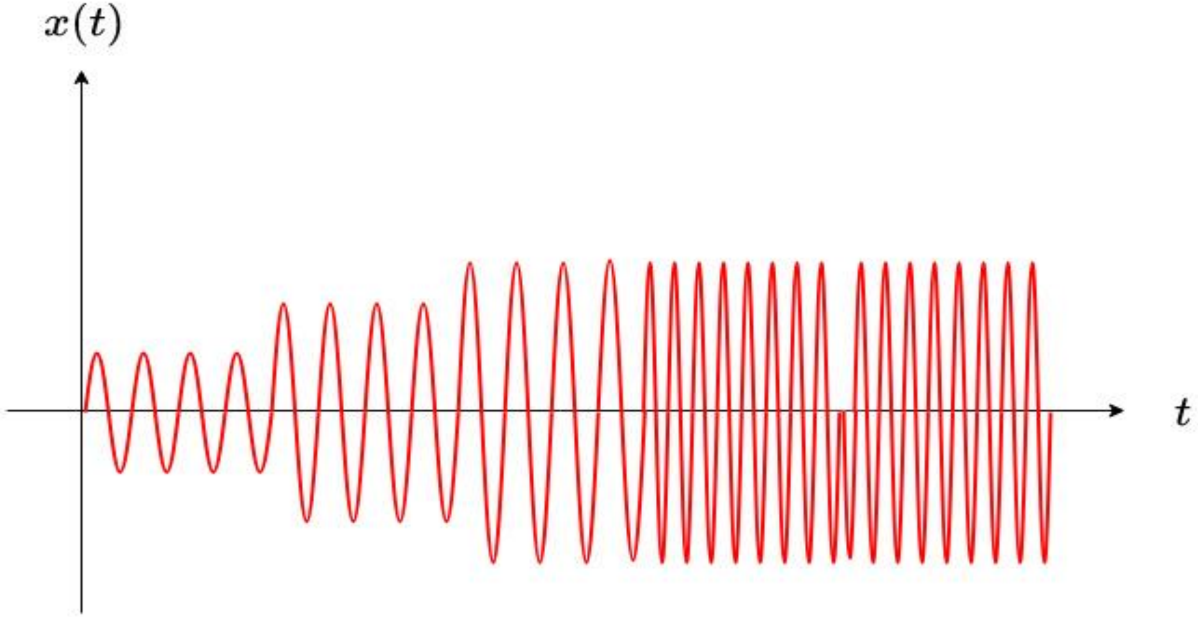
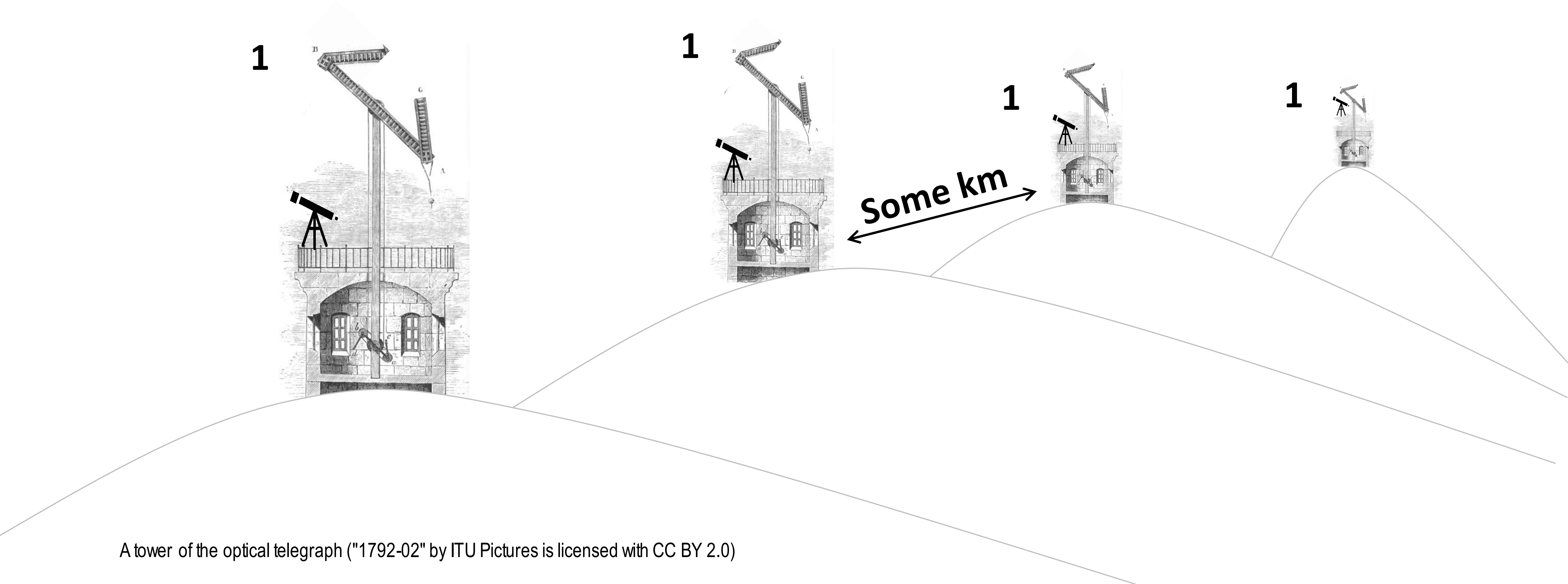


1- The Physical Layer

“Wireless” well before radios…

Chappe's optical telegraph (late 18th century)

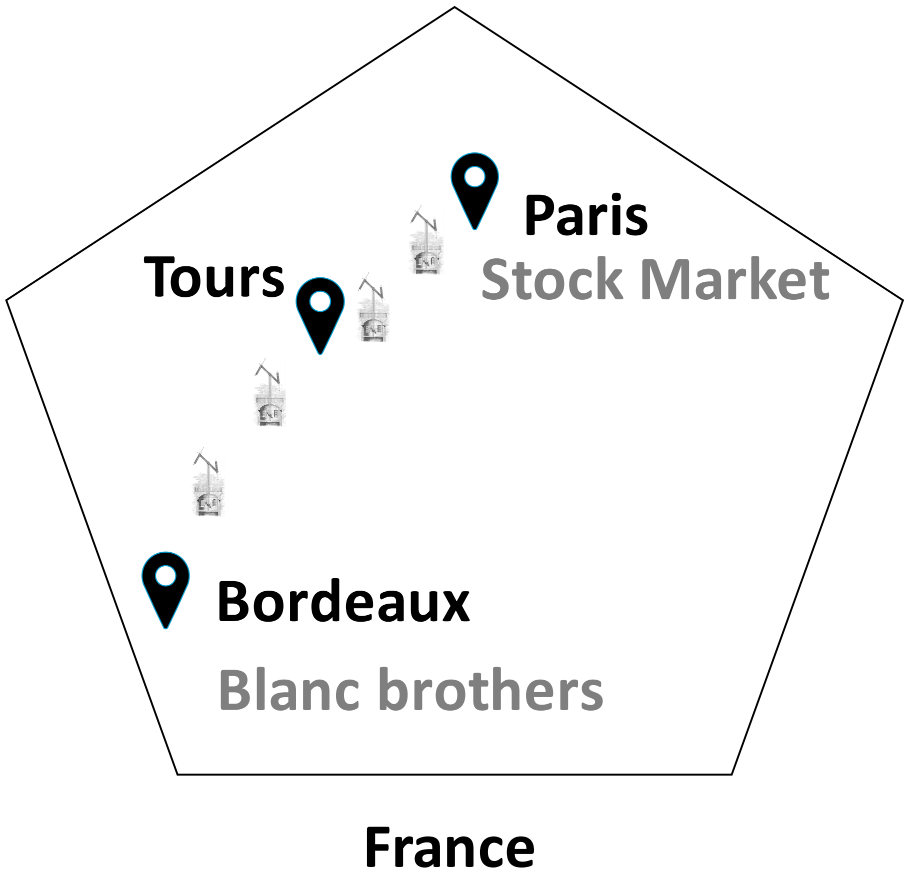


A smart fraud (1834-1837)

Blanc brothers' goal
Get stock market news before competitors

The solution
Hack the optical telegraph
Covert channel faster than mail

How??
Exploit error correction!



Hiding stock market trends

“Backspace” for error correction

Legitimate message

Come t↑’\b’o P↓’\b’aris at once

Market prices going up or down

1. Added by an accomplice operator in Tours
2. Observed by an accomplice in Bordeaux
2. Discarded by legitimate receiver thanks to ‘\b’

References

"1834: The First Cyberattack - Schneier on Security," accessed June 28, 2021, https://www.schneier.com/blog/archives/2018/05/1834_the_first_.html.

"Journal Des Débats Politiques et Littéraires," issue, Gallica, January 29, 1837, https://gallica.bnf.fr/ark:/12148/bpt6k4393846.

"What the Count of Monte Cristo Can Teach Us About Cybersecurity - IEEE Spectrum," IEEE Spectrum: Technology, Engineering, and Science News, accessed June 28, 2021, https://spectrum.ieee.org/tech-talk/telecom/security/what-the-count-of-monte-cristo-can-teach-us-about-cybersecurity.

Radio communications

A brief history

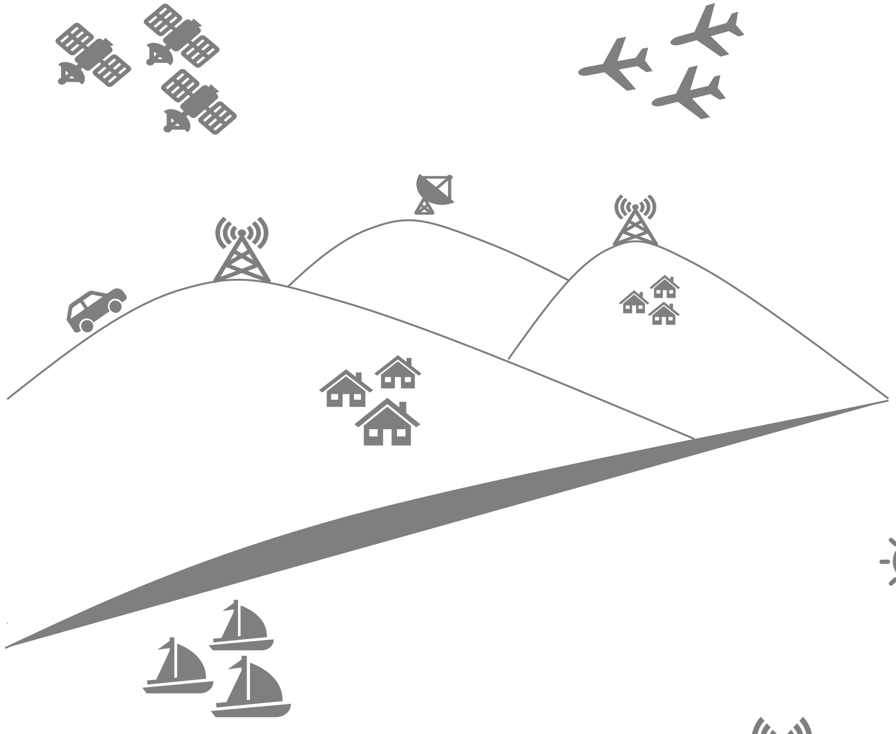
1950

2020

End of the 19th Century
Electromagnetism
Radio communications

20th Century
Huge development
Many applications + Integration

21st Century
Integration + computation + embedded
Smartphones, Embedded, IoT, sensors
Software Defined Radios



How many radios?

Broadcast Radar IoT

Positioning

Mobile

Embedded

How many radios on a smartphone?

GNSS (km)

Cellular (km)

FM (km)

WiFi (m)

BT/BLE (m)

NFC (mm)

UWB (m)

References

G. R. M. Garratt, T. B. A. Senior, and John L. Volakis, The Early History of Radio: From Faraday to Marconi (Institution of Engineering and Technology, 1994).

Massimo Guarnieri, “A Question of Coherence [Historical],” IEEE Industrial Electronics Magazine 10, no. 3 (September 2016): 54–58, https://doi.org/10.1109/MIE.2016.2590718.

“Hedy Lamarr,” in Wikipedia, June 25, 2021, https://en.wikipedia.org/w/index.php?title=Hedy_Lamarr&oldid=1030354762.

How do radio communications work?

(A minimalistic overview)

The goal

Transmit information

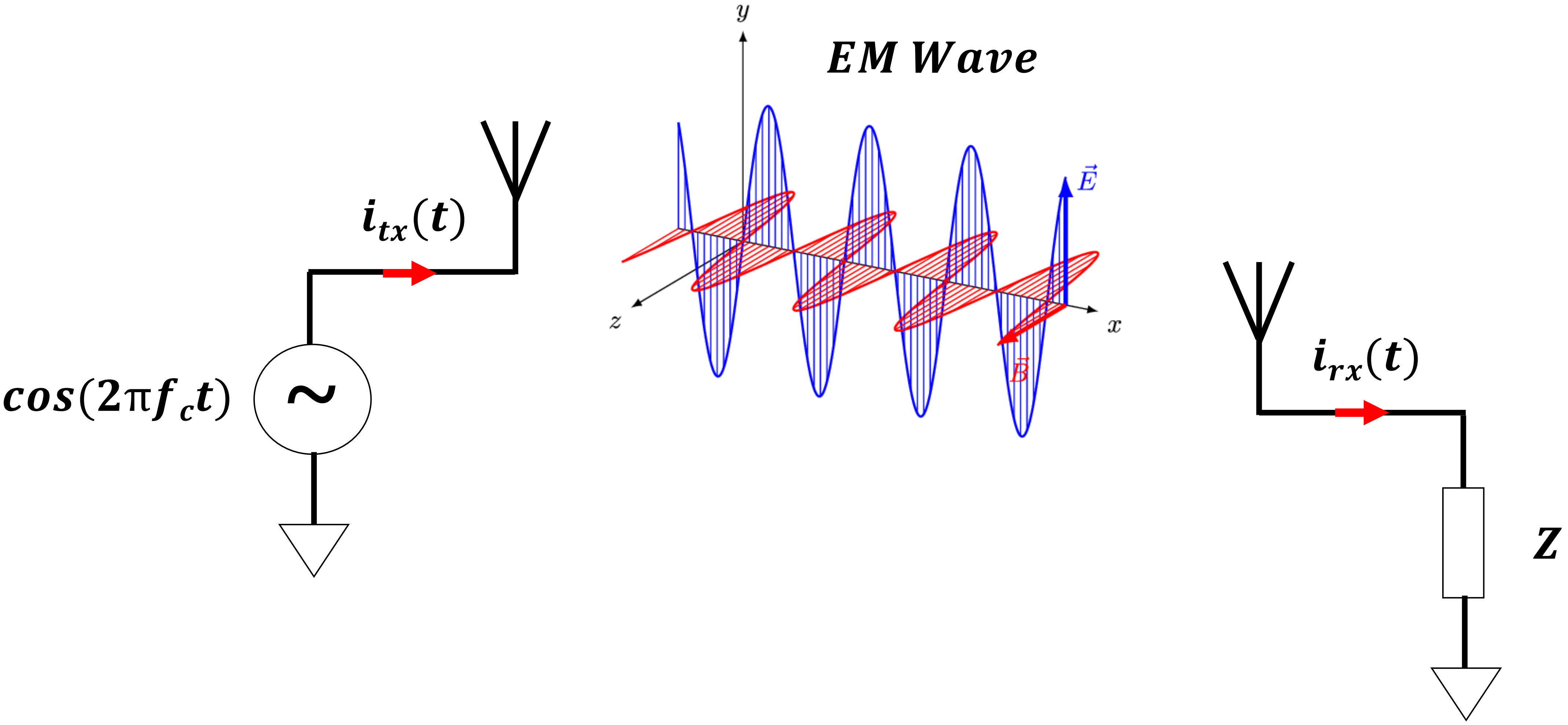
Which physical signal?

How to encode information?

What circuits?

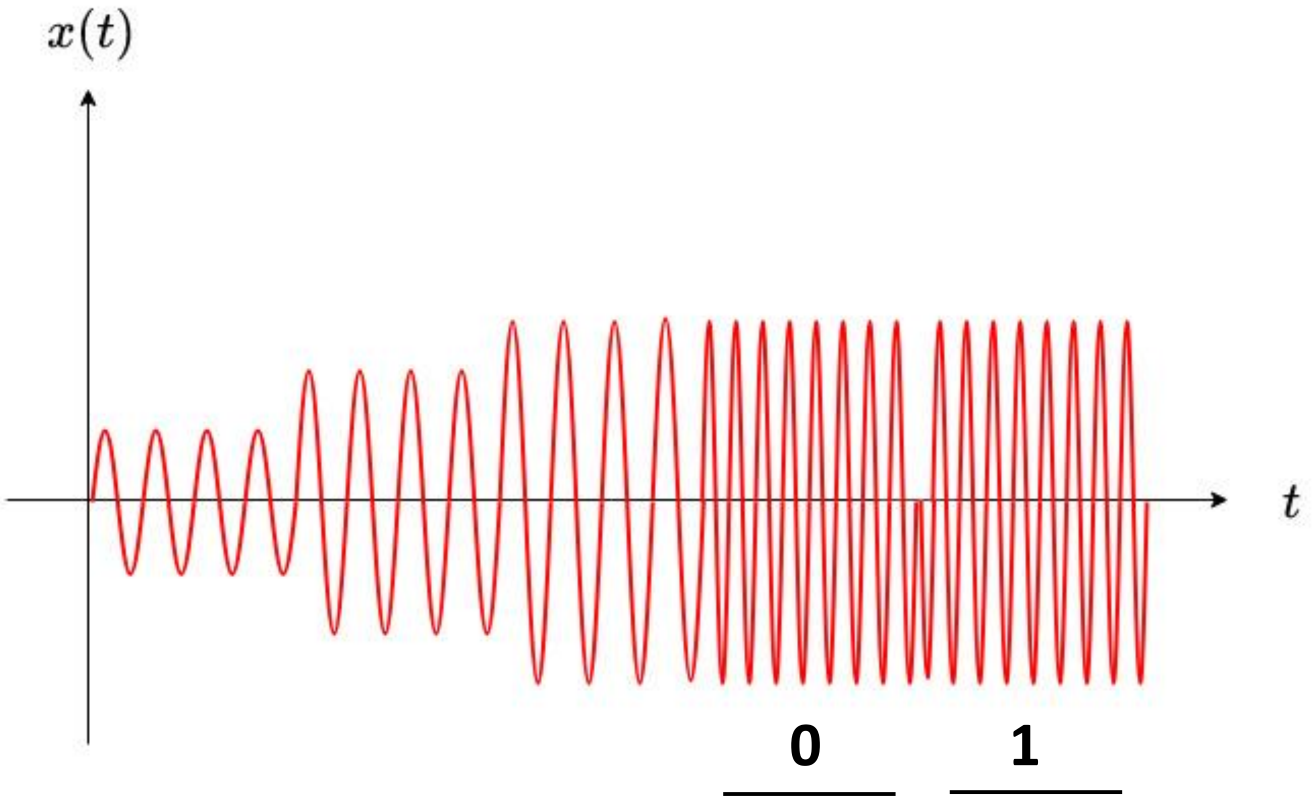
How to deal with errors?

Propagation

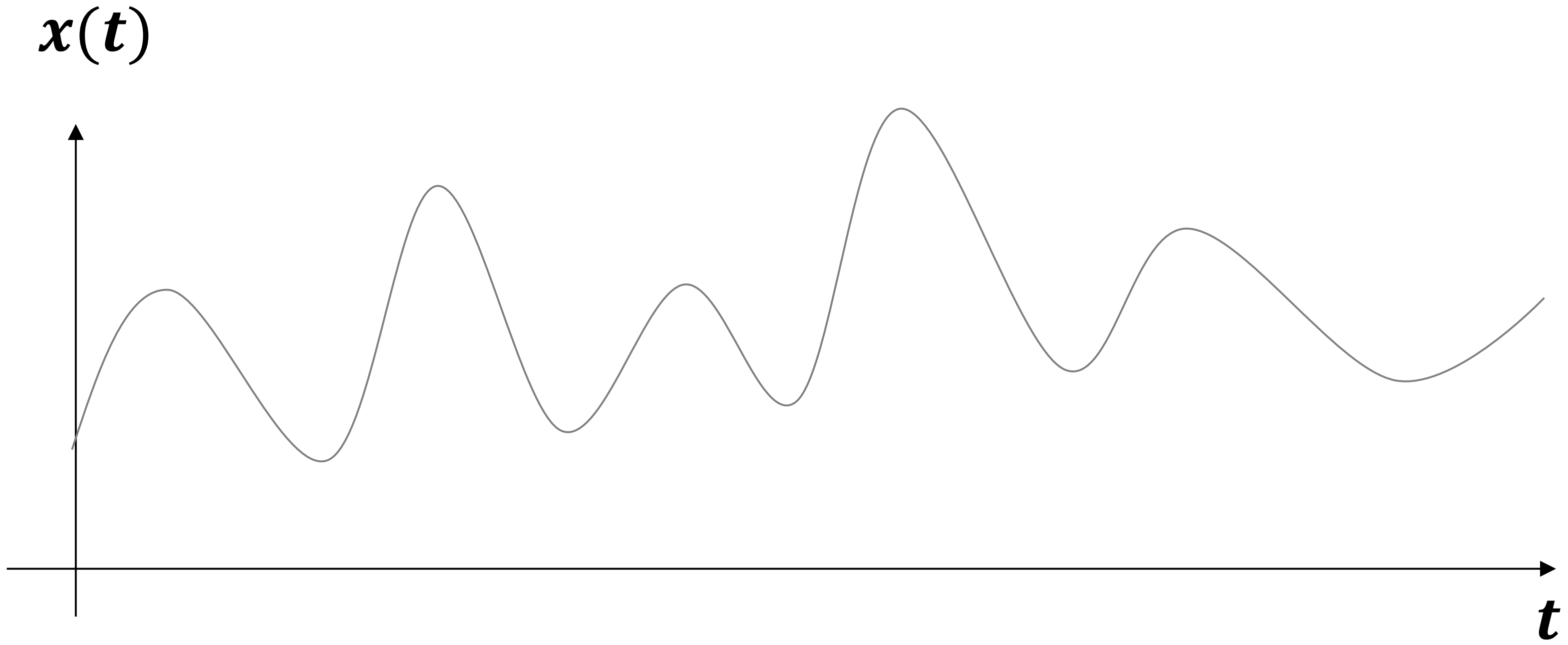


Transmitting information: Modulation

Intuition
Sinusoidal radio signal (carrier)
Modulate (information)
- Amplitude
- Frequency
- Phase



Some math…

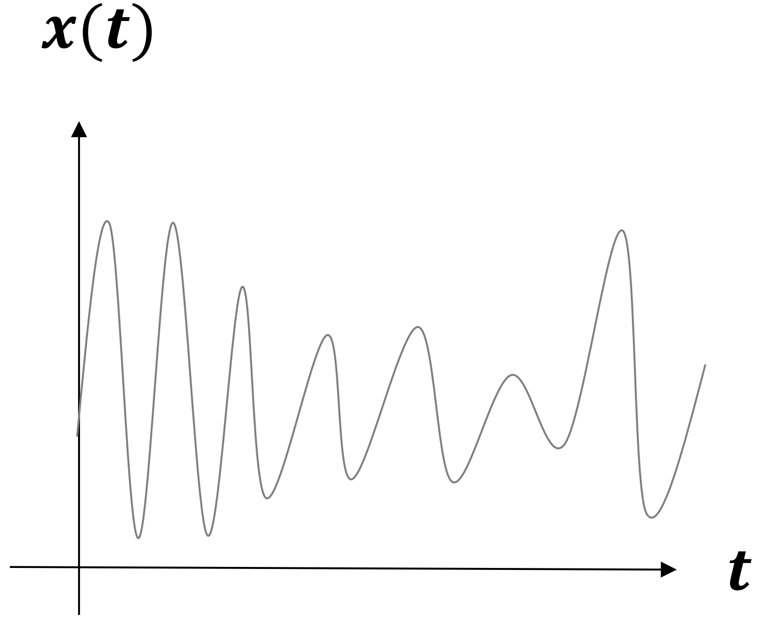


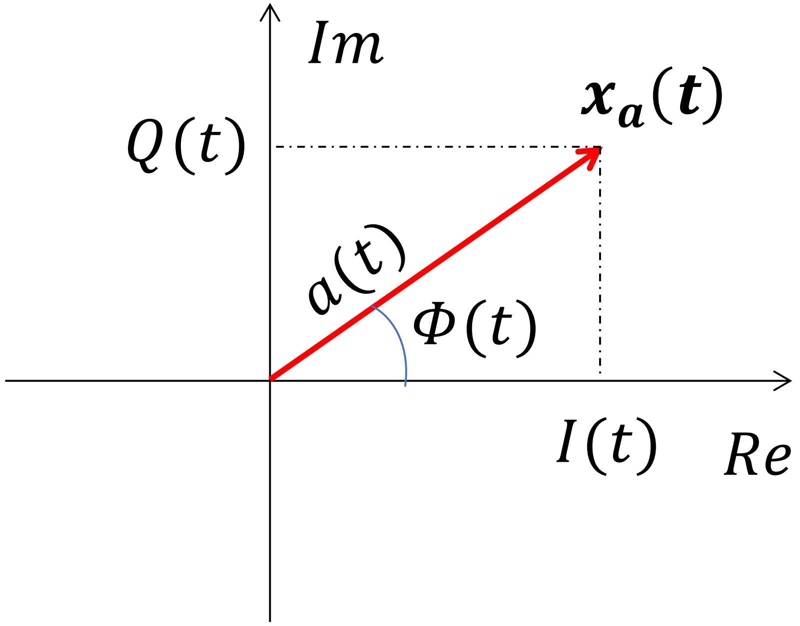
A signal

E.g., a quantity that varies over time

Some math…

Intuition
See the signal as the projection on the real axis of a rotating vector in the complex plane





Analytic signal representation

$$x(t) = Re\{x_a(t)\} = Re\left\{a(t)e^{i\Phi(t)}\right\} = a(t)cos(\Phi(t))$$

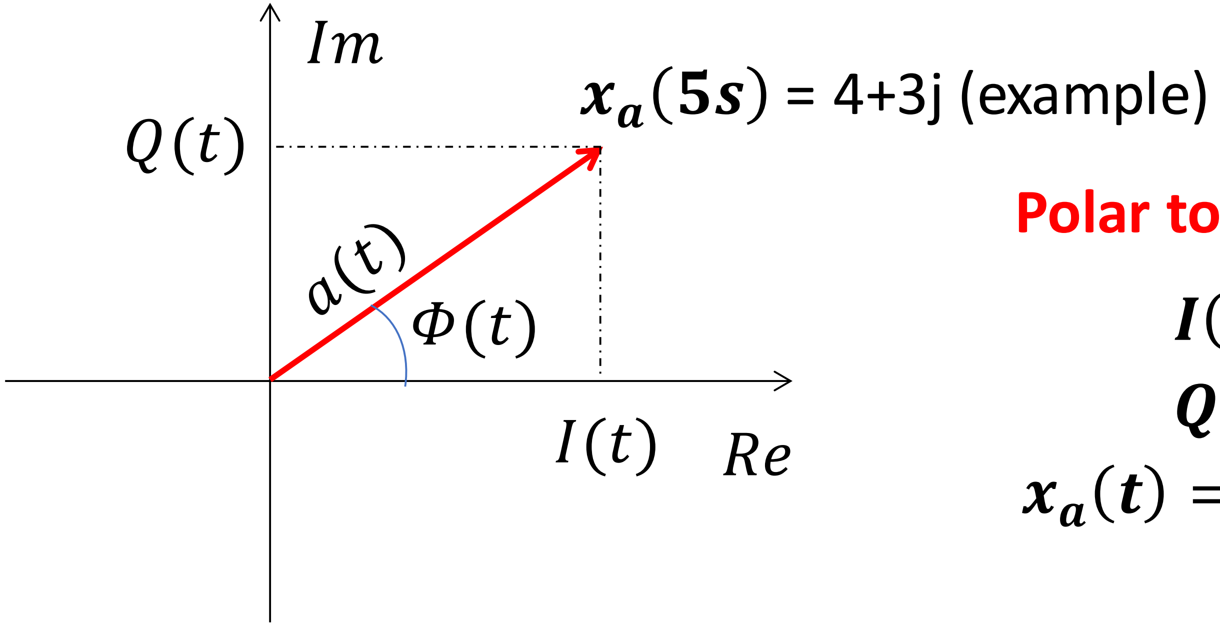
Analytical signal

$$x(t) = Re\{\boxed{x_a(t)}\} = Re\{a(t)e^{j\Phi(t)}\} = \boxed{a(t)}cos(\boxed{\Phi(t)})$$

Analytic signal **Amplitude** **Phase**

$$f(t) = \frac{1}{2\pi}\frac{d\Phi(t)}{dt}$$

Frequency

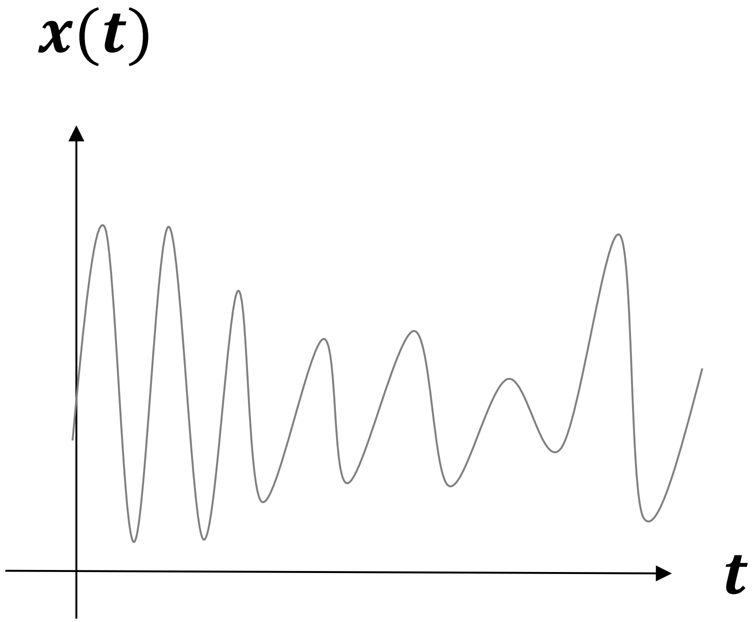


Polar to quadrature

$$I(t) = a(t)\cos(\Phi(t))$$
$$Q(t) = a(t)\sin(\Phi(t))$$
$$x_a(t) = I(t) + jQ(t) = a(t)e^{j\Phi(t)}$$

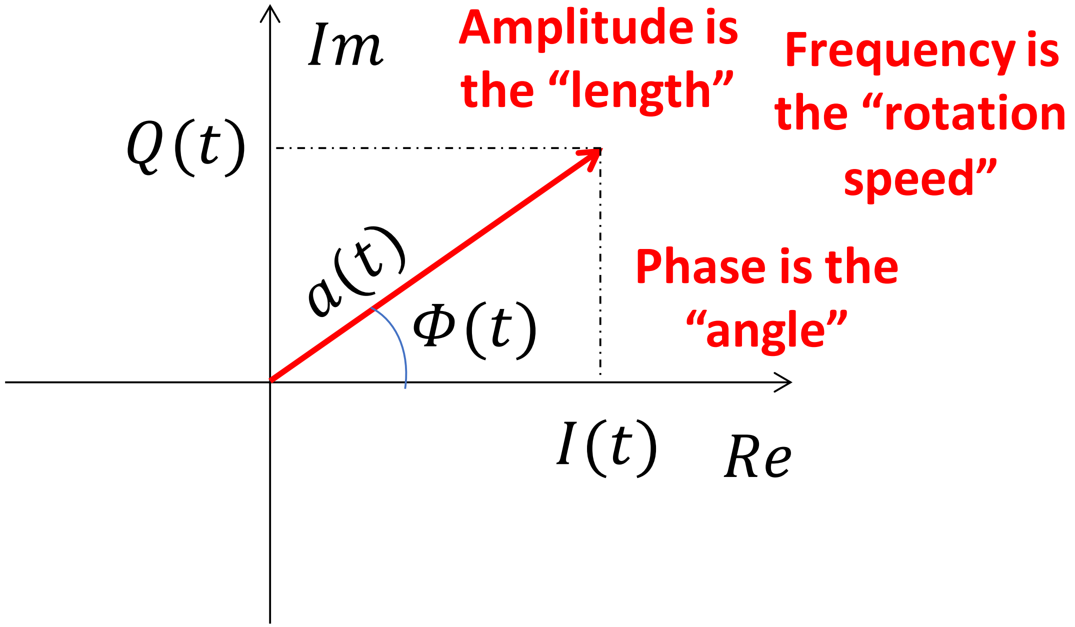
*sin(x) = cos(90-x)

Don’t be confused by math



$$\boldsymbol{x(t) = a(t)\cos(\Phi(t))}$$

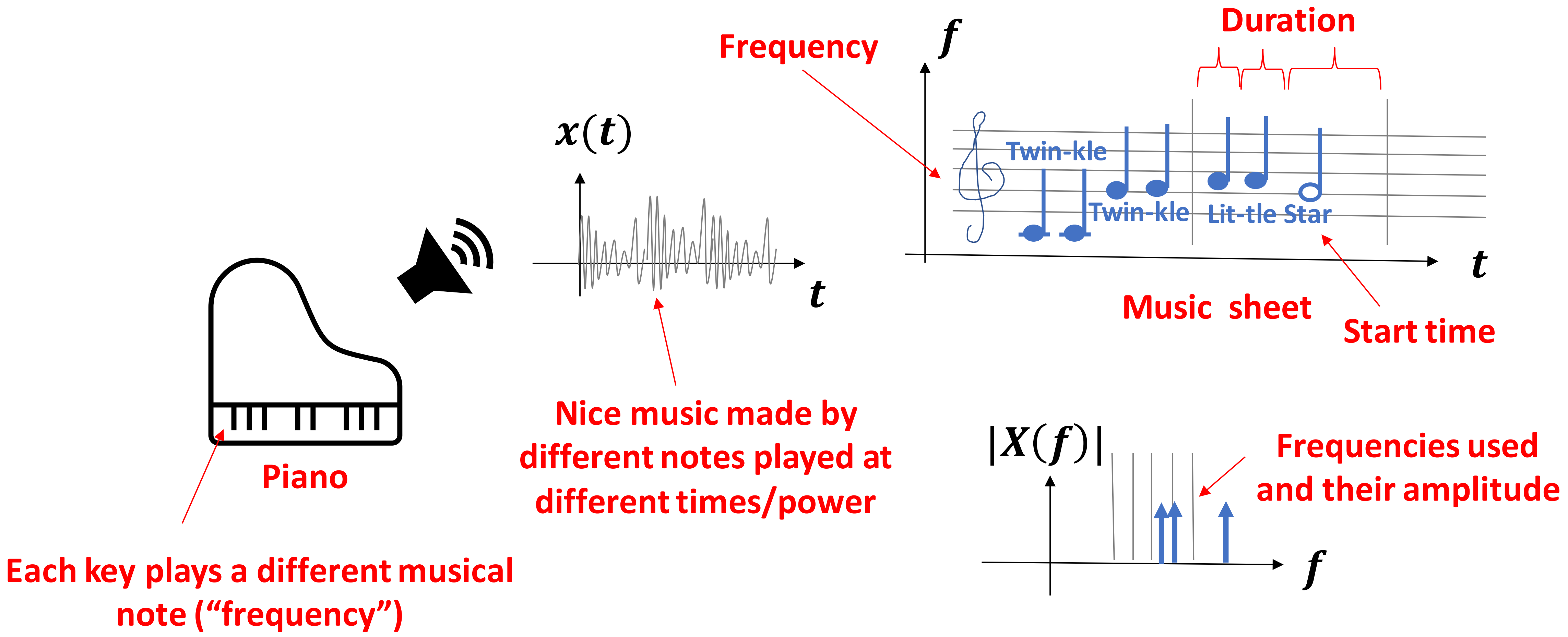
The physical signal
(The real part)



$$\boldsymbol{x_a(t) = a(t)e^{i\Phi(t)}}$$

The mathematical representation
(The complex analytical signal)

On time, frequency, and frequency over time

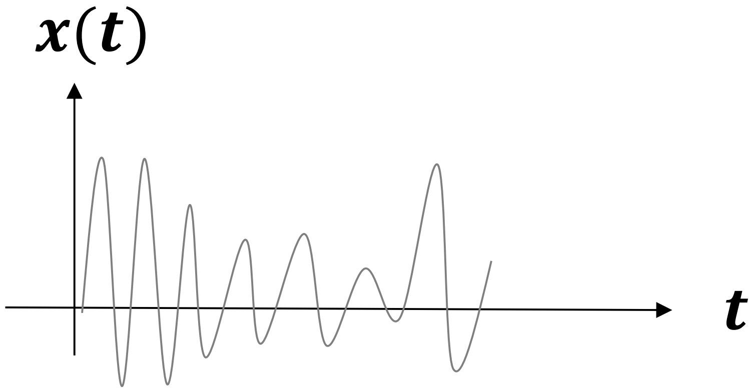


Frequency analysis

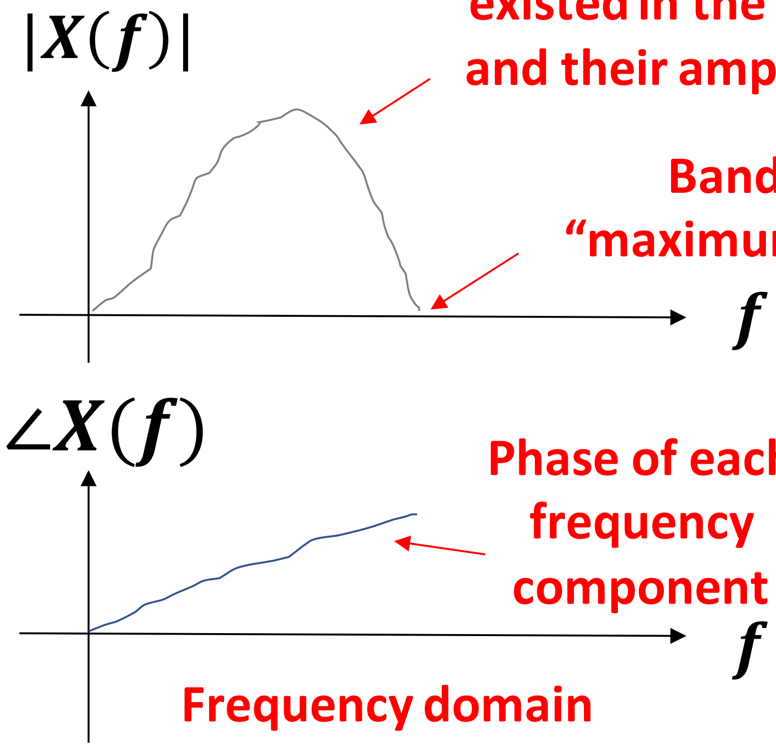
For real signals the transform is symmetric so we sometimes draw only the right side

Frequencies that existed in the signal and their amplitude

Bandwidth or “maximum frequency”



Time domain



Phase of each frequency component

Frequency domain

$$X(f) = F\big(x(t)\big) = \int_{-\infty}^{+\infty} x(t)e^{-i\overbrace{\boxed{\pi 2ft}}^{\Phi(t)}}$$

Decompose $x(t)$ into an infinite sum of complex sinewaves at different frequency

Fourier Transform

$$\cos x = \mathrm{Re}(e^{ix}) = \frac{e^{ix} + e^{-ix}}{2},$$

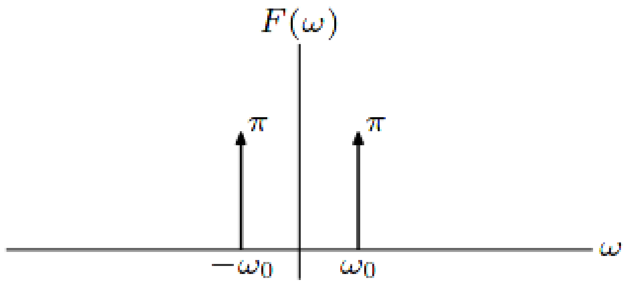
$$\sin x = \mathrm{Im}(e^{ix}) = \frac{e^{ix} - e^{-ix}}{2i}.$$

$\omega = 2\pi f$

Some examples

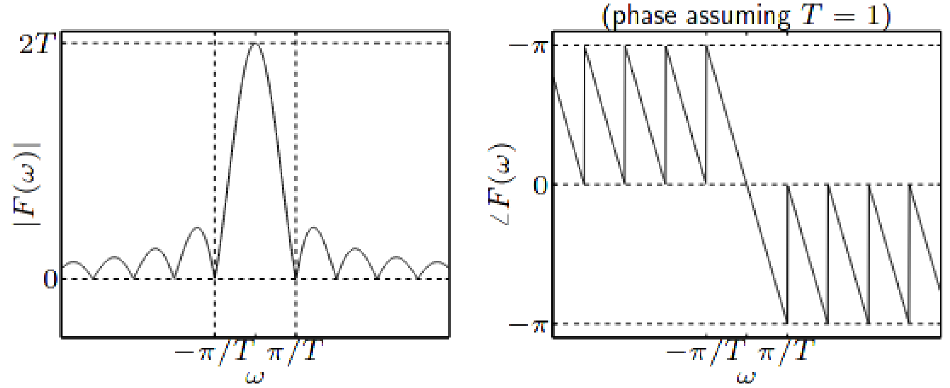
sinusoidal signals: Fourier transform of $f(t) = \cos\omega_0 t$

$$\begin{aligned} F(\omega) &= \frac{1}{2}\int_{-\infty}^{\infty}\left(e^{j\omega_0 t} + e^{-j\omega_0 t}\right) e^{-j\omega t}\, dt \\ &= \frac{1}{2}\int_{-\infty}^{\infty} e^{-j(\omega-\omega_0)t} dt + \frac{1}{2}\int_{-\infty}^{\infty} e^{-j(\omega+\omega_0)t} dt \\ &= \pi\delta(\omega-\omega_0) + \pi\delta(\omega+\omega_0) \end{aligned}$$



shifted rectangular pulse: $f(t) = \begin{cases} 1 & 1-T \le t \le 1+T \\ 0 & t < 1-T \text{ or } t > 1+T \end{cases}$

$$\begin{aligned} F(\omega) = \int_{1-T}^{1+T} e^{-j\omega t}\, dt &= \frac{-1}{j\omega}\left(e^{-j\omega(1+T)} - e^{-j\omega(1-T)}\right) \\ &= \frac{-e^{-j\omega}}{j\omega}\left(e^{-j\omega T} - e^{j\omega T}\right) \\ &= \frac{2\sin\omega T}{\omega} e^{-j\omega} \end{aligned}$$



https://web.stanford.edu/class/ee102/lectures/fourtran

https://ethz.ch/content/dam/ethz/special-interest/baug/ibk/structural-mechanics-dam/education/identmeth/fourier.pdf

Power Spectral Density (PSD)

Sometimes it is convenient to reason in terms of power

- **Signal:**
  - $x(t)$

$$x_T(t) = x(t)\ if\ -\frac{T}{2} < t < \frac{T}{2}\ else\ 0$$

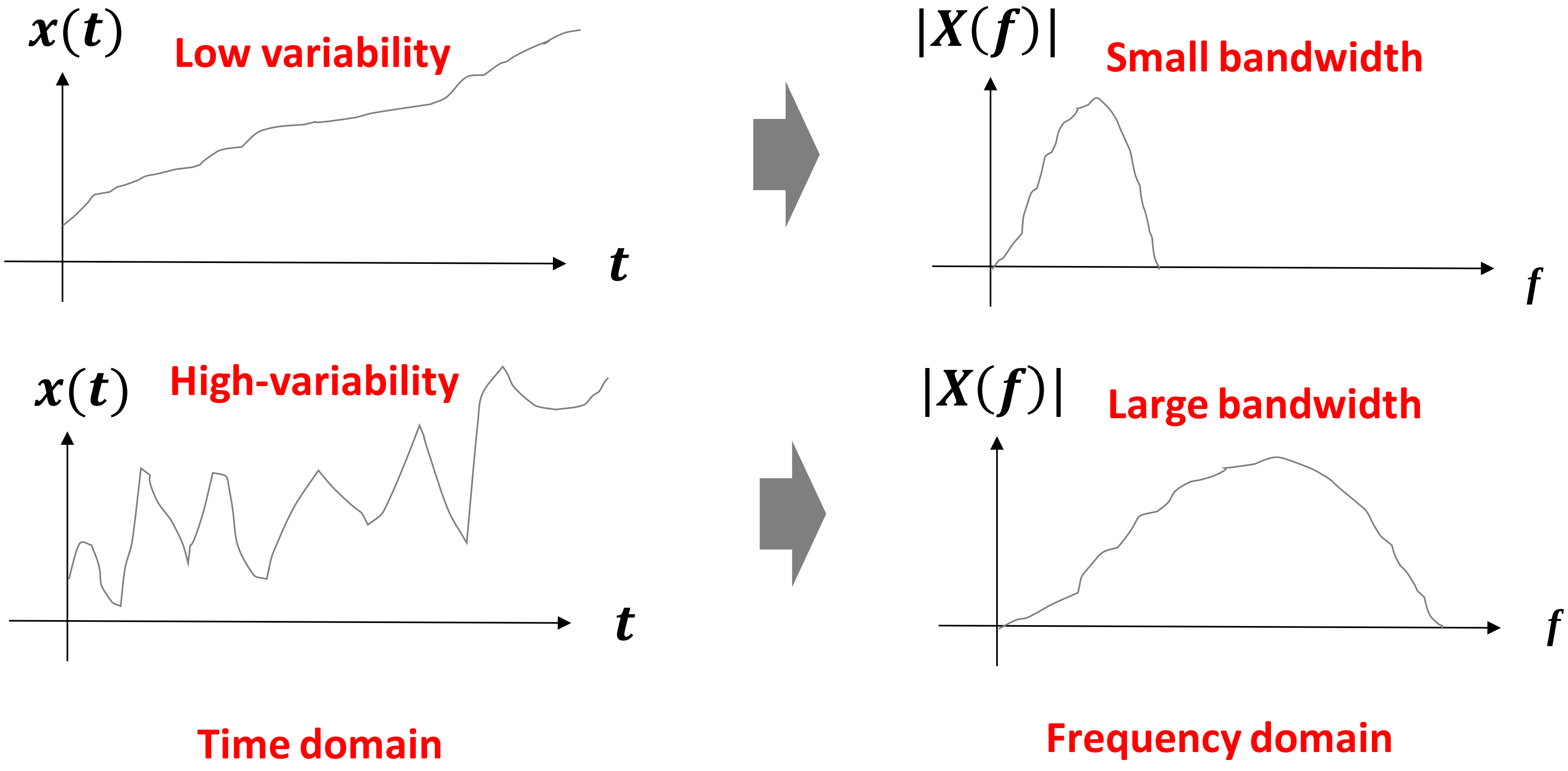
- **Power in the time domain**
  - **Power:** $\lim_{\boldsymbol{T}\to\infty} \frac{\mathbf{1}}{\boldsymbol{T}} \int |x_T(t)|^2 dt$

- **Power in the frequency domain**
  - **Power Spectral Density (PSD):** $PSD(f) = \lim_{\boldsymbol{T}\to\infty} \frac{\mathbf{1}}{\boldsymbol{T}} \int |X_T(f)|^2 dt$

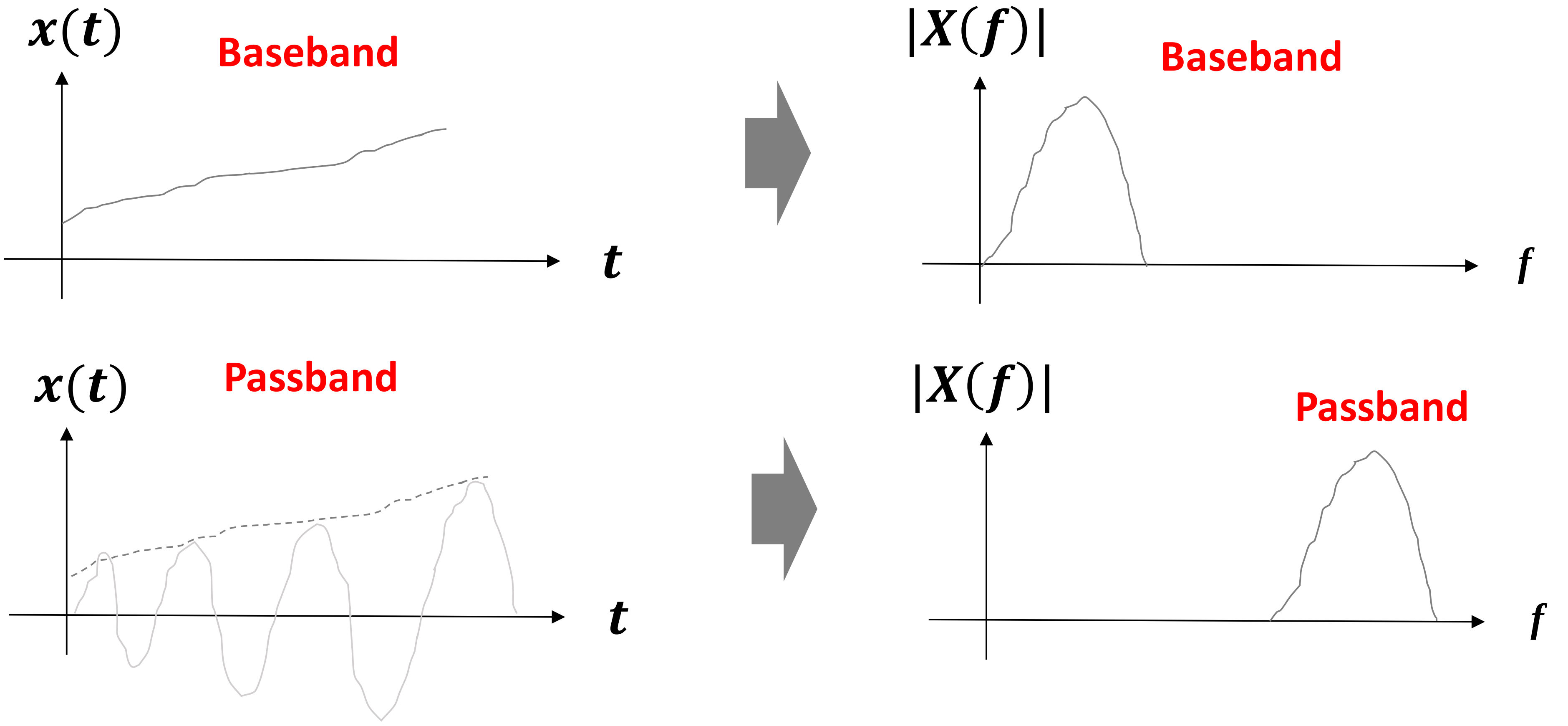
It tells us the distribution of power over the frequency components of $\boldsymbol{x(t)}$

https://www.egr.msu.edu/classes/ece458/radha/ss07Keyur/Lab-Handouts/PSDESDetc.pdf

High data-rate => Large bandwidth



Baseband to passband



Time domain

Frequency domain

Baseband and passband

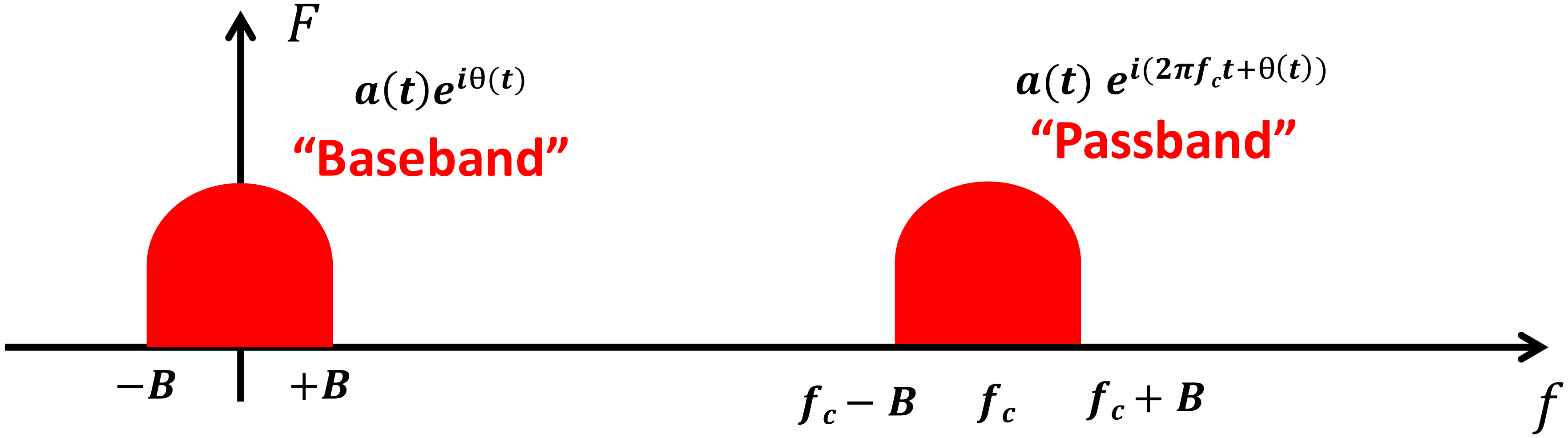
Amplitude Phase

$$x_{RF}(t) = RE\{\boxed{a(t)e^{i\theta(t)}}\boxed{e^{i2\pi f_c t}}\} = \boxed{a(t)}\cos(2\pi \boxed{f_c} t + \boxed{\theta(t)})$$

Complex envelope Carrier Carrier frequency

$$f(t) = f_c + \frac{1}{2\pi}\frac{d\theta(t)}{dt}$$

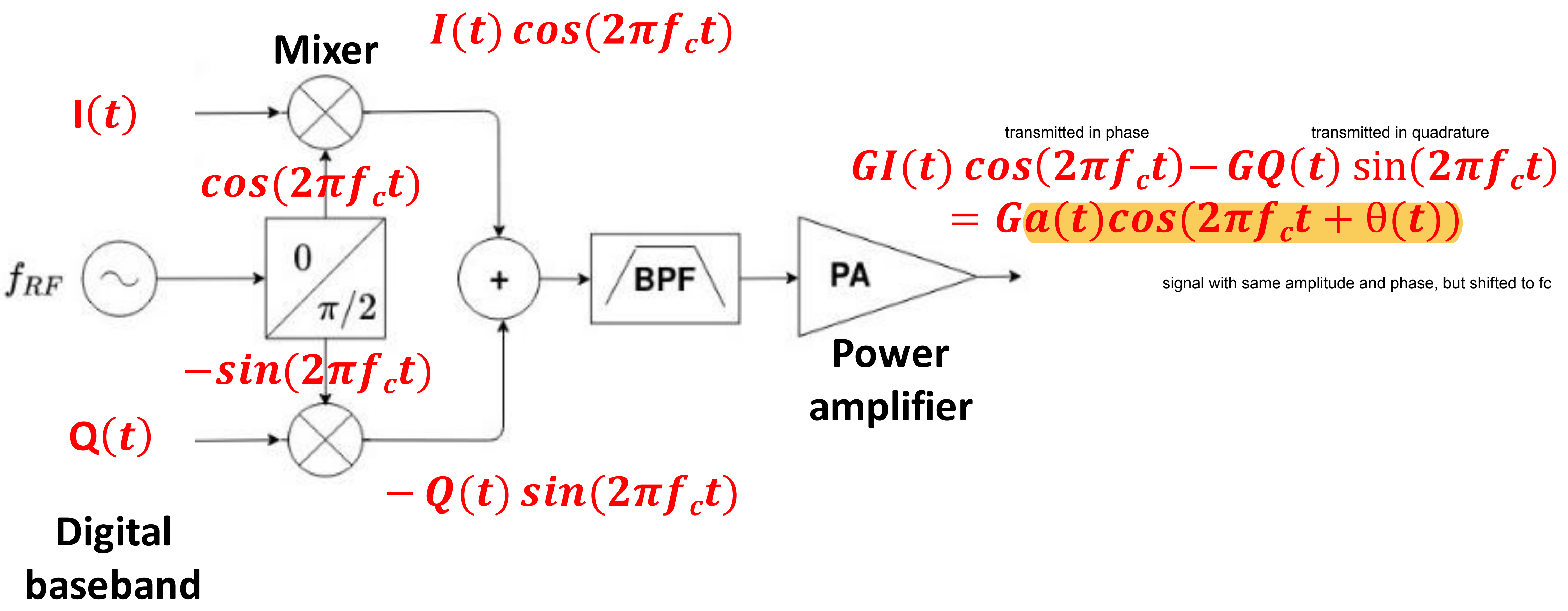
Frequency



Bandwidth

Upconversion

The Electronics

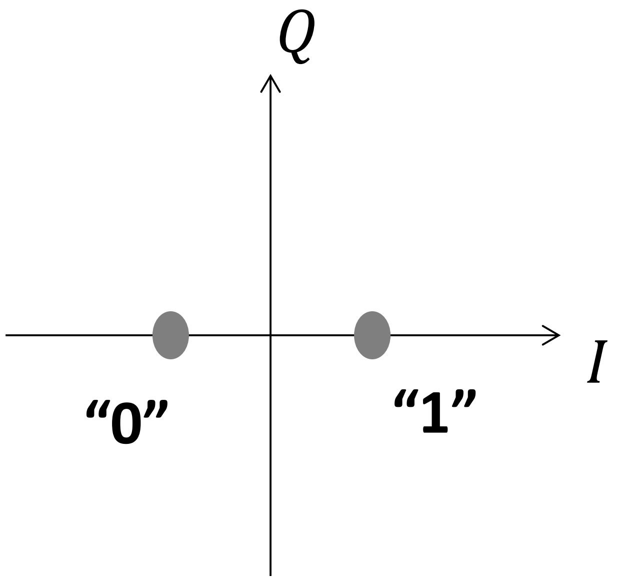


Quadrature Modulator

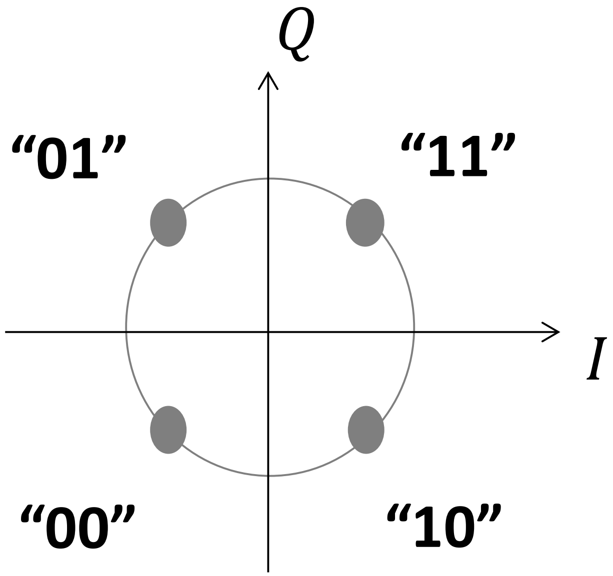
(This is just one possible architecture!)

It’s time for some examples

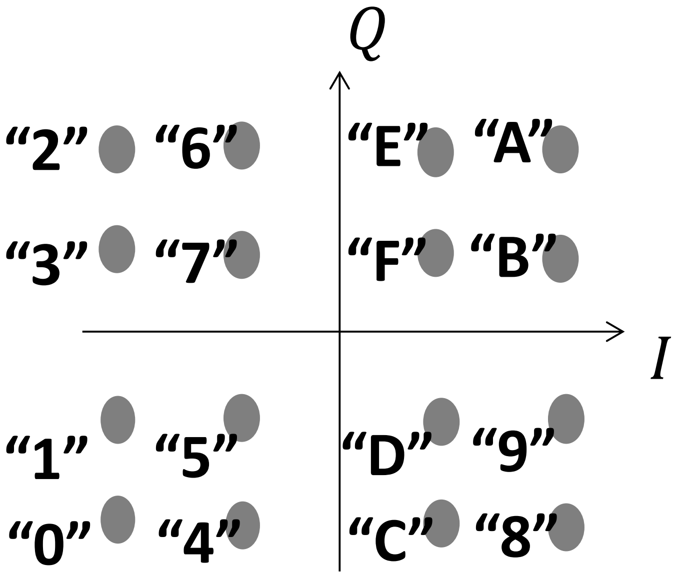
Phase-shift Keying (PSK) and Quadrature Amplitude Modulation (QAM)



Binary-PSK



Quadrature-PSK



QAM 16

BPSK with square pulses

```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
symbols_psk = bits
bpsk =  np.array((-1+0j, +1+0j))
Mbpsk = np.repeat(bpsk[symbols_psk], Ns)
```

Input bits one by one

Constellation

Baseband IQ samples

Find symbol in constellation

Repeat for the entire duration of the symbol

Q

I

```
bpsk = Mbpsk.real*np.cos(2*np.pi*f0*t_bpsk) - Mbpsk.imag*np.sin(2*np.pi*f0*t_bpsk)
```

Simulate quadrature modulator

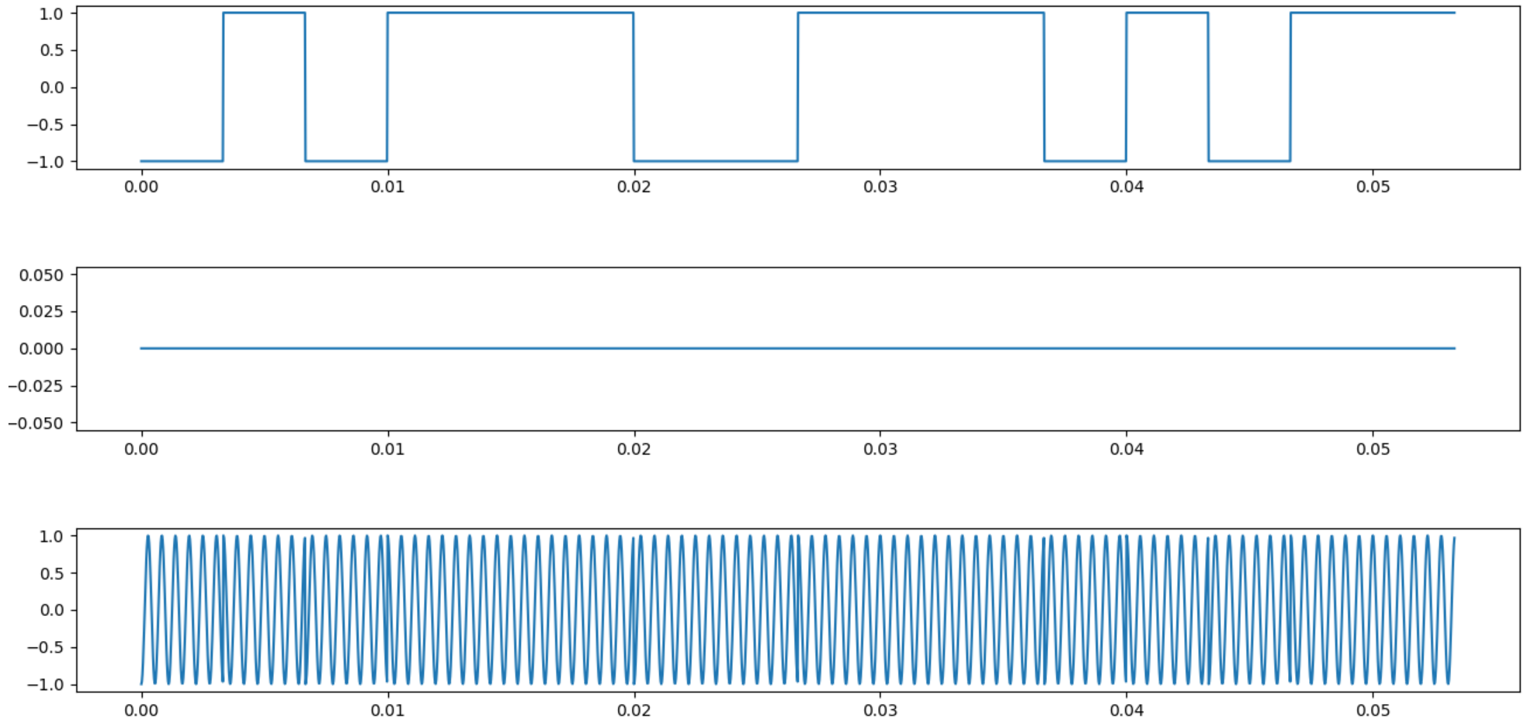
BPSK with square pulses

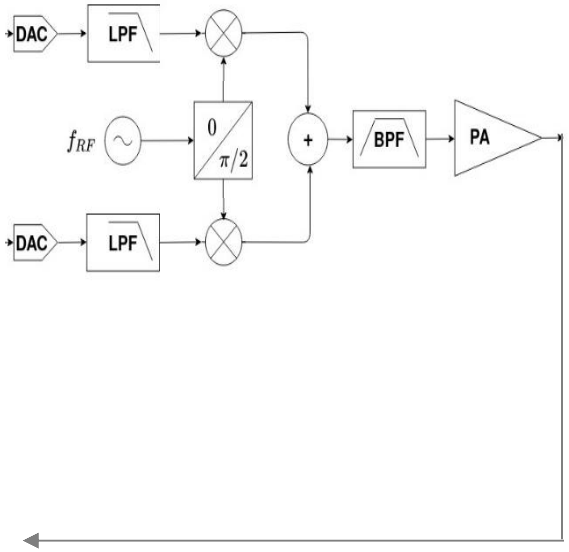
```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
```

I

Q

RF





$time\ (s)$

QPSK with square pulses

```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
```

Input bits two by two

```
symbols_qpsk = np.array([BitArray(i).uint for i in bits.reshape(-1,2)])
qpsk =  np.sqrt(2)*np.array((-1-1j, -1+1j, +1-1j, +1+1j))/2
```

Constellation

```
Mqpsk = np.repeat(qpsk[symbols_qpsk], Ns)
```

Baseband IQ samples

Find symbol in constellation

Repeat for the entire duration of the symbol

I **Q**

```
qpsk = Mqpsk.real*np.cos(2*np.pi*f0*t_qpsk) - Mqpsk.imag*np.sin(2*np.pi*f0*t_qpsk)
```

Simulate quadrature modulator

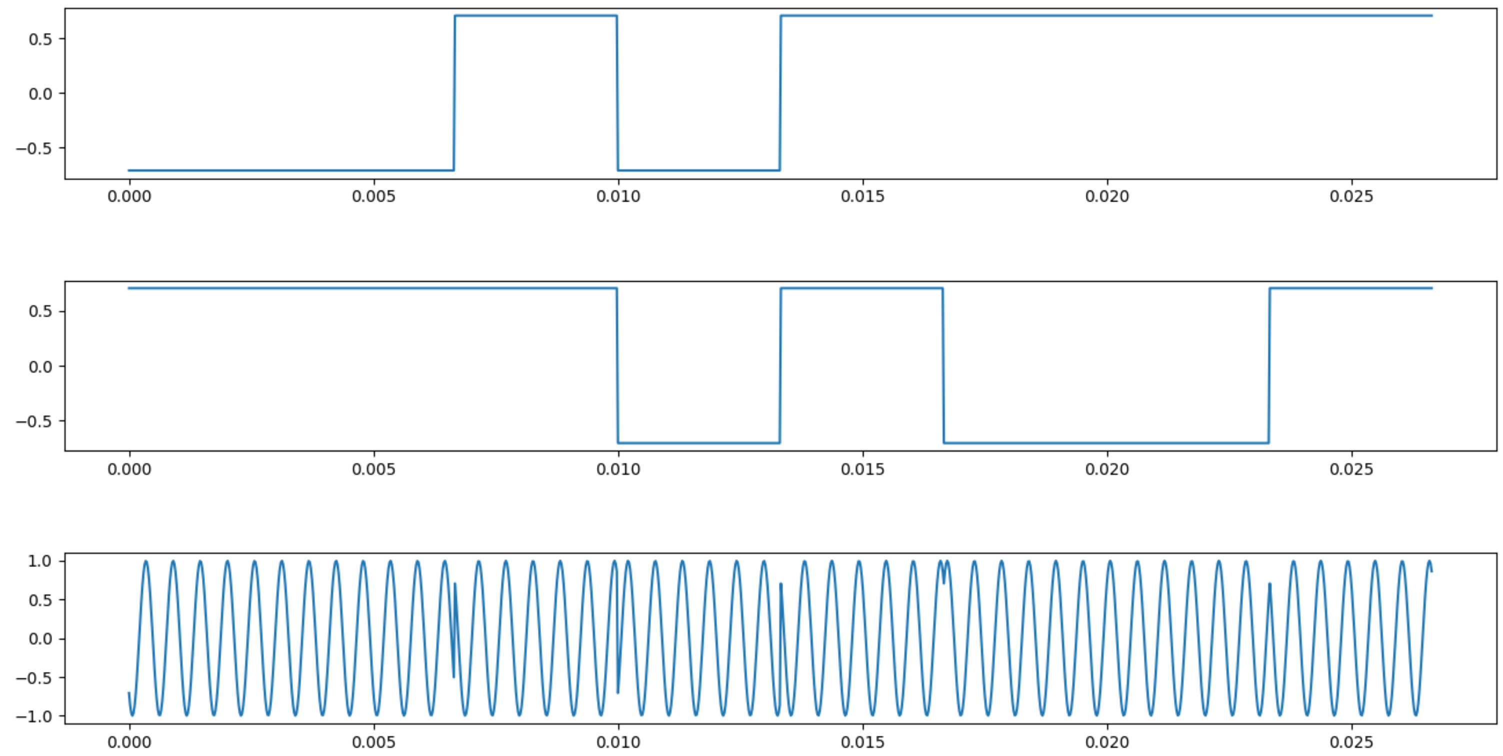
QPSK with square pulses

```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
```

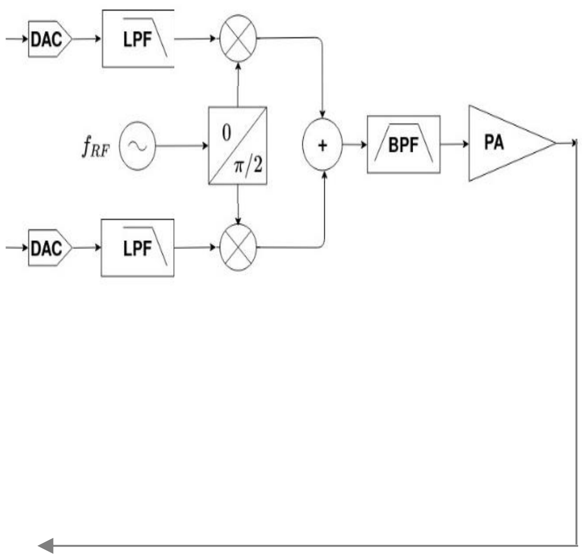
I

Q

RF



$time\ (s)$



QAM16 with square pulses

```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
symbols_qam16 = np.array([BitArray(i).uint for i in bits.reshape(-1,4)])
qam16 = np.sqrt(2)*np.array((-3-3j, -3-1j, -3+3j, -3+1j, -1-3j, -1-1j, -1+3j, -1+1j,
                              +3-3j, +3-1j, +3+3j, +3+1j, +1-3j, +1-1j, +1+3j, +1+1j))/4
Mqam16 = np.repeat(qam16[symbols_qam16], Ns)
```

Input bits four by four

Constellation

Baseband IQ samples

Find symbol in constellation

Repeat for the entire duration of the symbol

Q

I

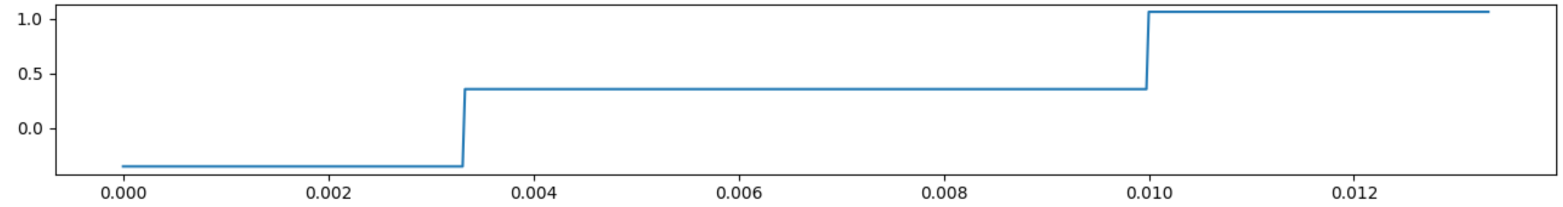
```
qam16 = Mqam16.real*np.cos(2*np.pi*f0*t_qam16) - Mqam16.imag*np.sin(2*np.pi*f0*t_qam16)
```

Simulate quadrature modulator

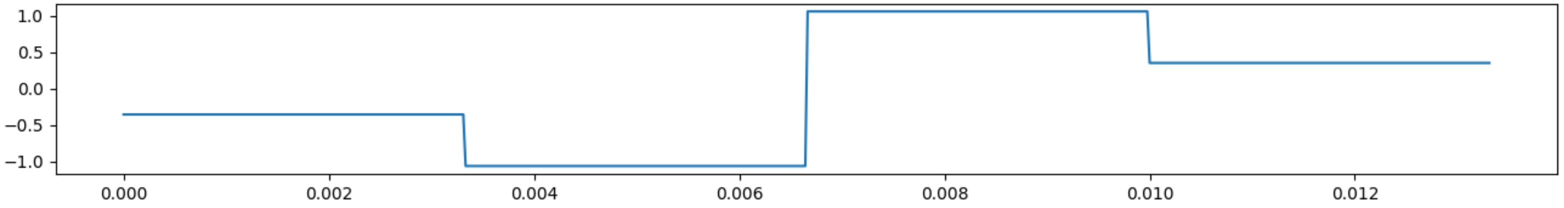
QAM16 with square pulses

```
bits = np.array([0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1])
```

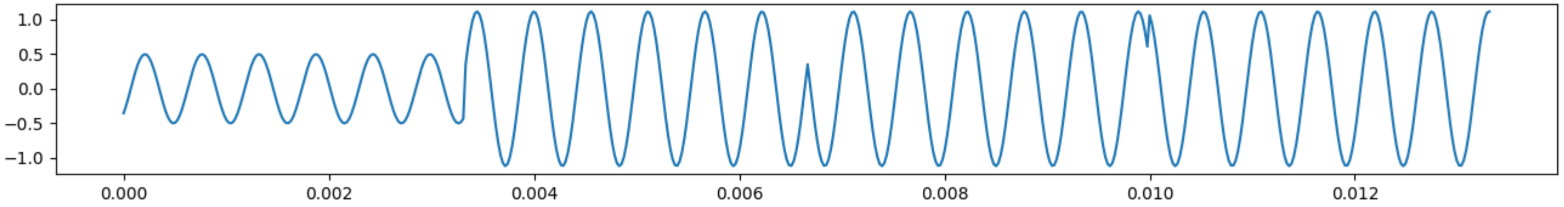
I

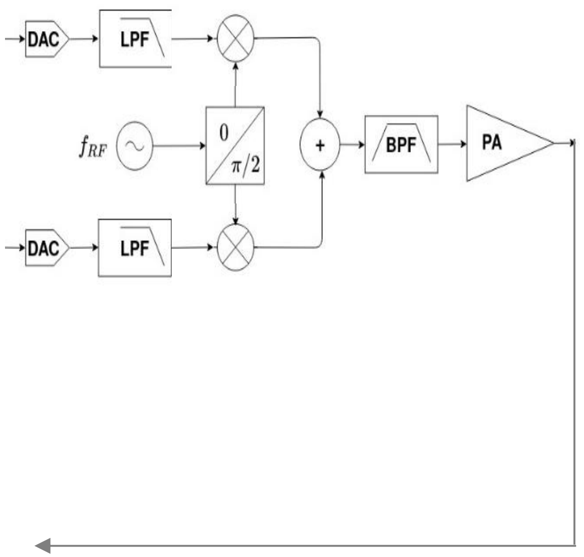


Q



RF



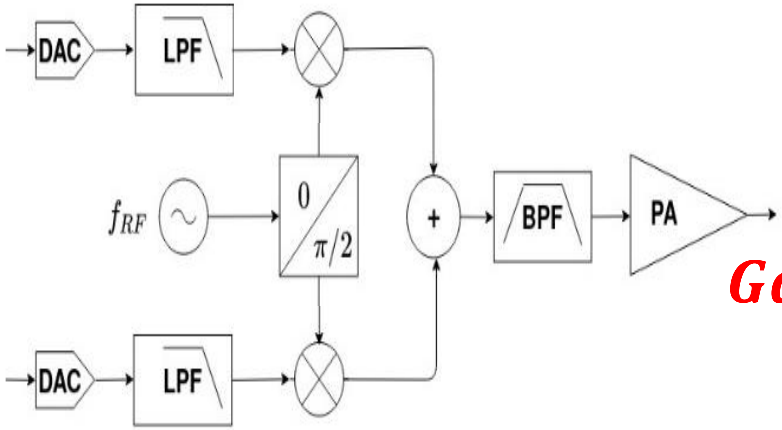


$time\ (s)$

More in general, a generic up-converter

$$I(nT_s) = a(nT_s)\cos\big(\Phi(nT_s)\big)$$

$$Q(nT_s) = a(nT_s)\sin\big(\Phi(nT_s)\big)$$



$$Ga(t)cos(2\pi f_c t + \theta(t))$$

- By properly choosing I and Q we can apply any analog/digital amplitude/frequency/phase modulation to the carrier
- In any case, I and Q can be generated in the digital domain (hardware or software) and then converted into physical signals with a (multi-bit) DAC
- The PSK/QAM examples seen before are a specific case of phase or phase+amplitude modulation

Some references

Check the full script plus look at the following links for more examples including other modulations

https://inst.eecs.berkeley.edu/~ee123/sp15/lab/lab6/Pre-Lab6-Intro-to-Digital-Communications.html

https://pysdr.org/content/digital_modulation.html

Security Implications

Fingerprinting based on Quadrature Errors

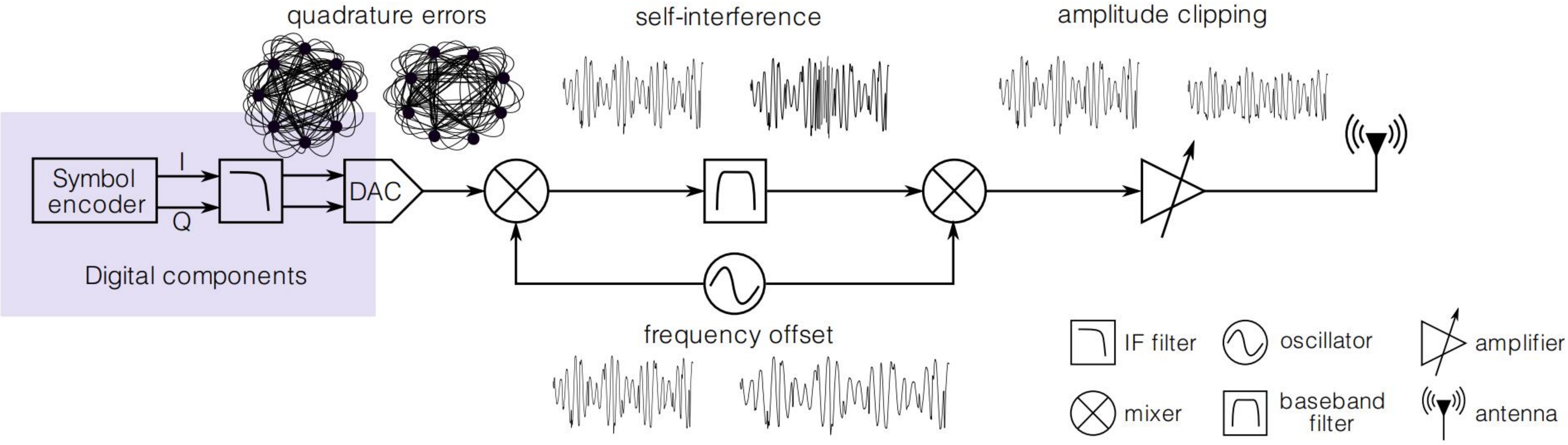


Figure 1: Common transmitter impairments and their sources

http://www.winlab.rutgers.edu/~gruteser/papers/brik_paradis.pdf

Fingerprinting based on Quadrature Errors

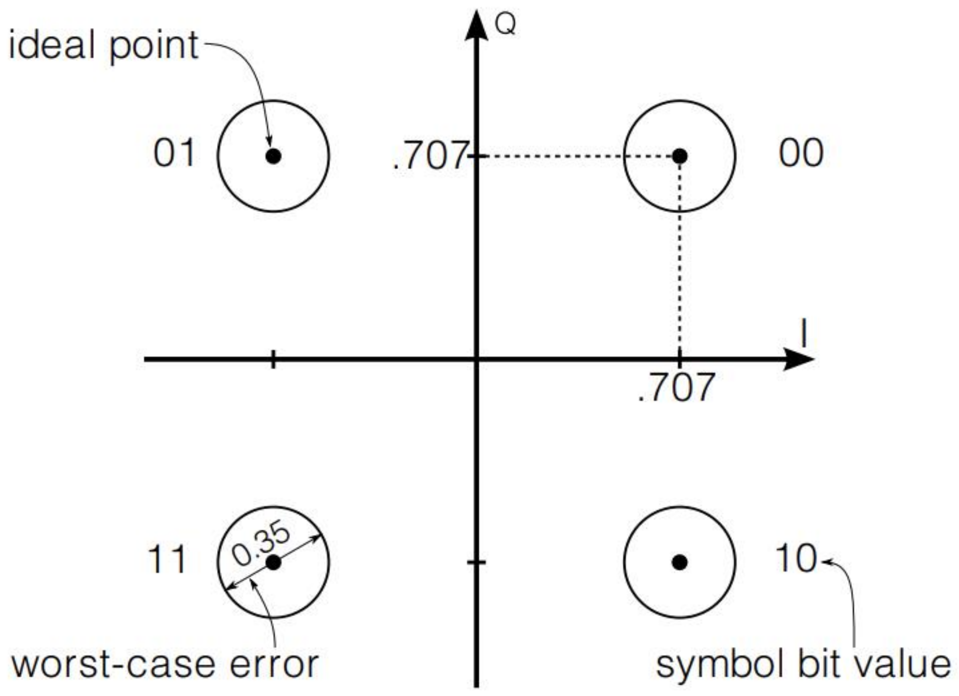


Figure 4: The 4 symbols of QPSK on I/Q plane

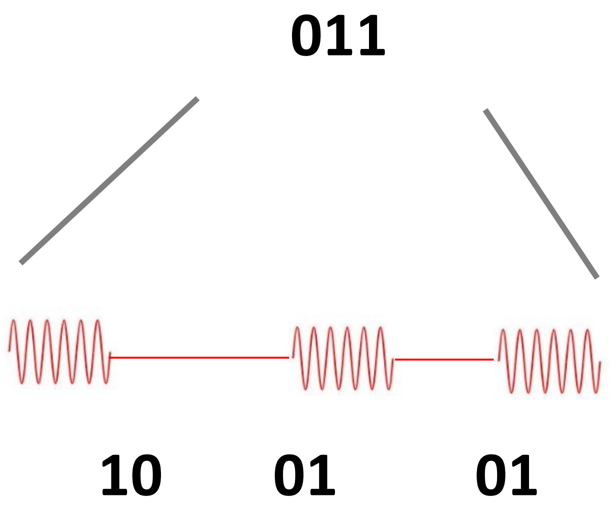
Some more considerations

Sending data in practice

Bits

Encoding & Modulation

Symbols



E.g., On-Off Keying (OOK) and Manchester Encoding

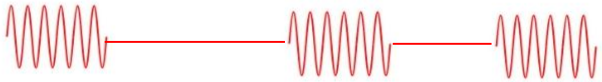
Sending data in practice

Upper layers (link, network, app, …)

Example of simple packet (a real remote, simplified)

Preamble (Sync)	Command (Payload)	CRC (Errors)	Rolling code (Freshness)	Address

Up = 011

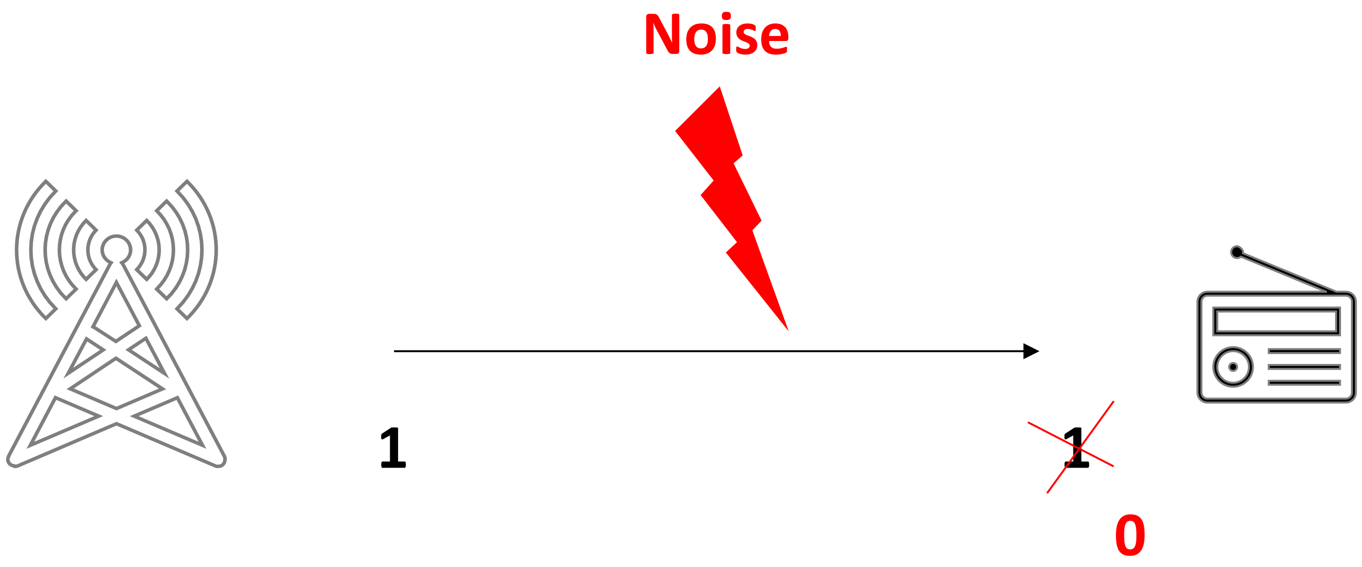


10 01 01

On-Off Keying (OOK)
+ Manchester encoding

Physical layer

Dealing with a noise (+ *channel – not shown)*

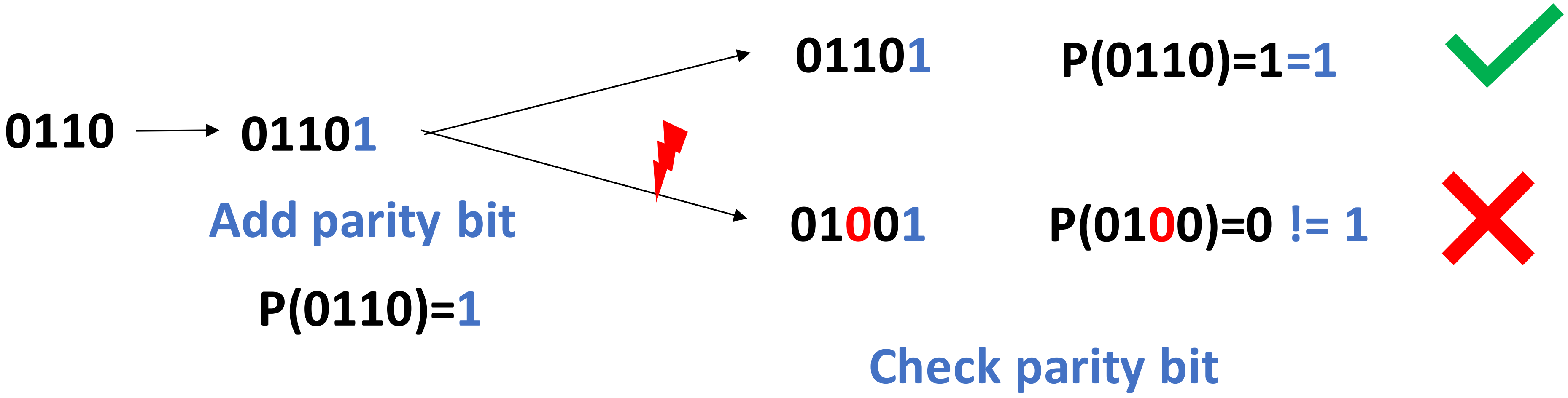


We need to deal with noise

Bit errors happen

How to correct errors?

Error detection and correction (intuition only)



Error Detection

(Add redundant bits for checking errors)

Error detection and correction (intuition only)

0110 → 010 / 100 / 00 → 010 / 110 / 00 ← P(11)=1 != 0 → 0110

010
100
00

Detection bits placed on multiple dimensions to detect error position

010
110
00

P(11)=1 != 0

P(11)=1 != 0

Wrong bit identified

0110

Correction

Error Detection & Correction

(Add redundant bits to detect errors and their position)

Interleaving (intuition only)

Adviser expects TEMPEST becomes quickly serious problem

Interleaving **“Shuffle in time”**

AxMokum eEccoer Teiiles burbstT qeoicSs srveEey pdpPmls

References

"A Foundation in Digital Communication," accessed May 11, 2021, https://www.afidc.ethz.ch/A_Foundation_in_Digital_Communication/Home.html.

Arya Behzad, Wireless LAN Radios: System Definition to Transistor Design (IEEE Press Series on Microelectronic Systems) (Hoboken, NJ, USA: John Wiley & Sons, Inc., 2008).

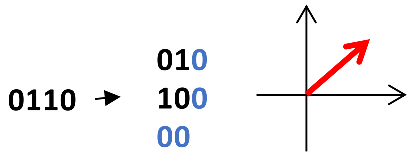
Quick recap of this part

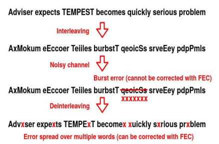
- Transmitting information with radio waves:
  - EM waves at radio frequency propagate from transmitter to receiver
    - Currents in antennas generate EM signals (TX)
    - EM signals propagate (Propagation)
    - EM signals generate currents in antennas (RX)
  - The waves are modulated to transmit information
    - Analytical signals are a convenient representation
    - AM/FM/PM modulation
    - Baseband vs. passband (Up/Down-conversion)
  - Transmission in practice
    - Electronic circuits in a typical transmitter (receiver is symmetrical)
    - Encoding, modulation, packets, upper protocol layers
    - Dealing with noise and bit errors:
      - Detection, detection and correction, interleaving

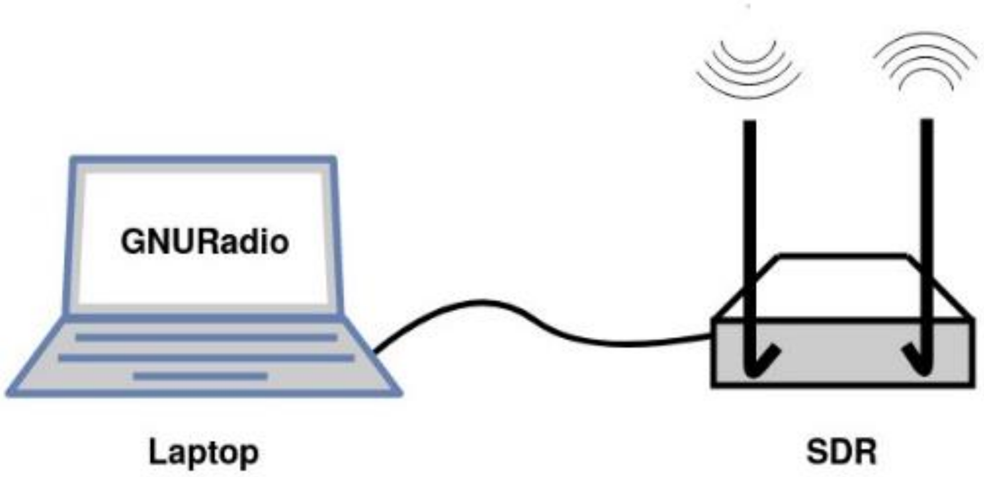
Software Defined Radios (SDR)

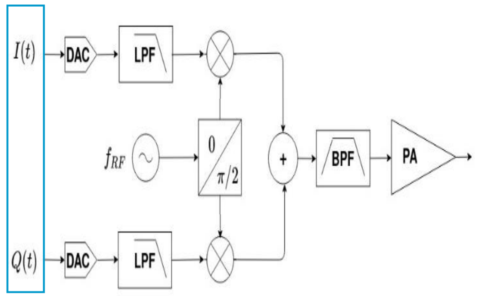
(A quick introduction)

Software Defined Radio (SDR)









"Radio in which some or all of the **physical layer functions** are software-defined"

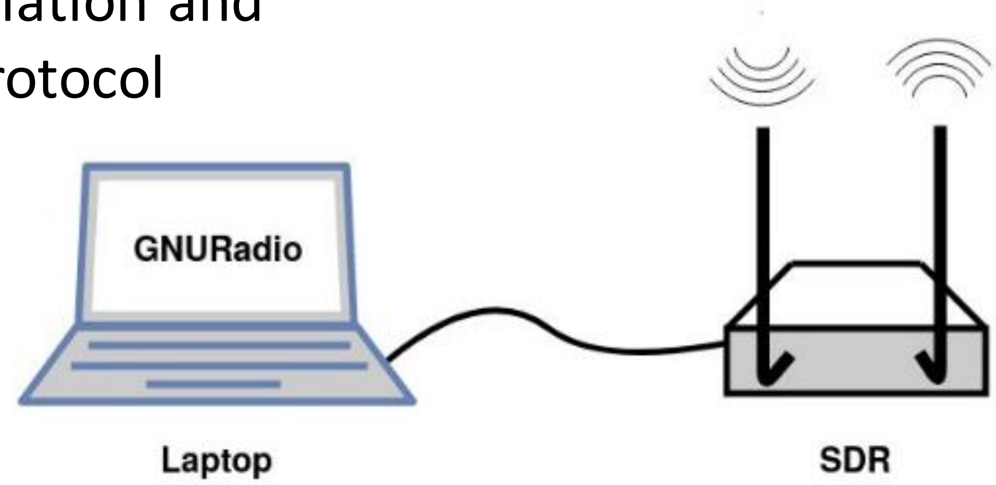
Software Defined Radio Forum, "SDRF Cognitive Radio Definitions Working Document SDRF-06-R-0011-V1.0.0", 2007, http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-R-0011-V1_0_0.pdf.

Software Defined Radio (SDR)

Virtually any modulation and protocol

A lot of cheap user-friendly devices

Software from digital baseband to upper layers



Minimal configurable hardware

A lot of open-source tools already implemented

SDR hardware examples

Warning:
There is more! This is just an example, no advertisement!

RTL-SDR
https://www.rtl-sdr.com/
Entry level, simple, only RX, cheap 20 euros

HackRF
https://greatscottgadgets.com/hackrf/
RX/TX, higher bandwidth and range, more expensive

USRP B210
https://www.ettus.com/all-products/ub210-kit/
RX/TX, dual channel, high quality, expensive

SDR software examples

Warning: There are so many more! And you can write your own

https://gqrx.dk/
https://cubicsdr.com/

Simple AM/FM/…

Generic framework

https://www.gnuradio.org/
https://github.com/bastibl/gr-ieee802-11
https://github.com/tapparelj/gr-lora_sdr
gr-* many more projects

A lot of projects

https://github.com/osqzss/gps-sdr-sim
https://gnss-sdr.org/

GPS spoofing and GNSS Rx

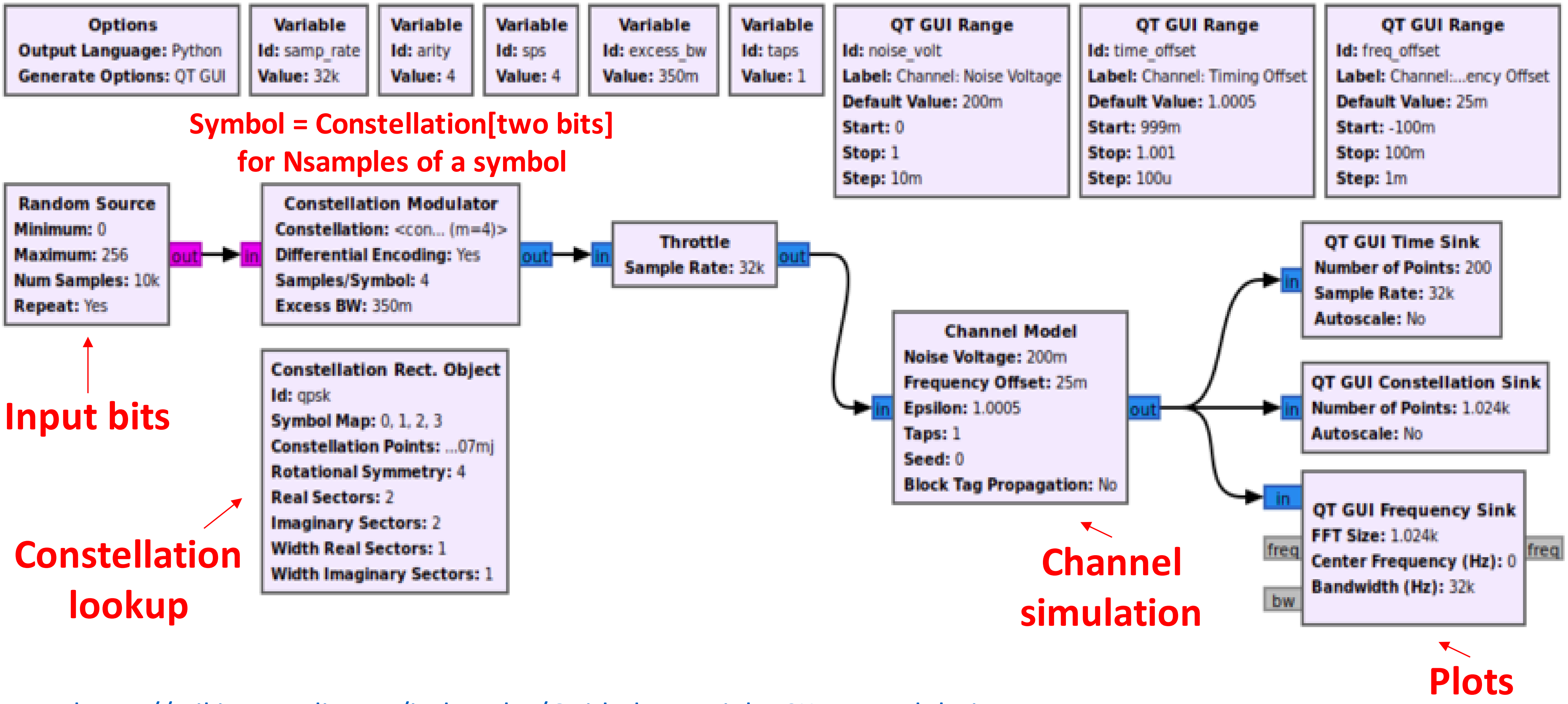
https://fr.wikipedia.org/wiki/FlDigi
https://physics.princeton.edu/pulsar/K1JT/wsjtx.html

Ham radio (Amateur)

https://github.com/jopohl/urh
https://batchdrake.github.io/SigDigger/

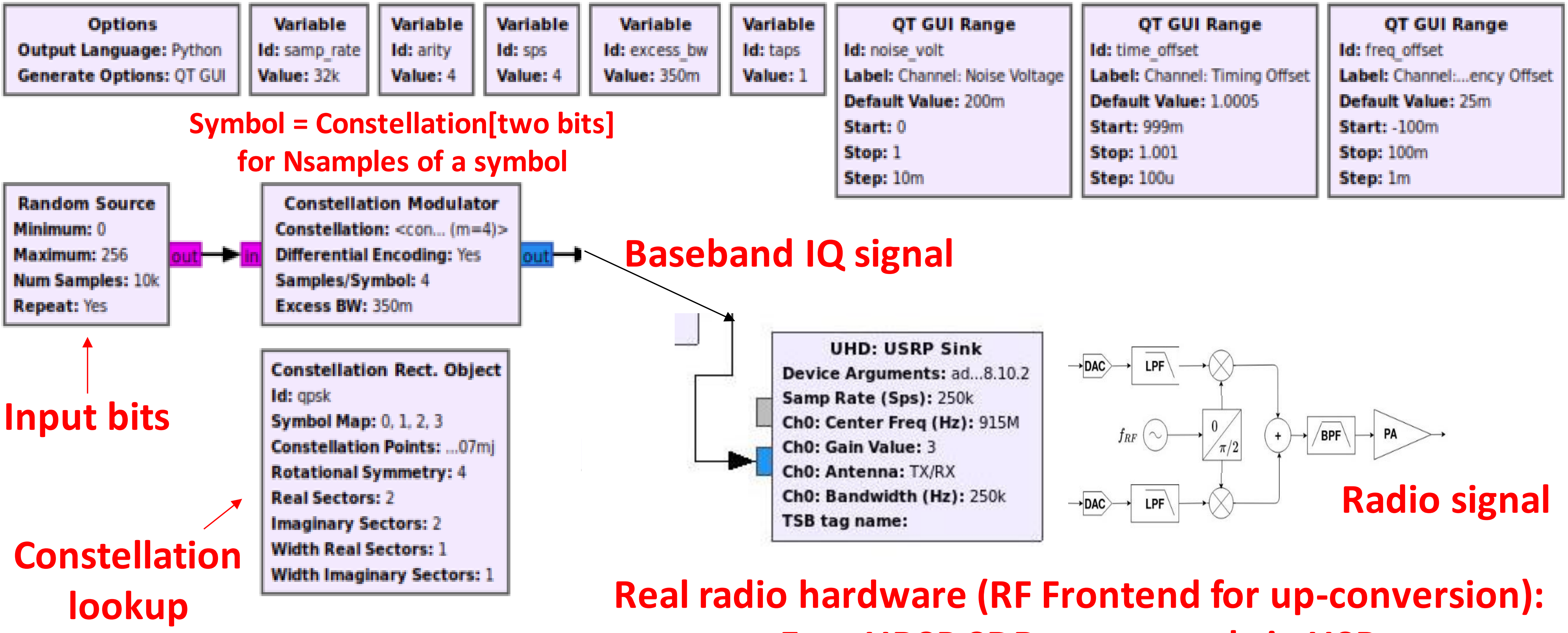
Reverse engineering radio protocols

An example: QPSK simulation



https://wiki.gnuradio.org/index.php/Guided_Tutorial_PSK_Demodulation

An example: QPSK transmission

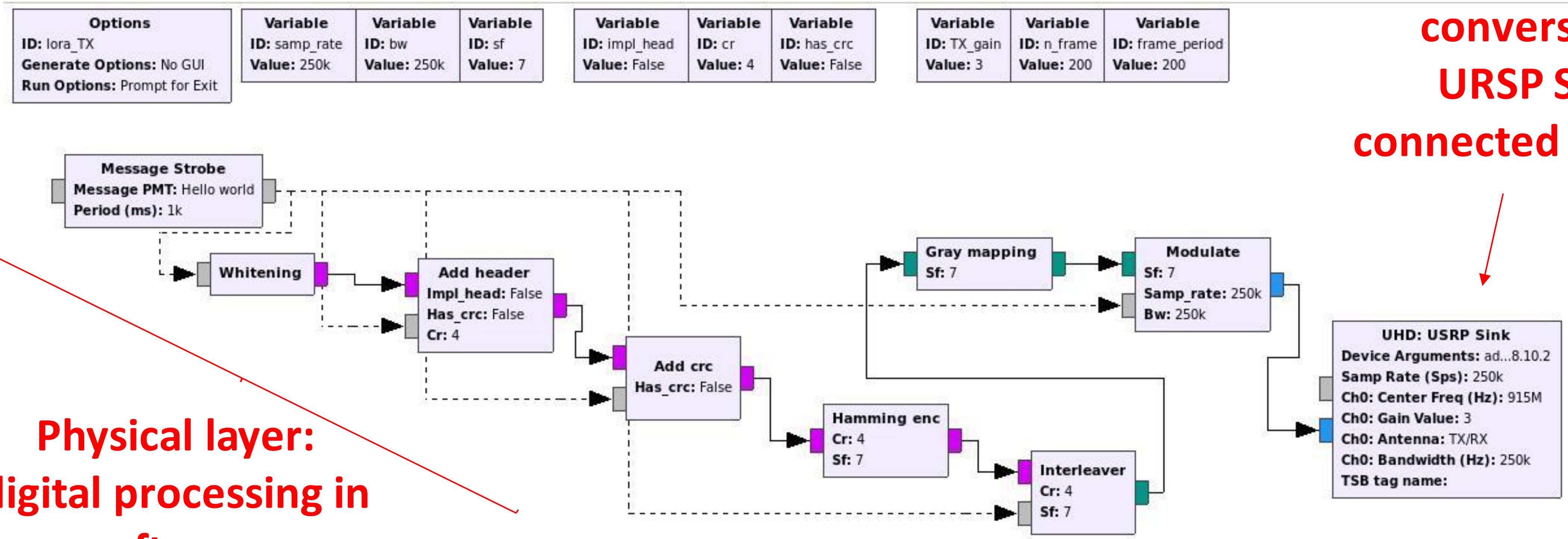


Real radio hardware (RF Frontend for up-conversion):
E-g., URSP SDR connected via USB

https://wiki.gnuradio.org/index.php/Guided_Tutorial_PSK_Demodulation

An example: LoRa

RF Frontend of up-conversion: URSP SDR connected via USB



Physical layer: digital processing in software

J. Tapparel, O. Afisiadis, P. Mayoraz, A. Balatsoukas-Stimming, and A. Burg, “An Open-Source LoRa Physical Layer Prototype on GNU Radio”

References

Software Defined Radio Forum, “SDRF Cognitive Radio Definitions Working Document SDRF-06-R-0011-V1.0.0”, 2007, http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-R-0011-V1_0_0.pdf.

https://www.gnuradio.org/

https://wiki.gnuradio.org/index.php/Tutorials

“Homework”:

1. Familiarize with GNURadio

2. Start studying the tutorials

It will be useful for the lab!

Important to Know

- Analytical Signal Representation vs Real Signal
- Frequency Representation: Baseband vs Passband
- Operation of the Quadrature Modulator
- What is an IQ diagram and How are Modulations Mapped onto it
- Basic Packet Structure and Error Correction

Next Week:

- Basics of the Wireless Communication Channel
- Physical Layer Based Security

Questions?