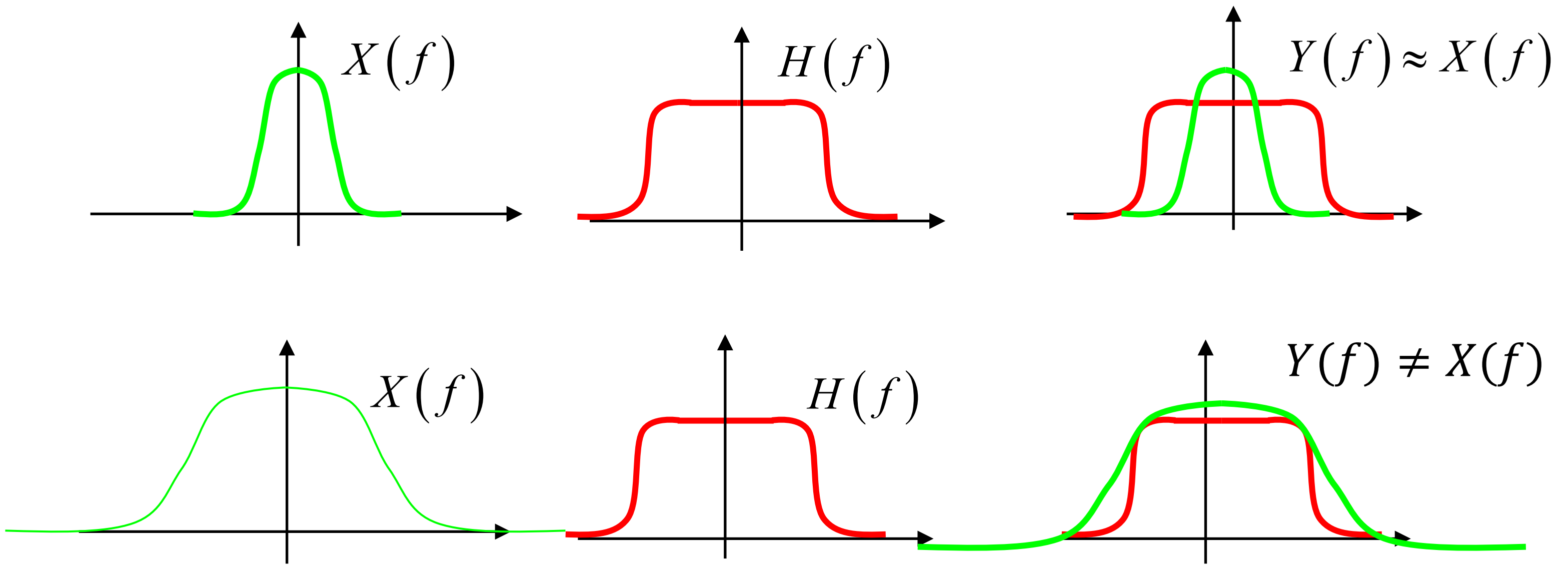


Two-sided 3dB Bandwidth

Bandwidth in Linear Systems

- The relationship between the bandwidth of the input signal and the bandwidth of a system is usually very important
- A set of operations applied to signals can be modeled as a *system*
  - When a system is used to pass/remove particular frequencies of a signal, it can be regarded as a *filter*
- ***Linear time-invariant*** **systems** (LTI) are modeled by a **frequency response** *H(f)*
  - And we have that $Y(f) = X(f)H(f)$

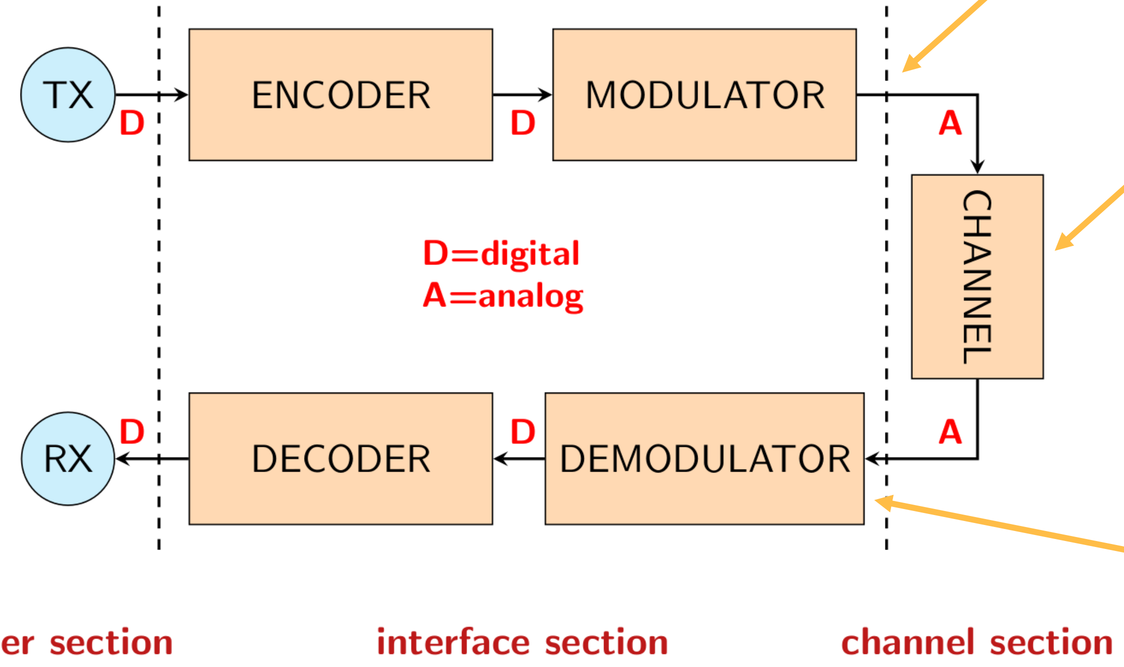



Input bandwidth is narrower than system bandwidth

Input bandwidth is wider than system bandwidth

Filters

- **Systems/filters** can be used to model desired and undesired effects over signals
  - Process the signals to obtain desired features
  - Model channel effects



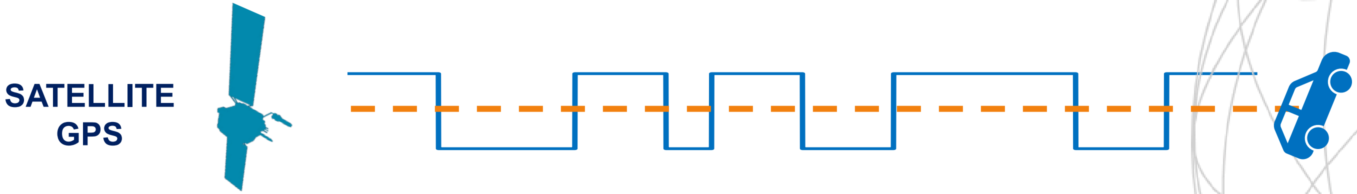
Share a wireless medium

Model the channel

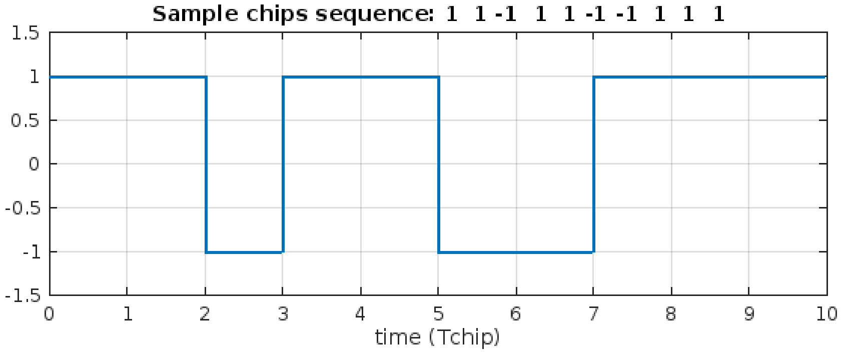
Mitigate undesired effect through equalizers

An example from the GPS world

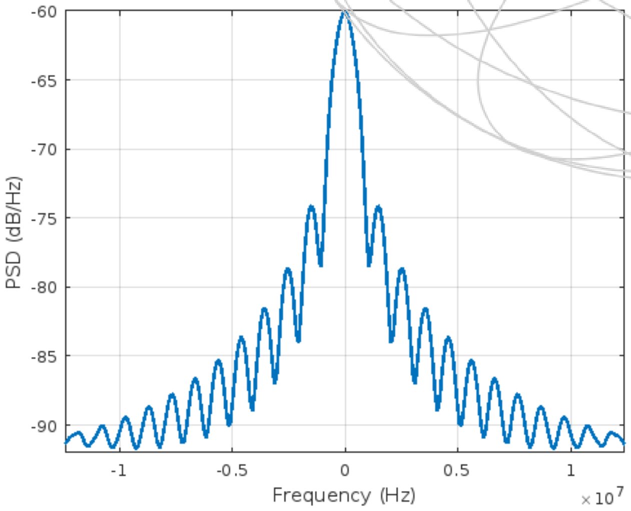
- A GPS satellite generates, approximately, the following time-domain waveform to be broadcasted



- Thanks to the Fourier transform and its properties, we know which are the strongest **frequency components** of the signal
- We get, approximately, this equivalent representation



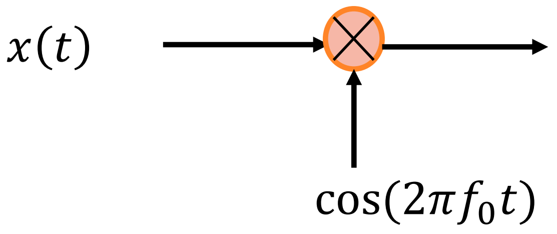
Time-domain representation



Frequency-domain representation

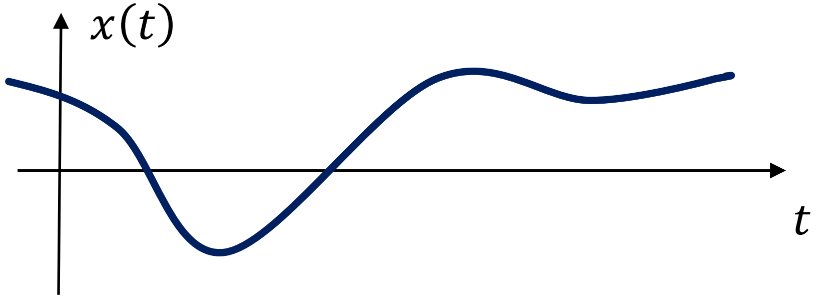
An important property: Signal Modulation

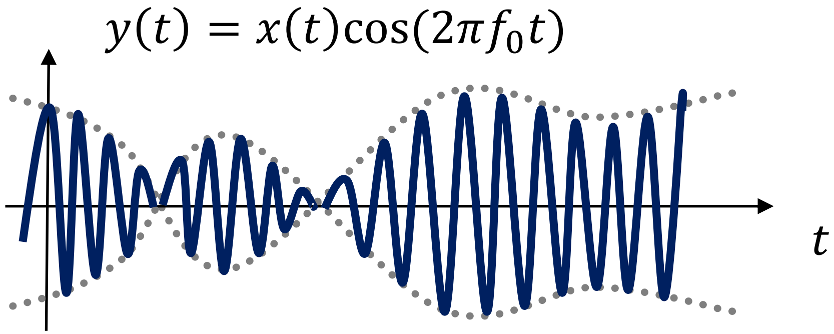
- Multiplying a signal by a sinusoidal function, results in a frequency shift

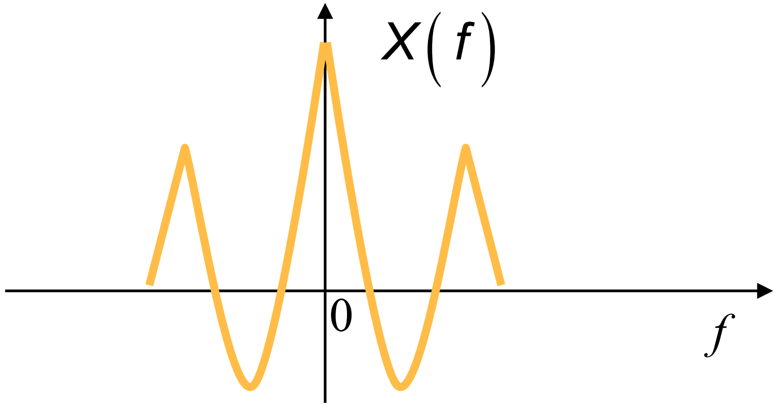


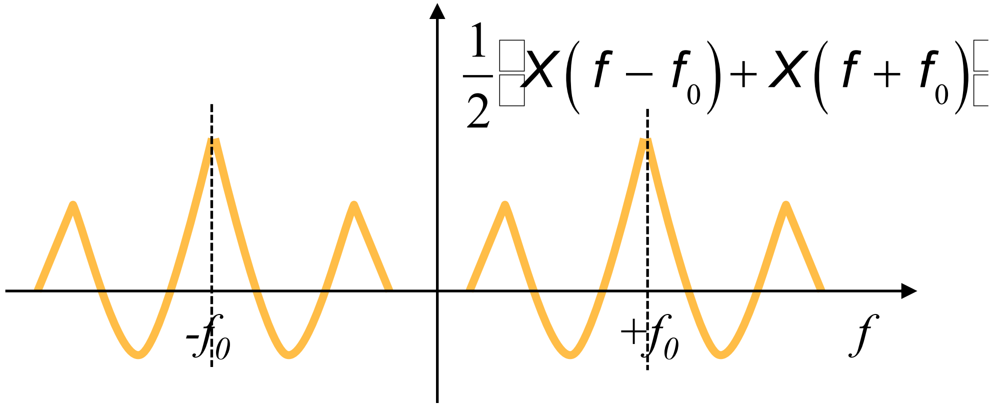
$$y(t) = x(t)\cos(2\pi f_0 t)$$

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



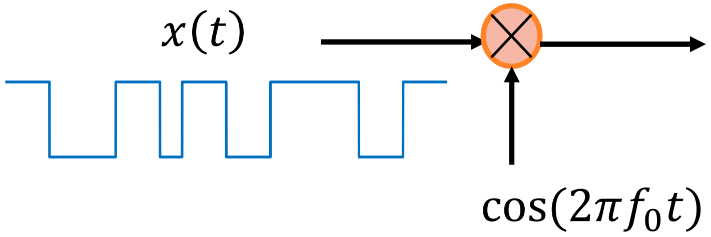






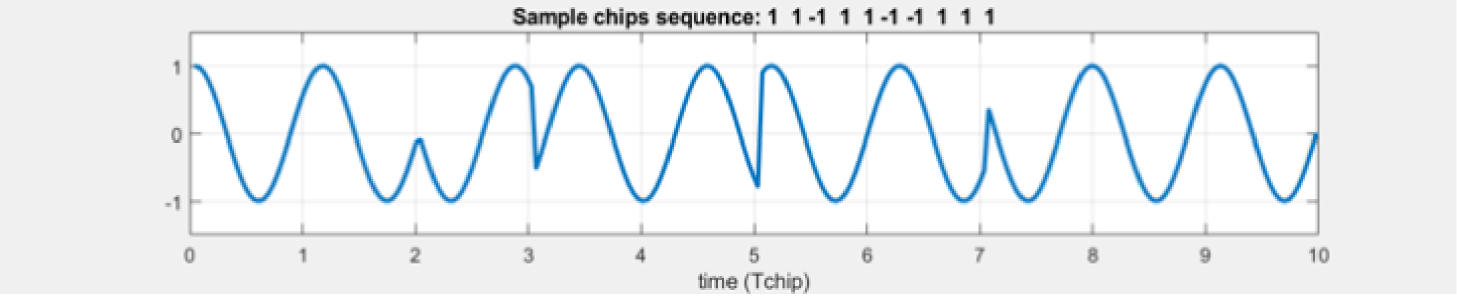
Signal Modulation: Example

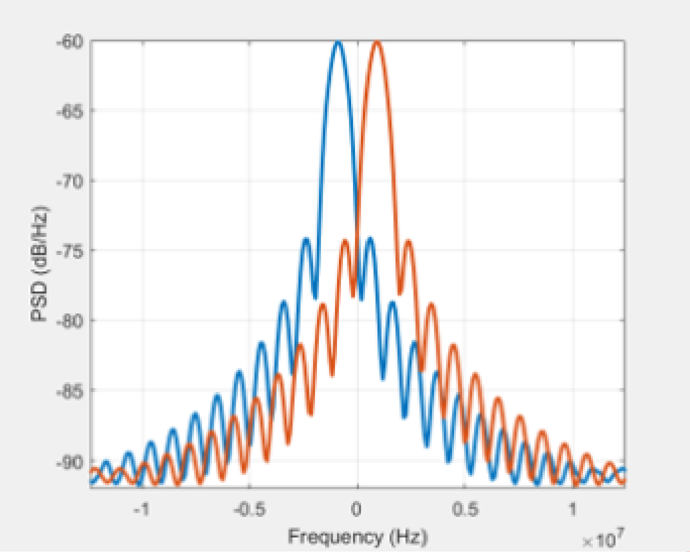
- Sine wave modulated by a GPS signal



$$y(t) = x(t)\cos(2\pi f_0 t)$$

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



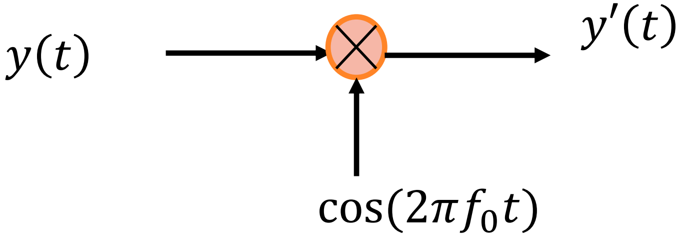


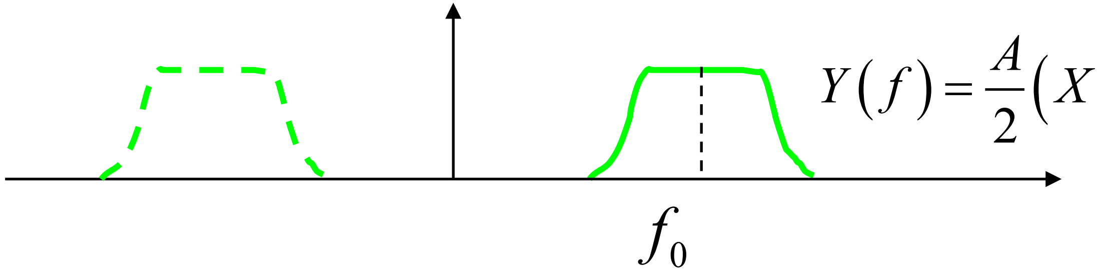
This result is FUNDAMENTAL for most wireless modulations to move the spectral content of the original signal to the most appropriate frequency band

How to go back to the original signal?

Signal Demodulation

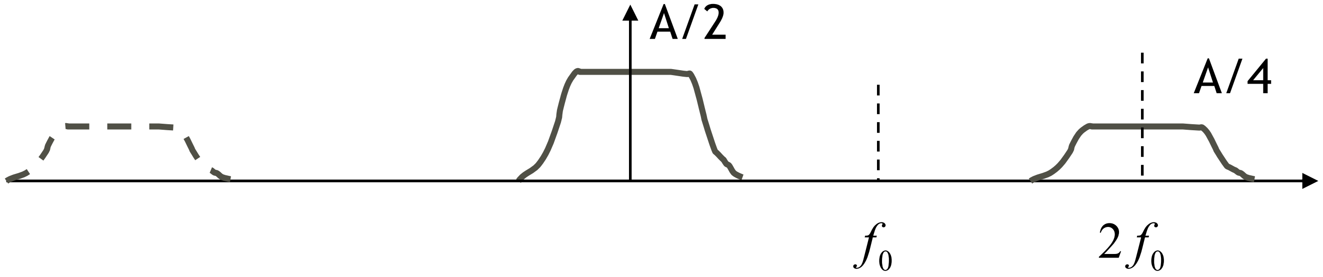
- When received, the signal can be recovered by
  - multiplying it for a sinusoid at the same frequency
  - Low pass filtering





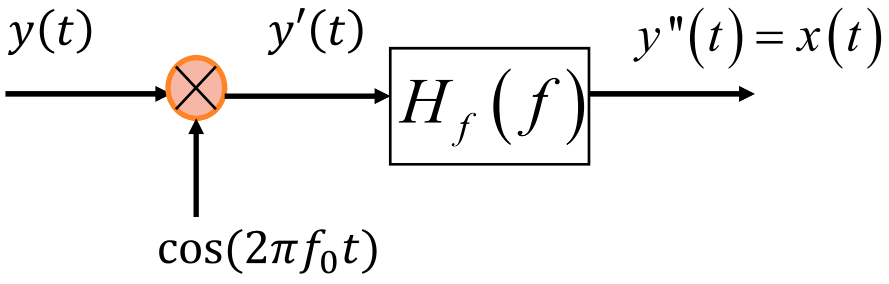
$$Y(f)=\frac{A}{2}\left(X(f-f_0)+X(f+f_0)\right)$$

$$Y'(f)=\frac{A}{2}X(f)+\frac{A}{4}\left(X(f-2f_0)+X(f+2f_0)\right)$$



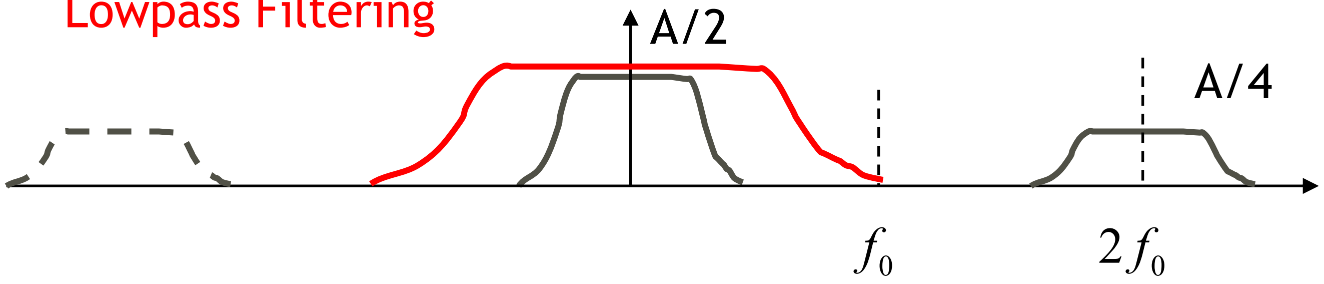
Signal Demodulation

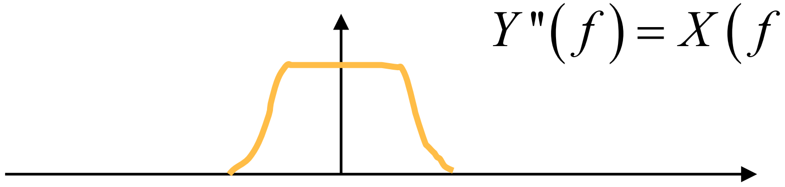
- When received, the signal can be recovered by
  - multiplying it for a sinusoid at the same frequency
  - Low pass filtering



$$Y'(f)=\frac{A}{2}X(f)+\frac{A}{4}\left(X(f-2f_0)+X(f+2f_0)\right)$$

Lowpass Filtering

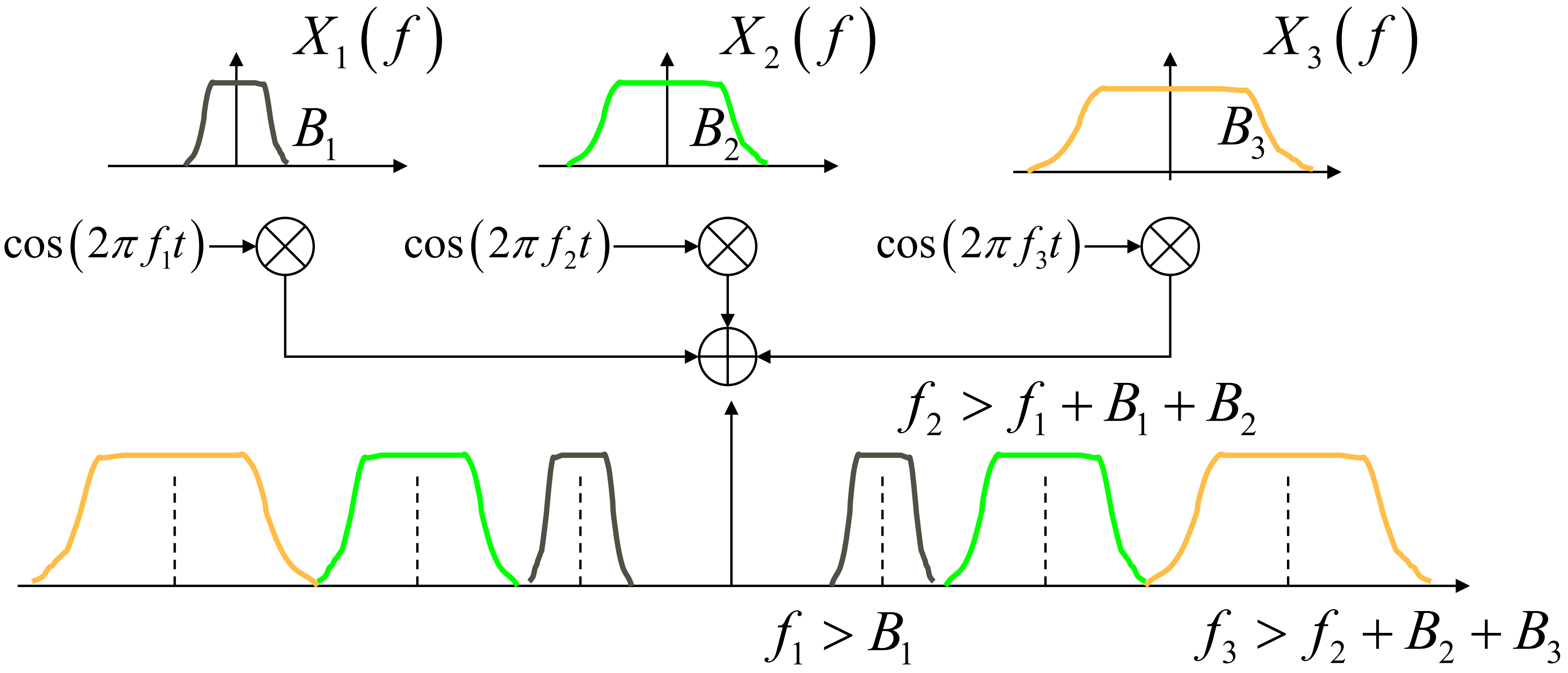




$$Y''(f)=X(f)$$

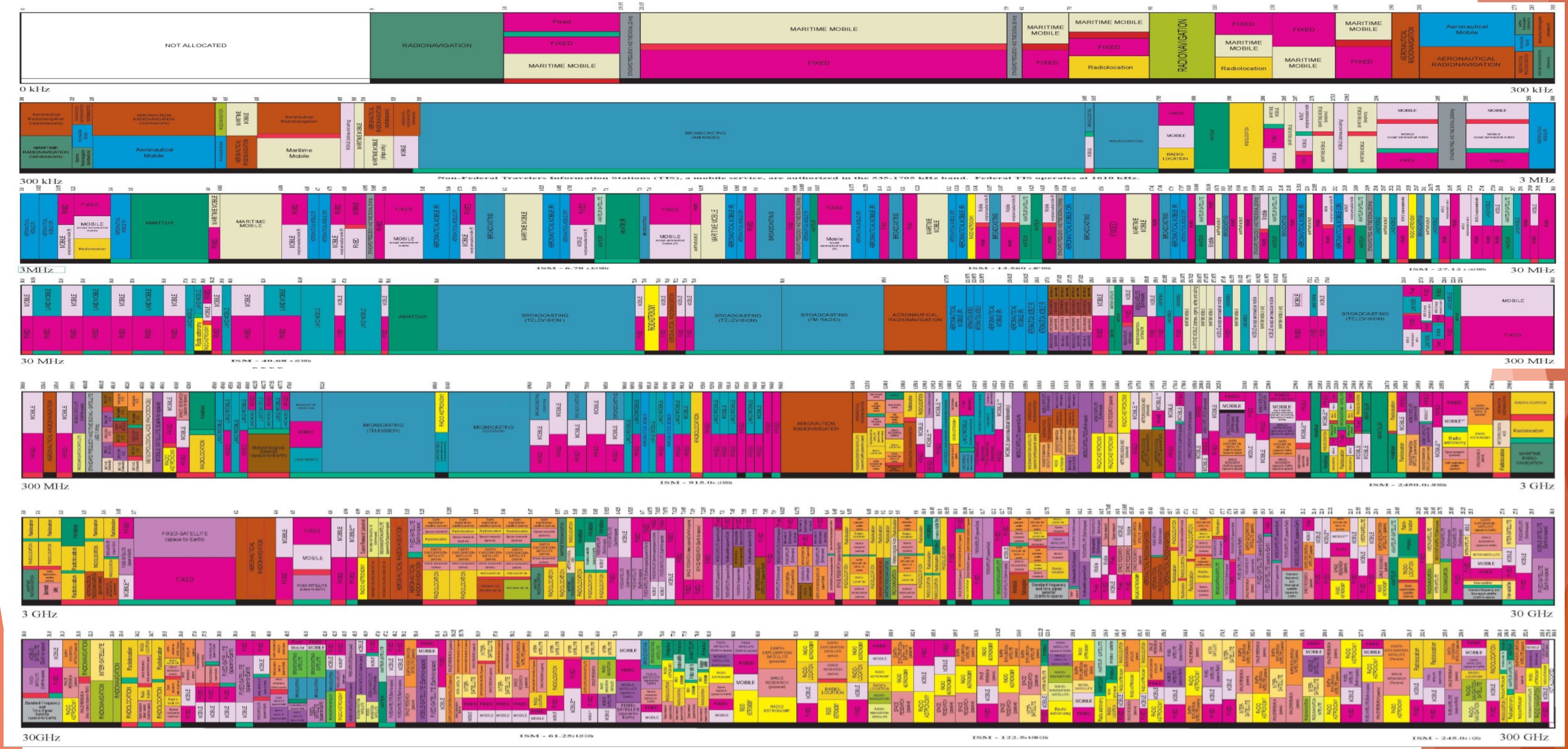
Frequency multiplexing (FDM)

- Different signals with overlapping bandwidths can be **frequency-modulated** in different portions of the spectrum.
- Once they are received they can be **de-multiplexed** withouth distortions.



0-300 GHz Spectrum Allocation

https://upload.wikimedia.org/wikipedia/commons/c/c7/United_States_Frequency_Allocations_Chart_2016_-_The_Radio_Spectrum.pdf



Contents

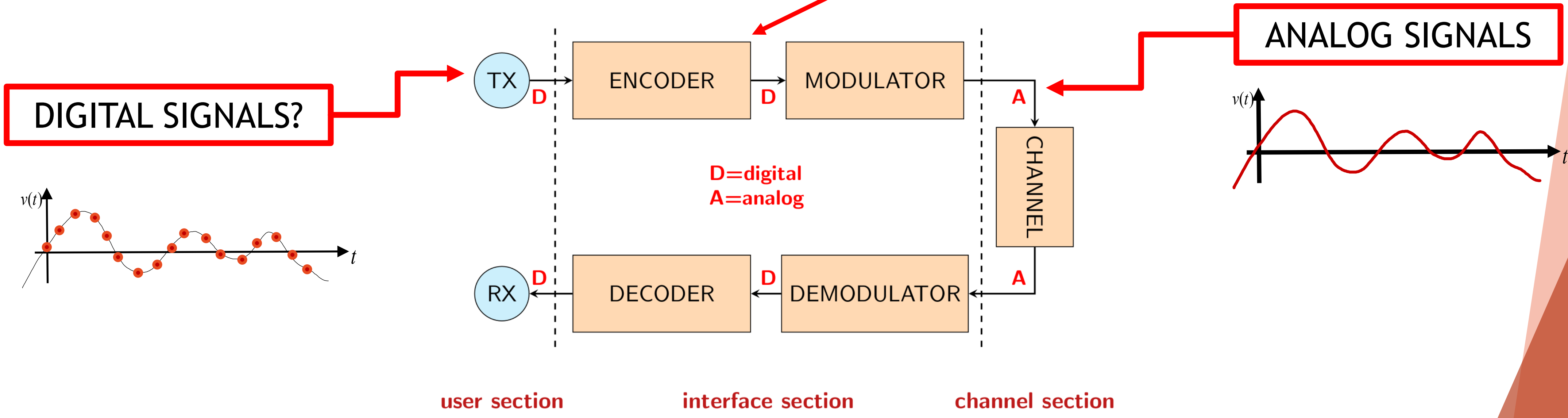
- Review of basic concepts for digital communications
  - Introduction
  - Digital Communications Overview
  - **Signals Representation and Processing**
    - Signal representation
    - Frequency domain, filters, modulation
    - **Sampling Theorem and Discrete Time Signals**
  - Signals Transmission and Reception
    - Digital Modulations
    - AWGN channel and equalization
    - Received symbols and decision regions
    - Link Budget
    - Multiplexing / Multiple Access schemes (FDM/A, TDM/A, CDM/A)
    - Source and channel coding

Source of information

- We have now acquired some tools to deal with signals. How do we use them?
- Which kind of **information** do we need to transmit?
  - Analog
  - Digital
- Digital signals allow for more sophisticated processing methods
  - error detection and correction, data compression, etc.
- How to **convert** an analog signal in a numerical signal?

Bits

…001101010100…



DIGITAL SIGNALS?

ANALOG SIGNALS

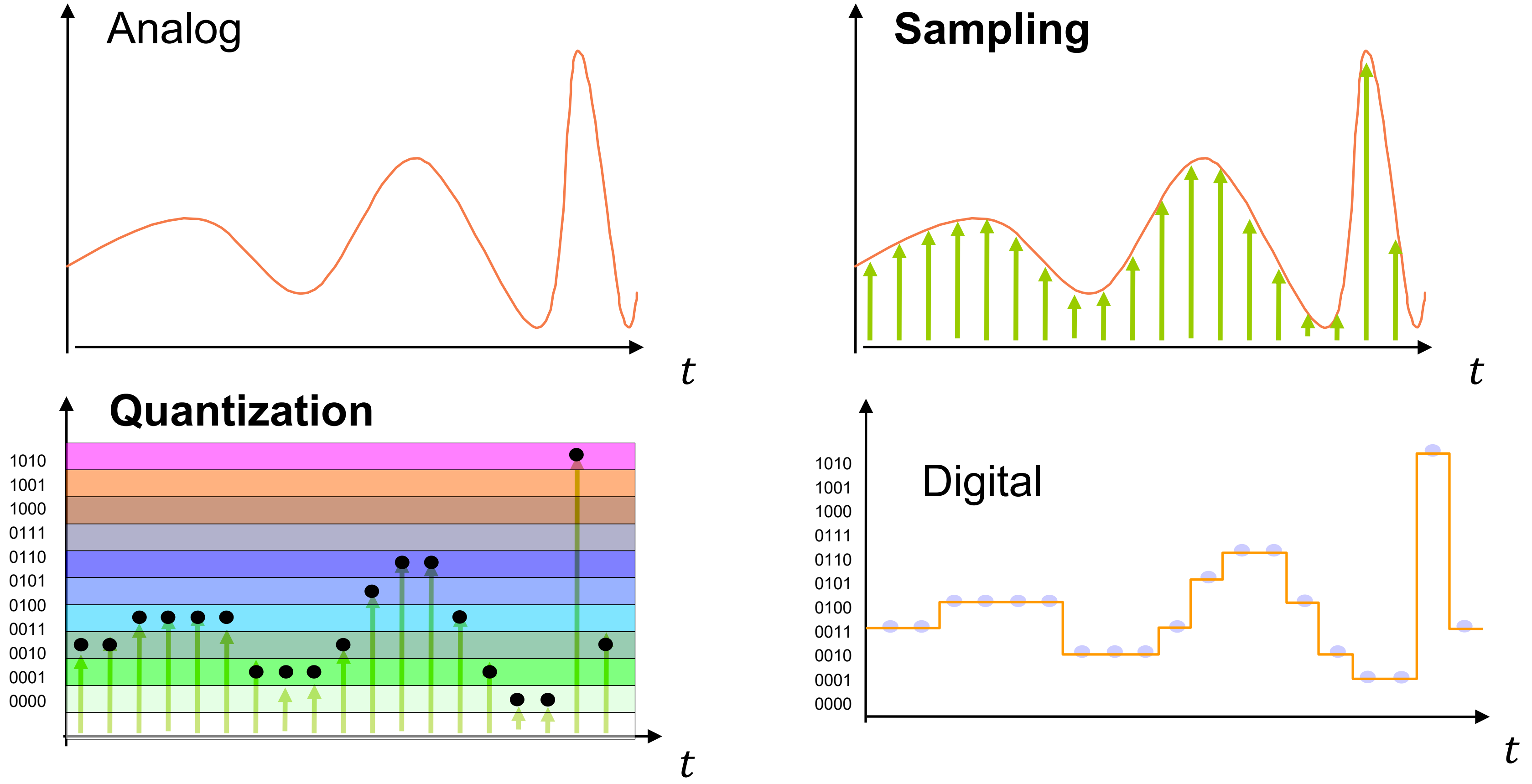
D=digital
A=analog

user section

interface section

channel section

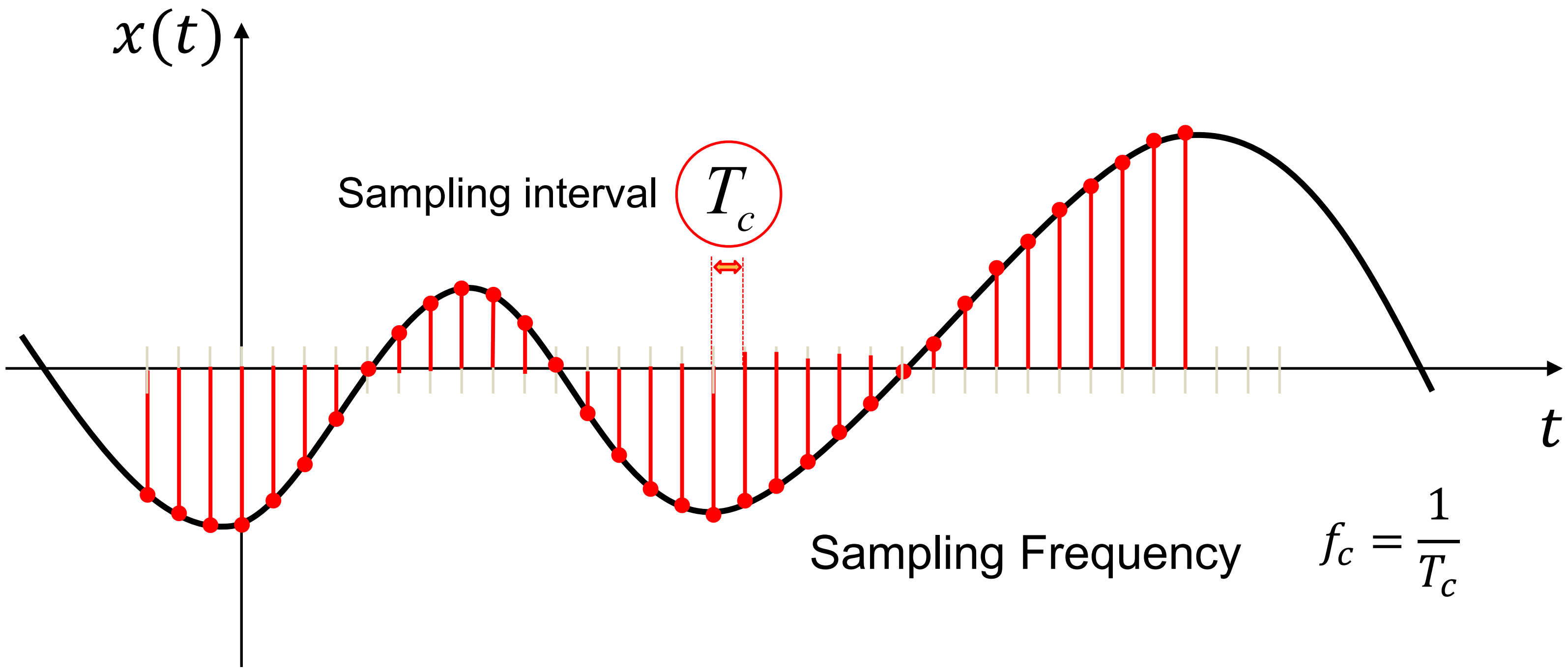
Analog-to-Digital Conversion



0011 – 0011 – 0100 – 0100 – 0100 – 0100 – 0010 – 0010

Sampling theorem

- ***Nyquist Theorem***: A continuous time signal can be sampled and perfectly reconstructed from its samples if the sampling frequency is greater than twice the "band" of the signal.

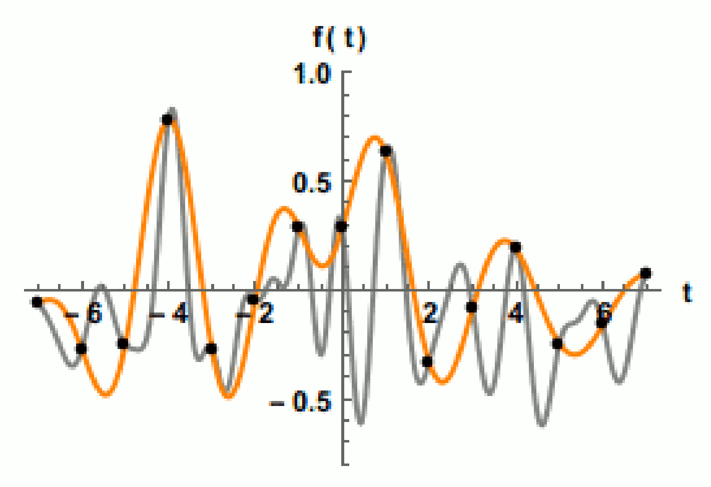


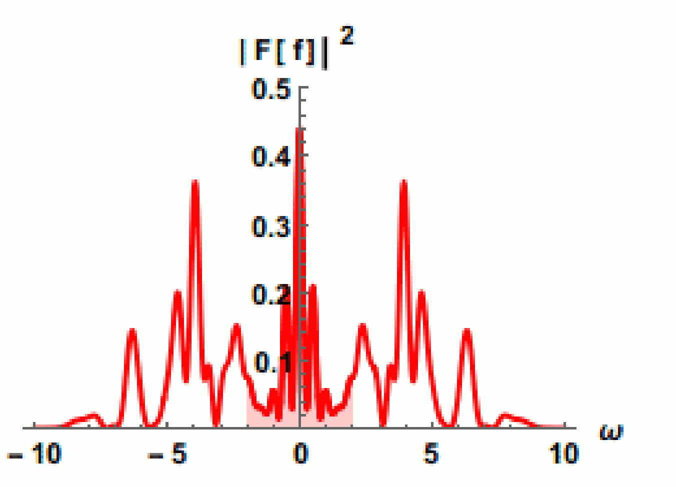
Sampling theorem

- ***Nyquist Theorem***: A continuous time signal can be sampled and perfectly reconstructed from its samples if the sampling frequency is greater than twice the "band" of the signal.

$$\boxed{f_c \triangleq \frac{1}{T_c} > 2B \rightarrow T_c < \frac{1}{2B}}$$

B is the one-side bandwidth of the analog signal.


f(t)
1.0
0.5
– 0.5
t
– 6
– 4
– 2
2
4
6


| F[f]| 2
0.5
0.4
0.3
0.2
0.1
ω
– 10
– 5
0
5
10