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

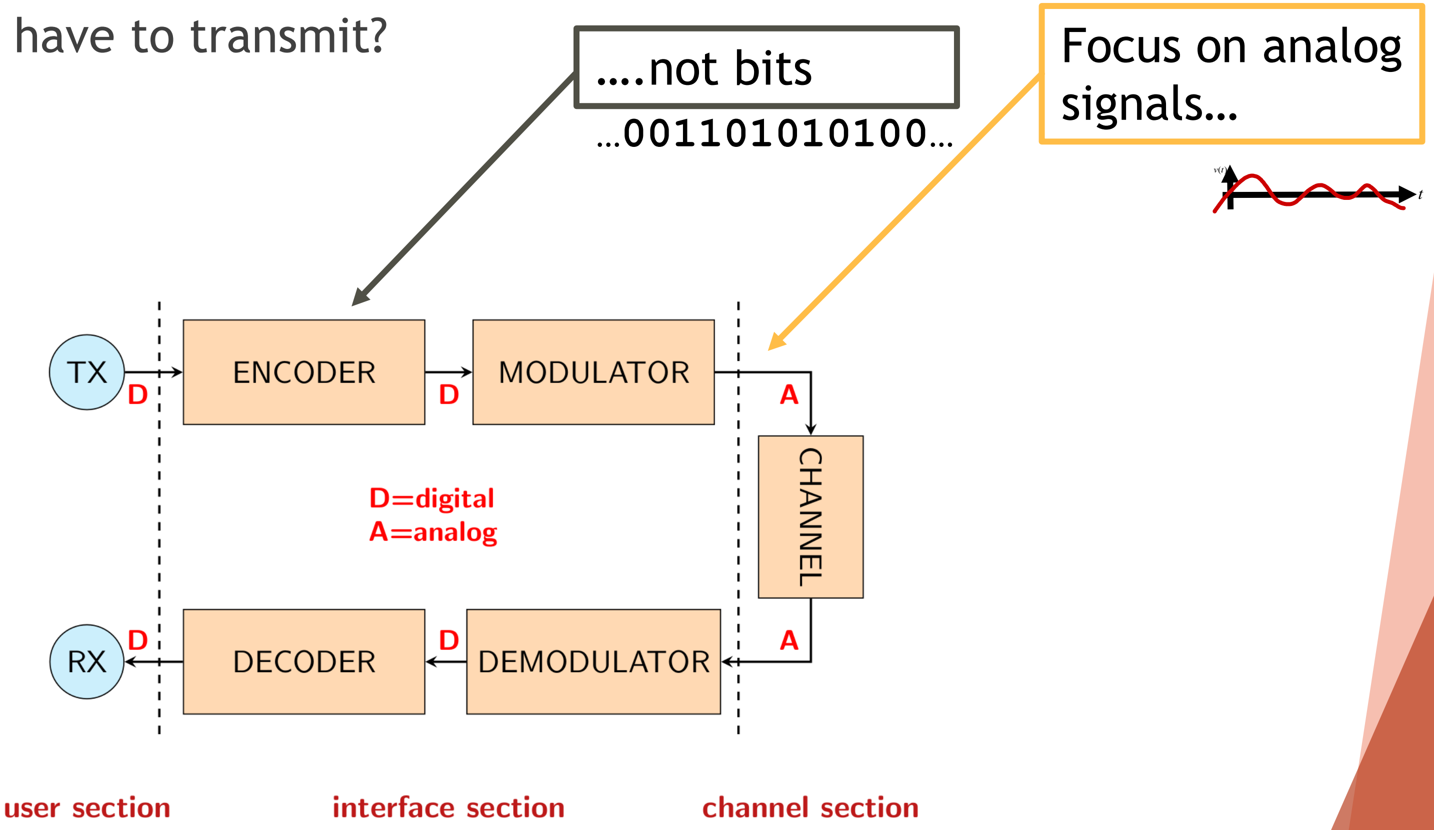
Basic Concepts for Digital Communications

Andrea Nardin

Contents

Which Waveforms Should We Transmit?

- We have now acquired the main tools to deal with signals
- Our goal is to use them to **communicate** some information (i.e. bits)
- I.e. to transmit something that will be **received correctly**
  - We talk binary, but we must transmit over analog media
- Which signal waveforms do we have to transmit?
  - (and possibly receive)



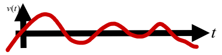
Recall: Modulator / Demodulator

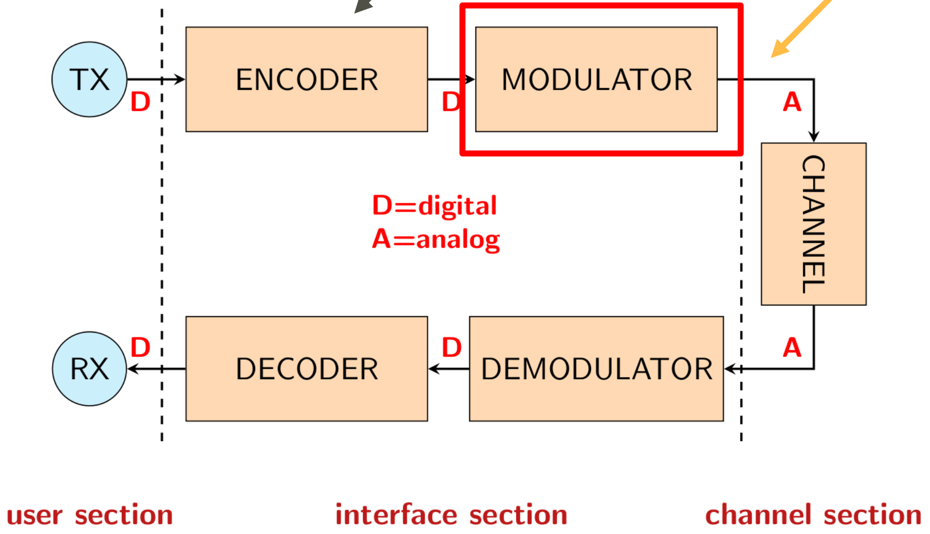
- *Modulator*:
  - Converts the digital signal into an analog signal to be transmitted over the channel
- *Demodulator*
  - Converts the received **analog signal** into a **sequence of samples** to be processed by the decoder

....not bits

...001101010100...

Focus on analog signals...





Modulation Basics

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

- Why?
  - Multiple signals over the same channel
  - Wireless transmission (pathloss and atmospheric attenuation)
  - Etc.

- Generally, digital and analog modulations resort to basic modulation types:
  - *Amplitude Modulation*: changes the amplitude
  - *Frequency Modulation*: changes the frequency
  - *Phase Modulation*: changes the phase

Amplitude Modulation (AM)

- *Amplitude modulation* (AM):
- The amplitude of high-carrier signal is varied according to the instantaneous amplitude of the modulating message signal $m(t)$.

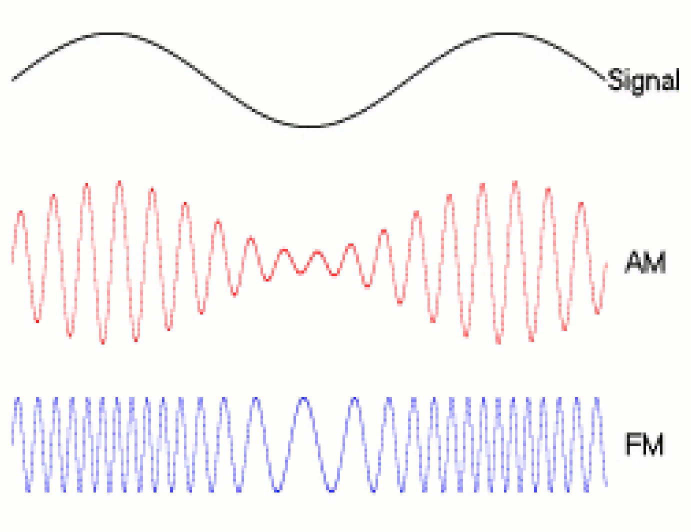


Figure: By Berserkerus - Own work, CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=5071748

Frequency Modulation (FM)

- *Frequency modulation* (FM):
- The carrier amplitude remains constant, and the carrier frequency is changed by the modulating signal $m(t)$.
- As the amplitude of the information signal varies, the carrier frequency shifts proportionately.
  - As the modulating signal amplitude increases, the carrier frequency increases.
  - With no modulation the carrier is at its normal center or resting frequency.

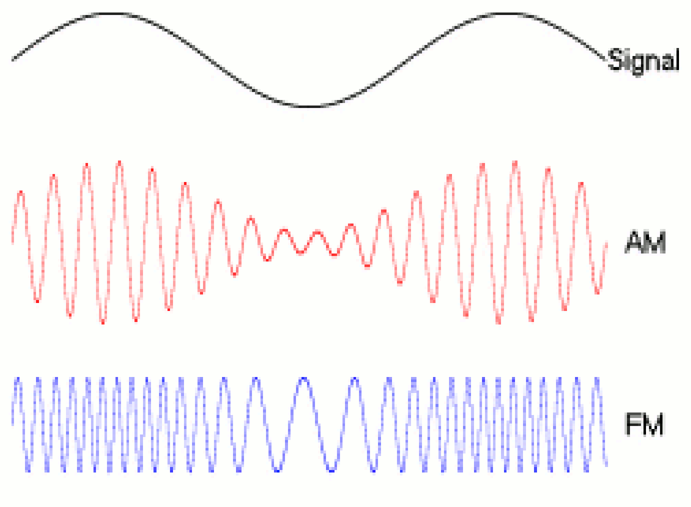


Figure: By Berserkerus - Own work, CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=5071748

Phase Modulation (PM)

- *Phase modulation* (PM):
- It encodes a message signal $m(t)$ as variations in the instantaneous phase of a carrier wave
- The **phase of a carrier** signal is modulated to follow the changing **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
- The modulating wave (blue) is modulating the carrier wave (red), resulting the PM signal (green)

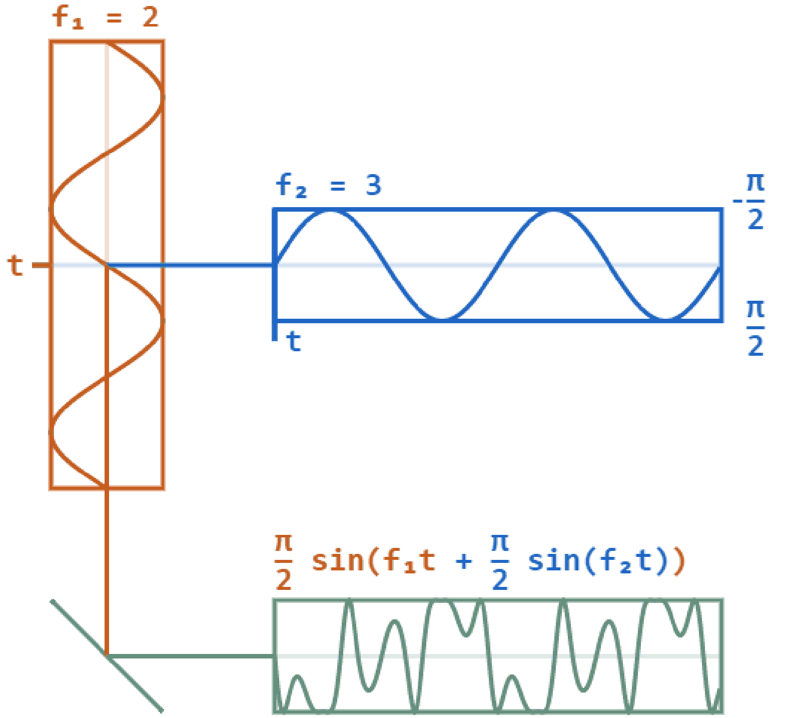
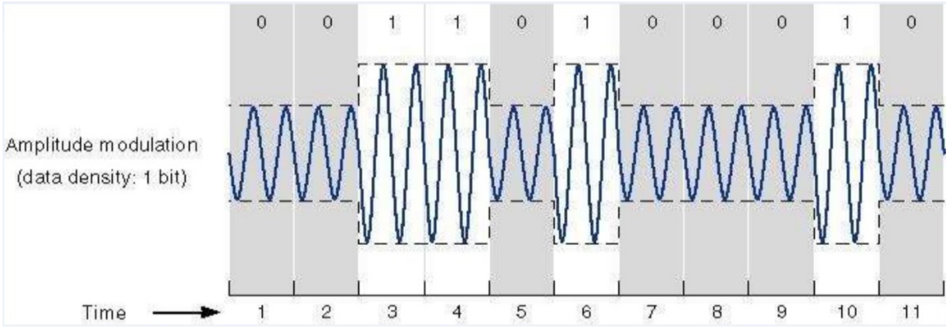
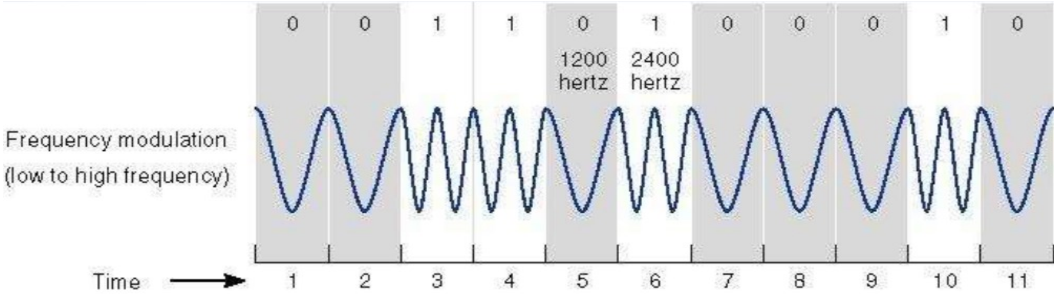


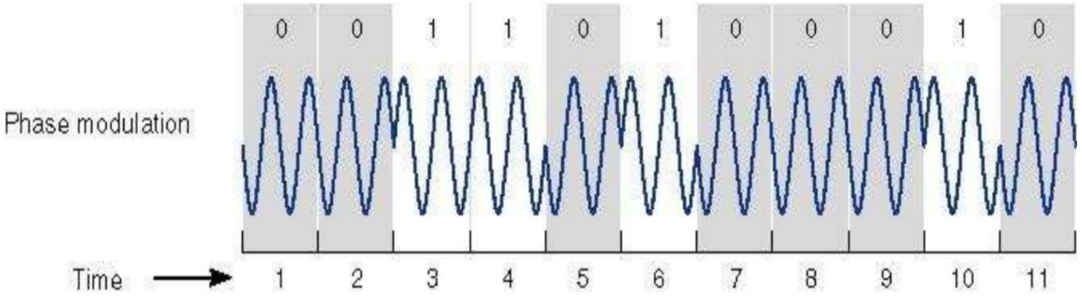
Figure: By Potasmic - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=50046376

Analog and digital modulations

- Even if the world has turned to **digital**, transmitted signals are **analog**
- Similar ideas have been applied to digital signals
  - *Amplitude Shift Keying* (ASK)
  - *Frequency Shift Keying* (FSK)
  - *Phase Shift Keying* (PSK)







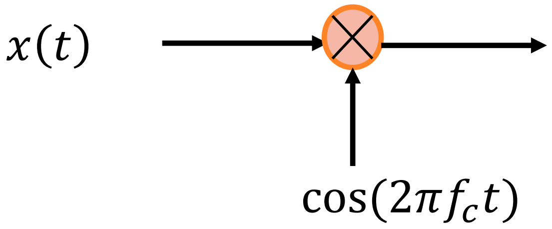
Analog and digital modulations

- Digital signals must be transmitted as **analog waveforms**

- *Baseband signals*
  - Signals whose frequency spectrum is concentrated around zero

- *Bandpass signals*
  - Signals whose frequency spectrum is centered at some frequency f_c away from zero

- **Baseband** signals can be converted to **bandpass** signals through *modulation:*
  - Multiplication by a sinusoid with frequency f_c

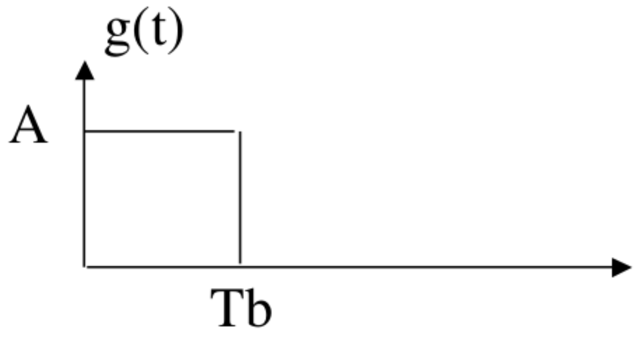


$$y(t) = x(t)\cos(2\pi f_c t)$$

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

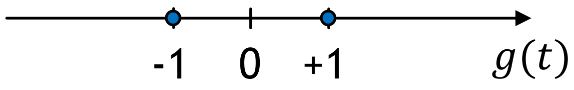
Baseband Signals

- The simplest digital modulation is ***Pulse Amplitude Modulation*** (PAM)
  - E.g. binary PAM or 2-PAM:
    - a pulse $g(t)$ of amplitude A is used to represent a "1"
    - a pulse $g(t)$ of amplitude -A to represent a "0"
- The simplest pulse is a rectangular pulse, but in practice other type of pulses are used



- We transmit the signal $s(t)$ corresponding to ***symbol*** s
- If we let $g(t)$ be the basic pulse shape, than with 2-PAM:
  - $s(t) = g(t)$ => "1"
  - $s(t) = -g(t)$ => "0"

Can we do better? Ideas?



Signals representation over the basis g(t)

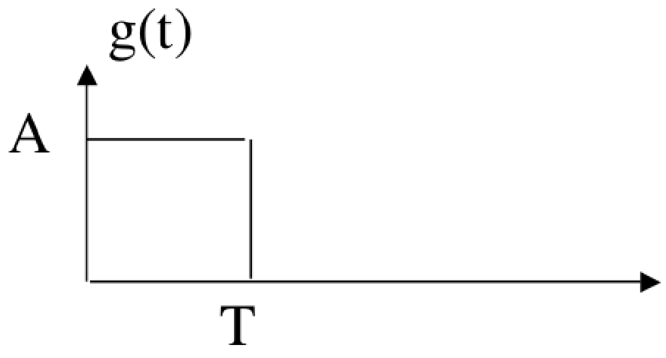
M-ary PAM

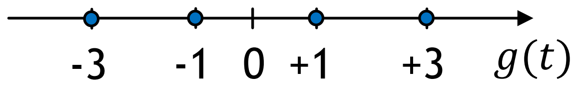
- Use M signal levels, $A_1 \ \ldots A_M$

- E.g., $M = 4 \Rightarrow A_1 = -3,\ A_2 = -1,\ A_3 = 1,\ A_4 = 3$
  - $s_i\,(t) = A_i\, g(t)$

- Mapping of bits to signals:
  - Each signal level can be used to represent $\log_2 M$ bits
  - E.g. $s_1(t) = 00;\ s_2(t) = 01;\ s_3(t) = 10;\ s_4(t) = 11$

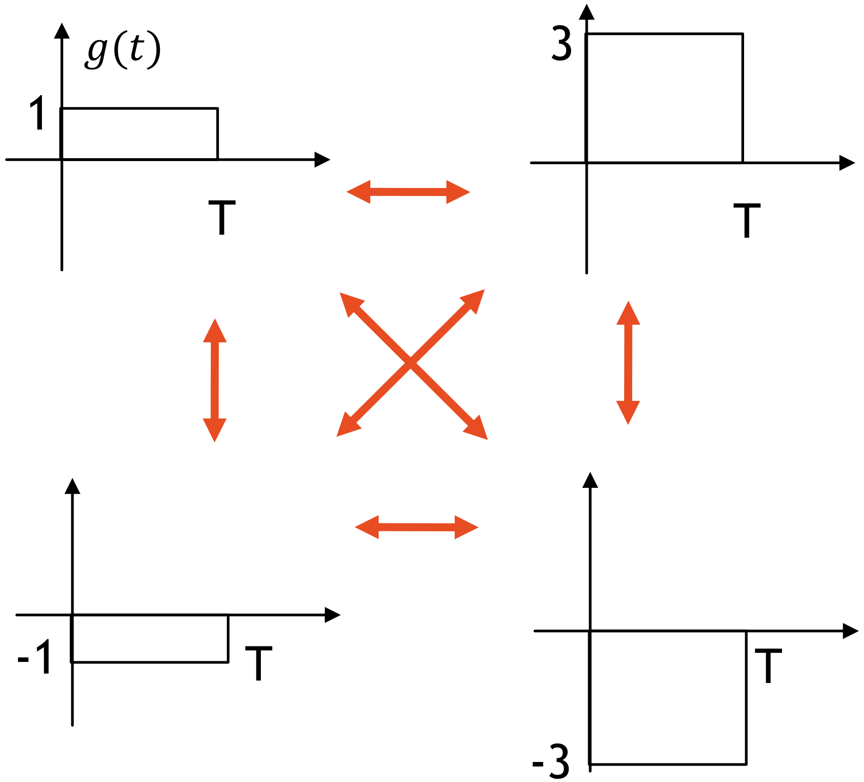
- Does the choice of bits matter?

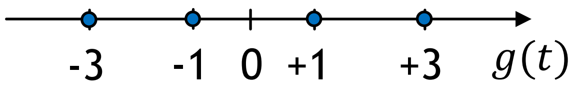




A look at signal detection

- Does the choice of bits matter?
  - What mistake is more likely?

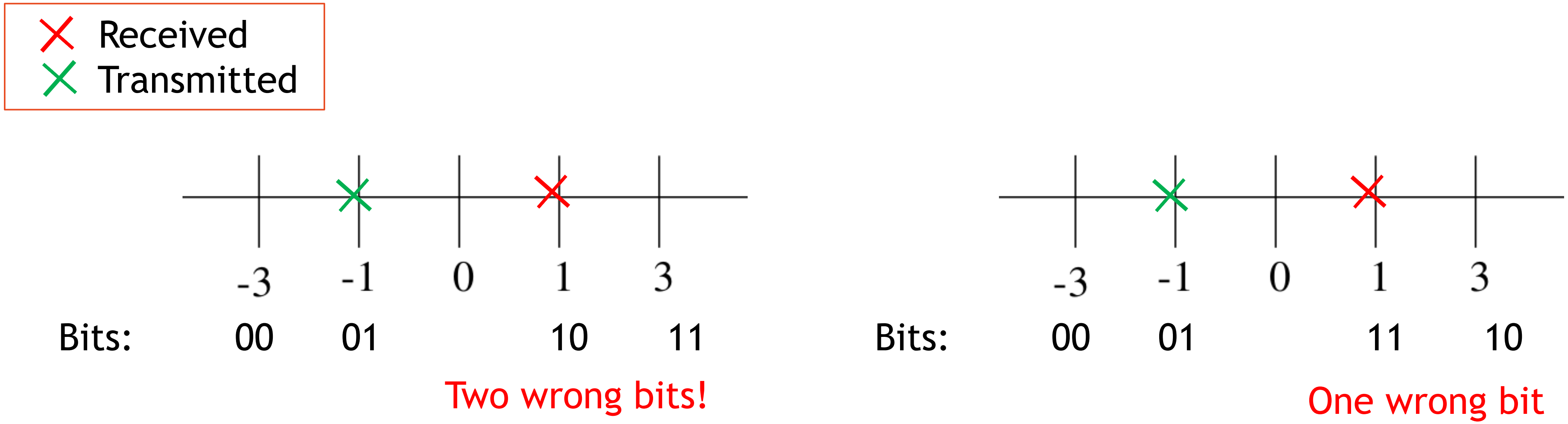




Signals representation over the basis g(t)

Gray Coding

- ***Gray coding***: strategy for **mapping bits to symbols** so that the number of bit errors is minimized
  - Most likely symbol errors are between adjacent levels
  - The number of bits that differ between adjacent levels is minimized
- Gray coding achieves 1 bit difference between adjacent levels
  - Most Likely error on symbols = error on one bit only

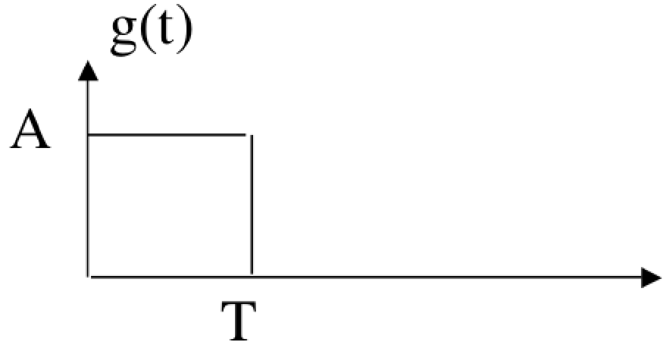


Energy per bit

- A measure of the ***energy efficiency*** of the modulation can be obtained from the **average** ***energy per bit***

$$E_b = E_s / \log_2 M$$

  - is the average energy per symbol divided by the number of bits carried by each symbol

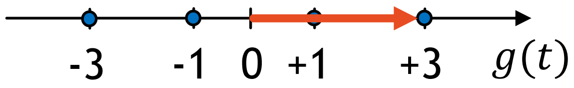


- Energy per symbol:

$$E_m = \int_0^T (S_m(t))^2\, dt = (A_m)^2 \int_0^T (g_t)^2\, dt = (A_m)^2 E_g$$

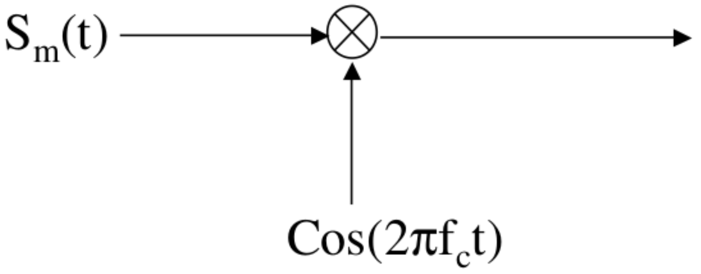
- Average energy per symbol $E_s = E_m / M$
- E.g., $M = 4 \Rightarrow A_1 = -3,\ A_2 = -1,\ A_3 = 1,\ A_4 = 3$
  - $s_i\,(t) = A_i\, g(t)$
  - $E_s = \frac{3^2T + 1^2T + 1^2T + 3^2T}{4} = 5T$

The distance from the origin is proportional to the energy of the symbol

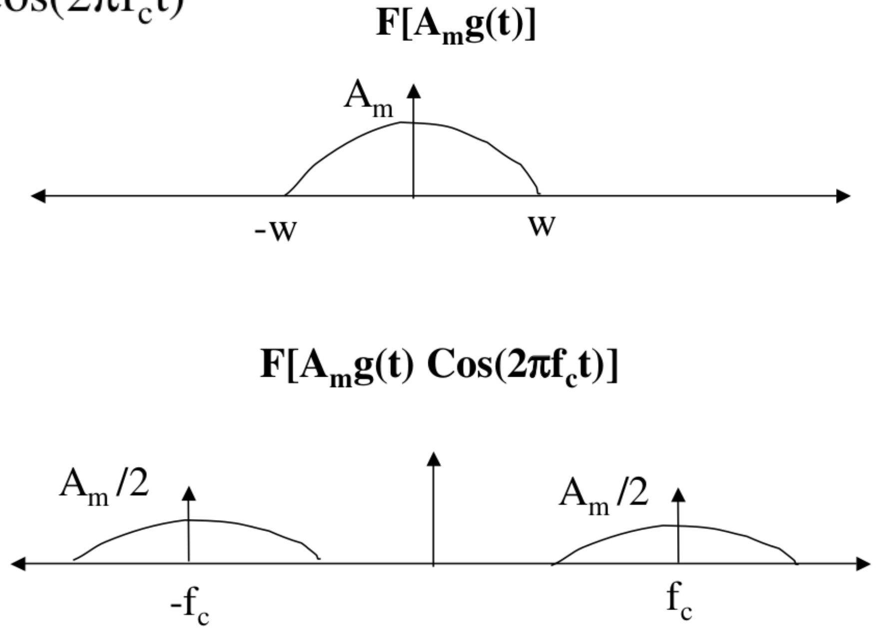


Bandpass signals

- To transmit a baseband signal $s(t)$ through a pass-band channel at some center frequency f_c, we multiply $s(t)$ by a sinusoid with that frequency
- The Fourier transform of $s_m(t) = A_m g(t)$ depends on $g(t)$

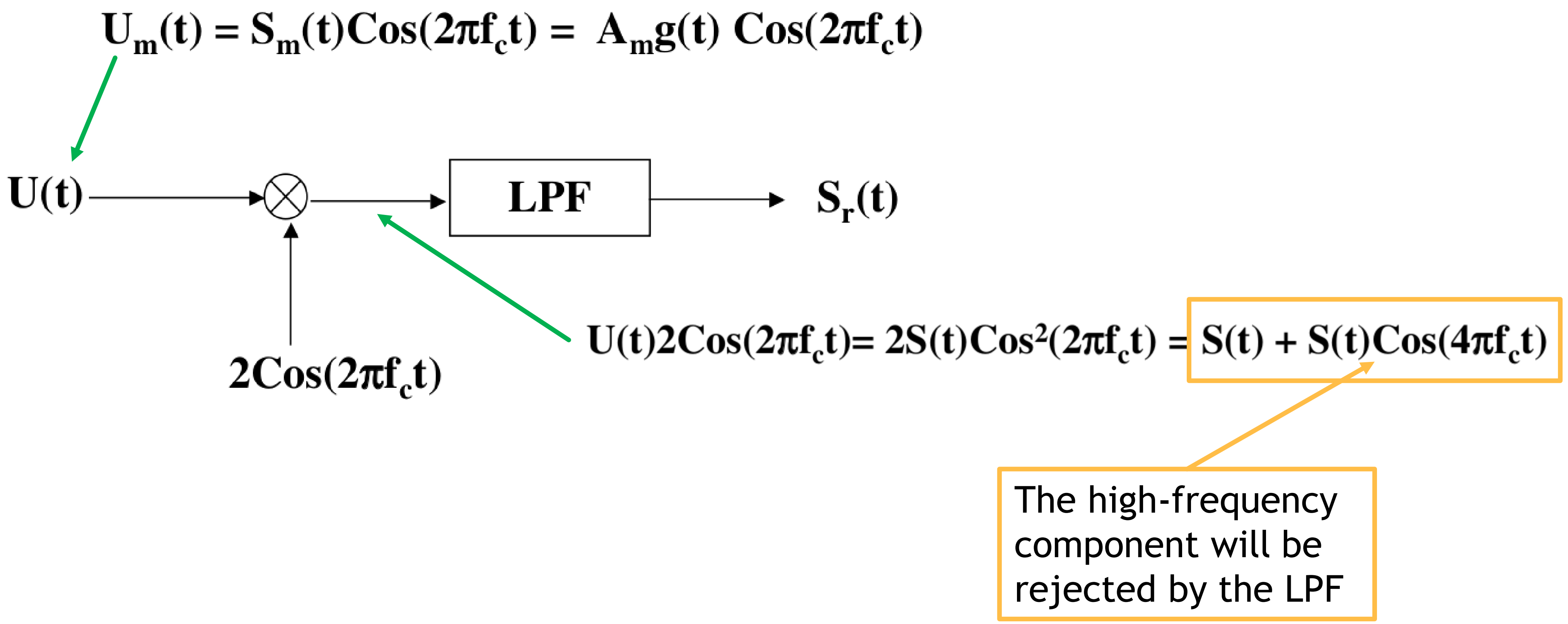


$$
\begin{aligned}
U_m(t) &= S_m(t)\mathrm{Cos}(2\pi f_c t) \\
&= A_m g(t)\ \mathrm{Cos}(2\pi f_c t)
\end{aligned}
$$



Demodulation

- To recover the original signal, multiply the received signal $U_m(t)$ by a cosine at the same frequency



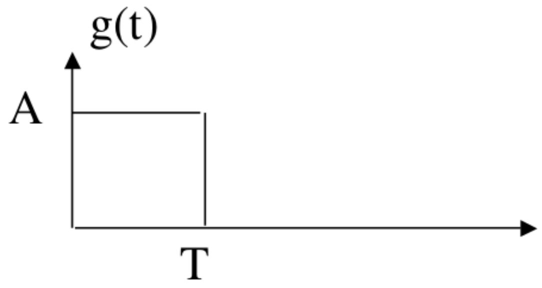
Bandwidth Occupancy

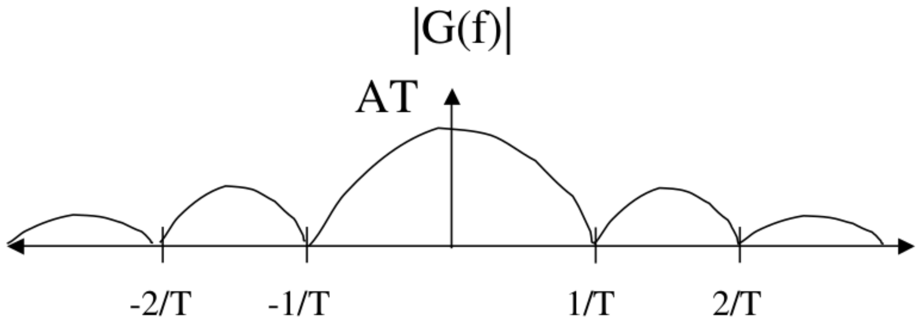
- Ideal rectangular pulse has unlimited bandwidth

$$G(f) = F[g(t)]$$

$$G(f) = \int_{-\infty}^{\infty} g(t) e^{-j2\pi f t} dt = \int_{0}^{T} A e^{-j2\pi f t} dt$$

$$G(f) = (AT) Sinc(\pi f T) e^{-j\pi f T}$$

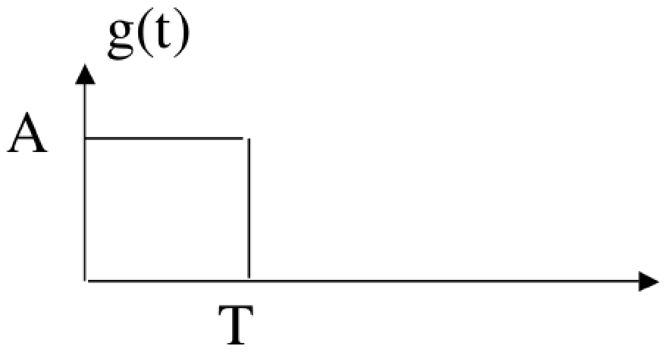


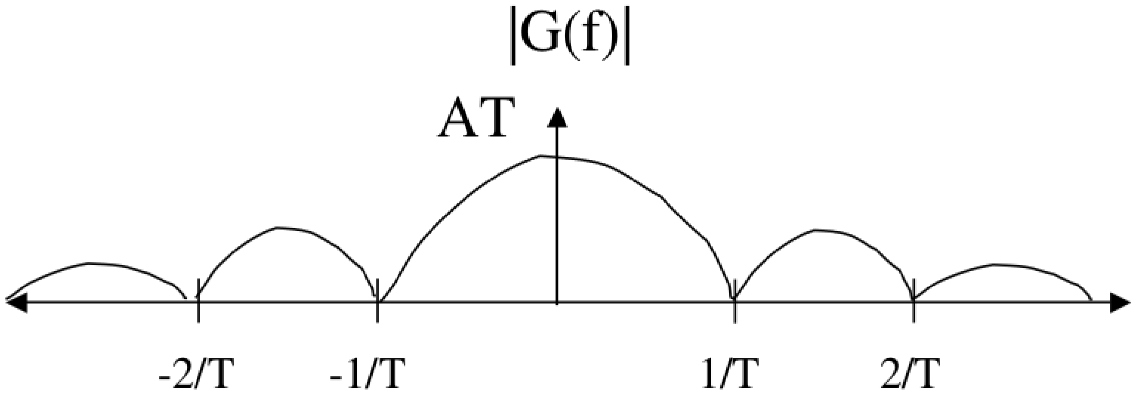


- Other types of pulses might be better
  - They shape the signal bandwidth!
  - We would like to put most of the energy in a small bandwidth

Bandwidth Efficiency

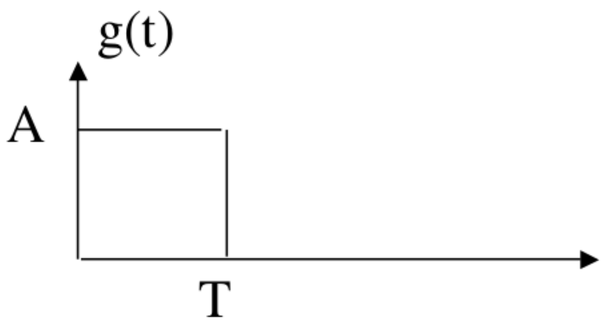
- Generally, we want to choose the pulse shape $g(t)$ in order to put more energy in a small bandwidth
- For a pulse of duration T,
  - the ***symbol rate*** is $R_s = 1/T$
- There are $\log_2(M)$ bits per symbol, therefore
  - the ***bitrate*** $R_b = \log_2(M)\, R_s$
- Roughly, the two-sided bandwidth is $BW \; = \; 2R_s = \frac{2}{T}$
  - The ***bandwidth efficiency*** is $\eta = \frac{R_b}{BW} = \frac{\log_2(M)}{T} * \left(\frac{T}{2}\right) = \frac{\log_2(M)}{2} \; bps/Hz$

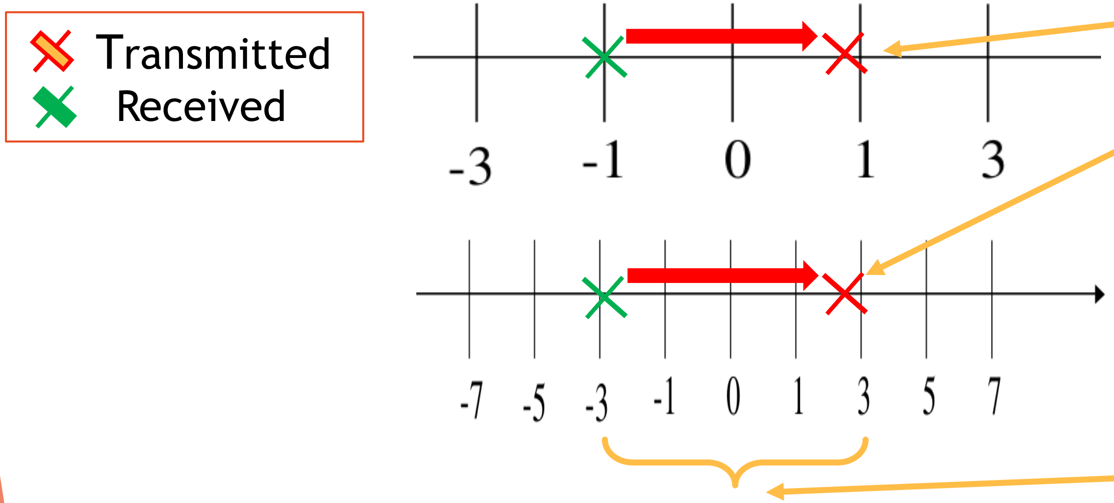




Bandwidth Efficiency (cont'd)

- The ***bandwidth efficiency*** is $\eta = \frac{R_b}{BW} = \frac{\log_2(M)}{2}\ bps/Hz$
- Increased BW efficiency with increasing M
- Example
  - M = 2 ⇒ BW efficiency = 1/2
  - M = 4 ⇒ BW efficiency = 1
  - M = 8 ⇒ BW efficiency = 3/2
- However, as M increases we are more prone to errors as symbols are closer together (for a given energy level)

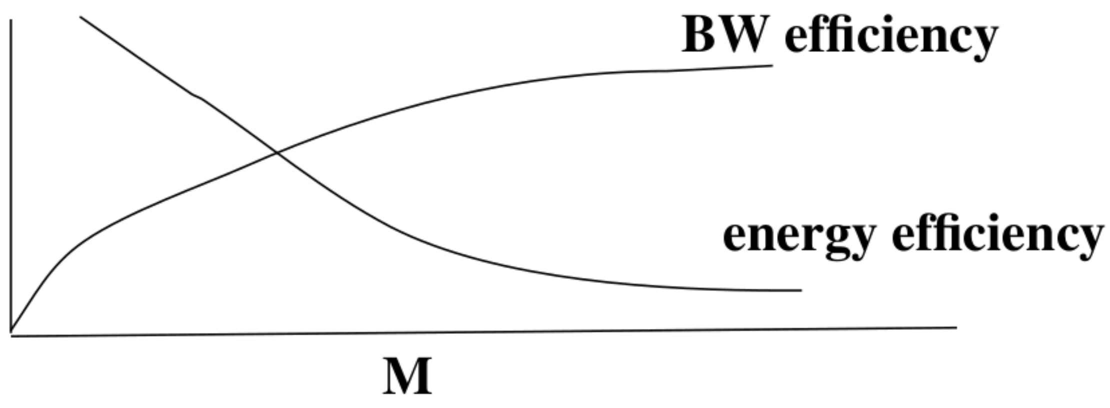


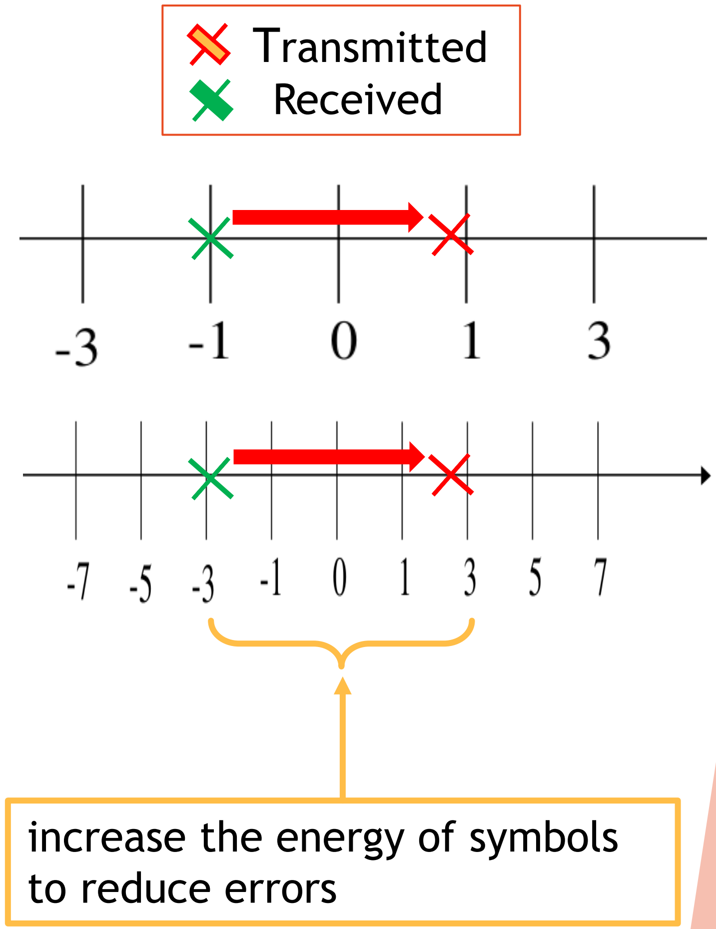


- The noise "moves" the received symbol
- The same amount of noise would result in a bigger error

Bandwidth Efficiency Vs Energy Efficiency

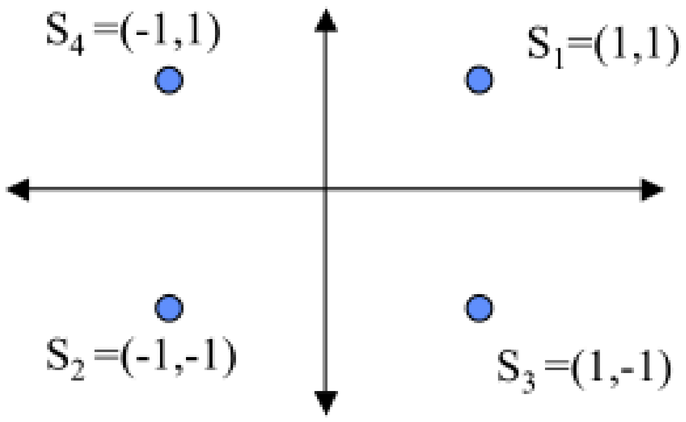
- BW efficiency increases with increasing M
- For a fixed energy level, as M increases, we are more prone to errors (closer symbols)
- Need to increase symbol energy level to overcome errors
- **Tradeoff** between **BW efficiency and energy efficiency**





Two-dimensional Modulations

- Signals can be represented over two orthonormal basis
  - A Set of signal points s_i is called a *constellation*
- 2-D constellations are commonly used
- Large constellations can be used to transmit many bits per symbol
  - More bandwidth efficient (higher bitrate)
  - More error prone
- The “shape” of the constellation can be used to **minimize error probability** by keeping symbols as far apart as possible
- Common constellations:
  - *QAM: Quadrature Amplitude Modulation*
    - a PAM in two dimensions
  - *PSK: Phase Shift Keying*
    - Special constellation where all symbols have equal power



Symmetric M-QAM

- M is the total number of signal points (symbols)
- $\sqrt{M}$ signal levels on each axis

$$S_m = (A_m^x, A_m^y),\ A_m^x, A_m^y \in \left\{+/-1, +/-3, \ldots, +/-(\sqrt{M}-1)\right\}$$

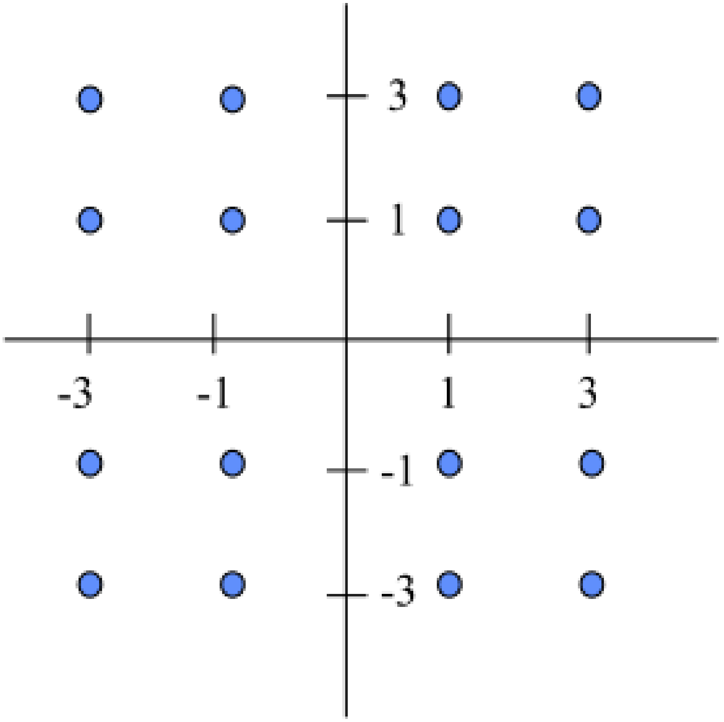
- Constellation is symmetric => M=K^2, for some K
- Signal levels on each axis are the same as for PAM

$$E.g., 4-QAM \Rightarrow A_m^x, A_m^y \in \{+/-1\}$$

$$16-QAM \Rightarrow A_m^x, A_m^y \in \{+/-1, +/-3\}$$

- Using the same pulse $g(t)$, the **bandwidth efficiency** is the same of M-PAM
- But QAM has a larger **energy efficiency** than PAM

16-QAM

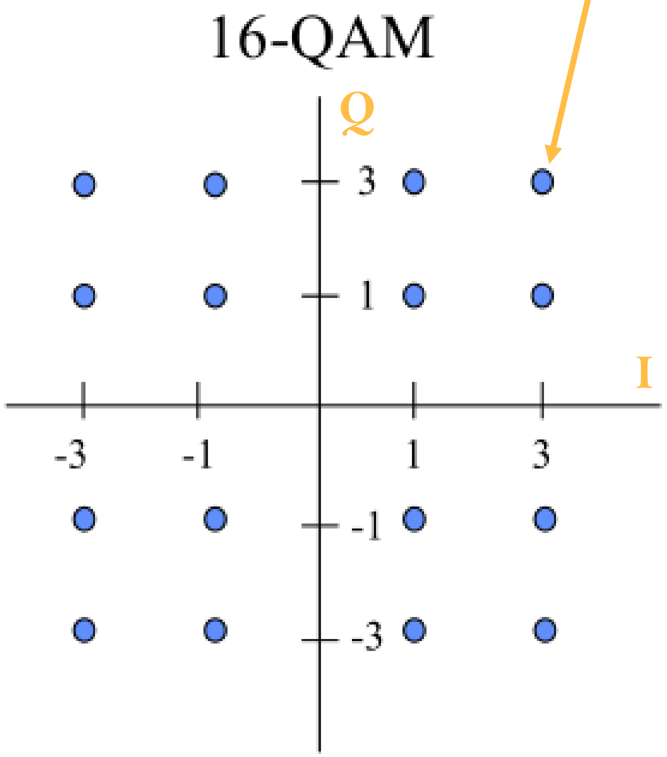


Bandpass QAM

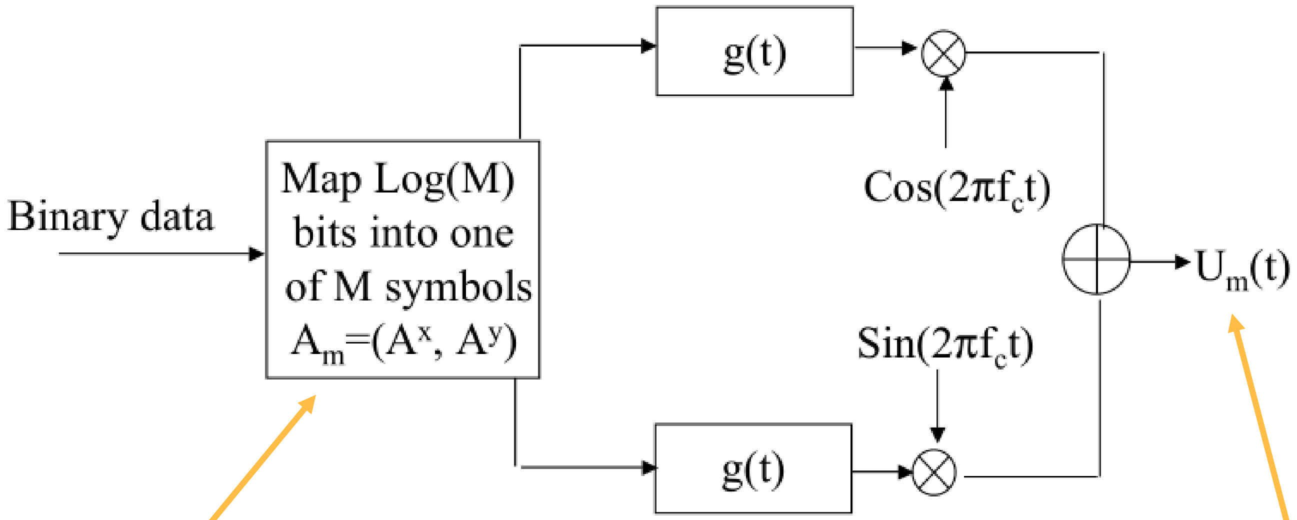
- Modulate the two dimensional signal by multiplication by orthogonal carriers (sinusoids): Sine and Cosine
  - This is accomplished by multiplying the A^x component by Cosine and the A^y component by sine
- The two carriers are a complete basis for the transmitted signals
  - Referred to as the ***In-phase*** **(I)** and ***quadrature phase*** **(Q)** axes
  - The constellation is the same, the basis accounts for the frequency modulation
- The transmitted signal, corresponding to the m-th symbol is:

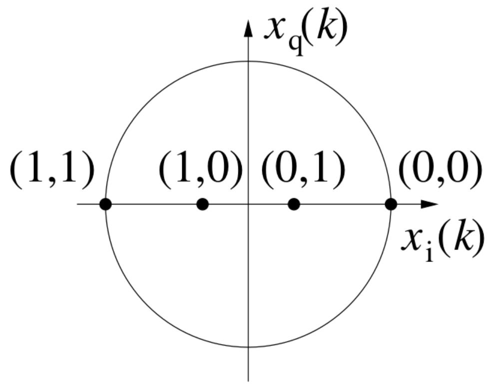
$$U_m(t) = A_m^x g(t) Cos(2\pi f_c t) + A_m^y g(t) Sin(2\pi f_c t), \; m = 1..M$$

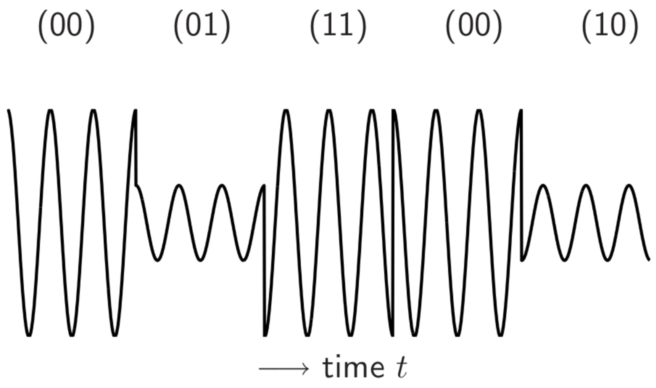
$$S_m = (A_m^x, A_m^y)$$



M-QAM Modulator





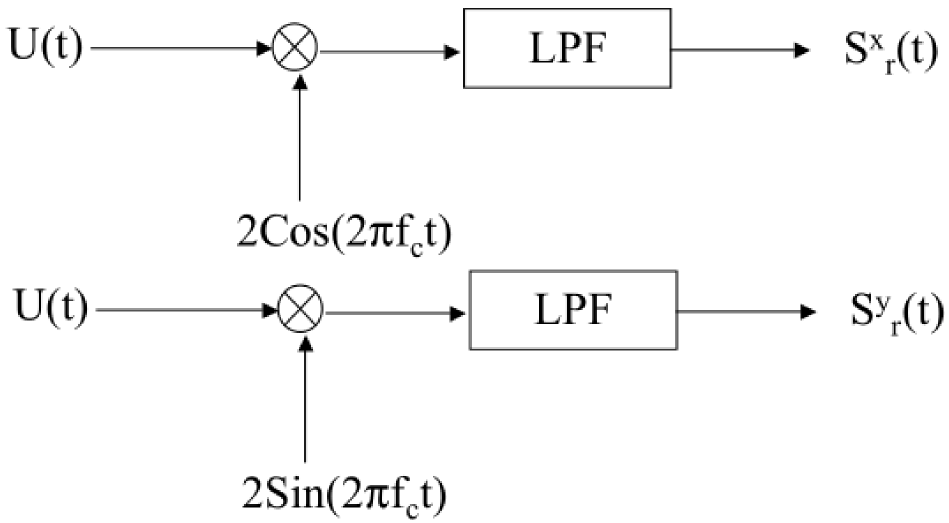


$00 \Rightarrow S_1$
$01 \Rightarrow S_2$
$11 \Rightarrow S_3$
…

M-QAM Demodulation: Recovering the baseband signals

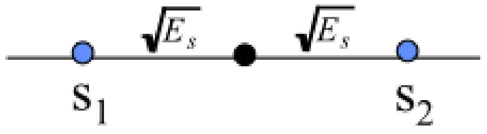
- Over a symbol duration, $\sin(2\pi f_c t)$ and $\cos(2\pi f_c t)$ are ***orthogonal***
- As long as the symbol duration is an integer number of cycles of the carrier wave
  - i.e. $f_c = n/T$ for some n
- When multiplied by a sine, the cosine component of $U(t)$ disappears after filtering
- Similarly, the sine component disappears when multiplied by cosine

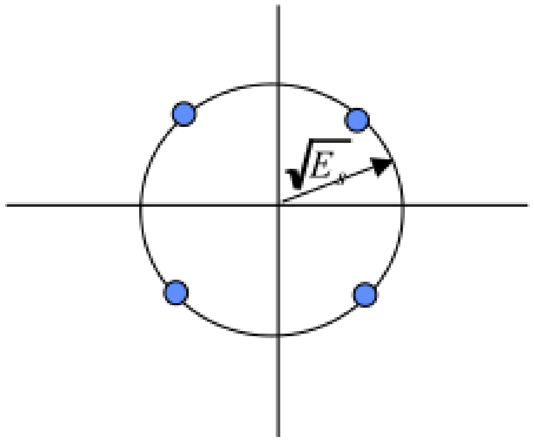
$$U_m(t) = A_m^x g(t) Cos(2\pi f_c t) + A_m^y g(t) Sin(2\pi f_c t), \; m = 1..M$$



Phase Shift Keying (PSK)

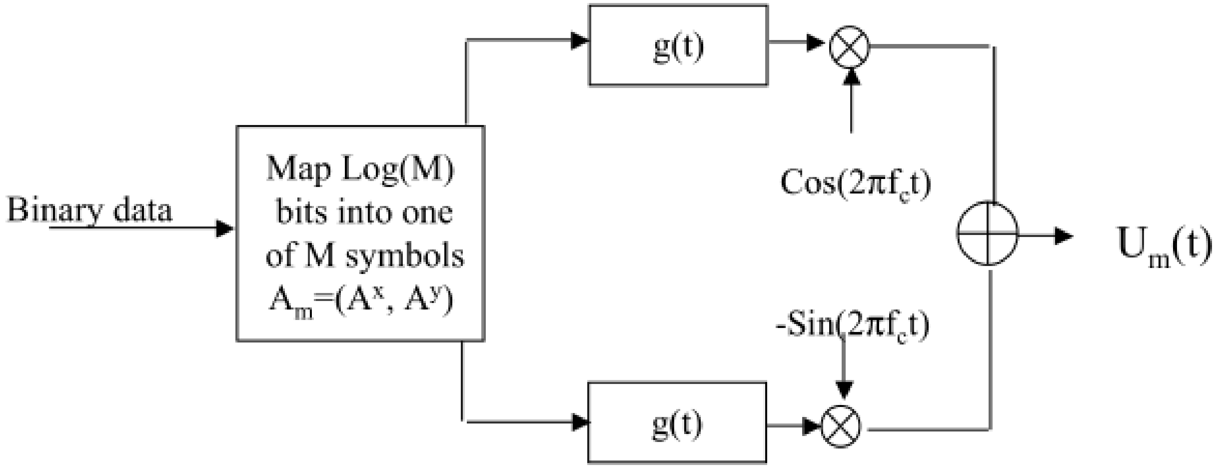
- ***Phase Shift Keying***
- Two Dimensional signals where all symbols have equal energy levels
  - I.e., they lie on a circle or radius $\sqrt{E_s}$
- Symbols are equally spaced to minimize likelihood of errors
  - E.g., Binary PSK
  - 4-PSK (same as 4-QAM)
- M-PSK
  - Constellation of M phase-shifted symbols
  - All have equal energy levels
  - $\log_2 M$ bits per symbol

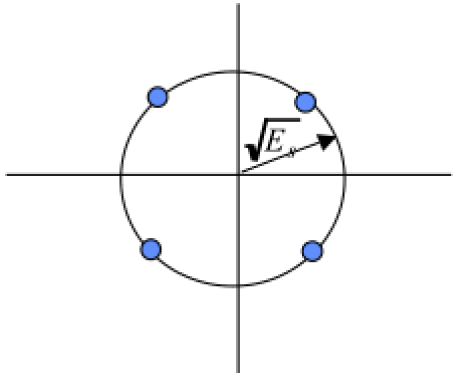


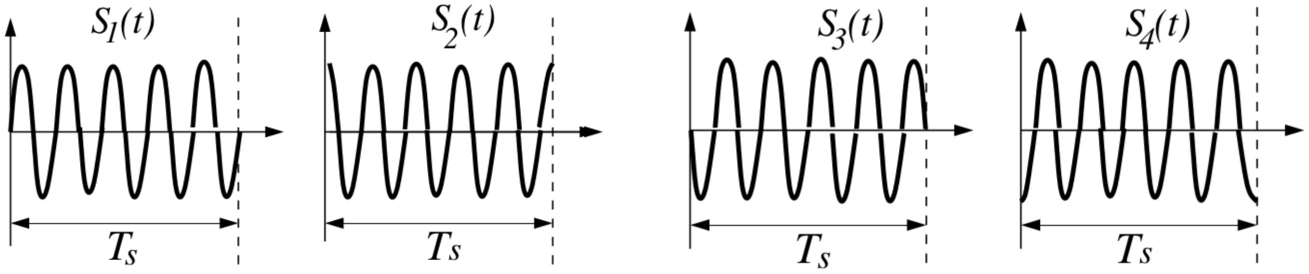


M-PSK Modulator

- Essentially the same modulator and demodulator of M-QAM







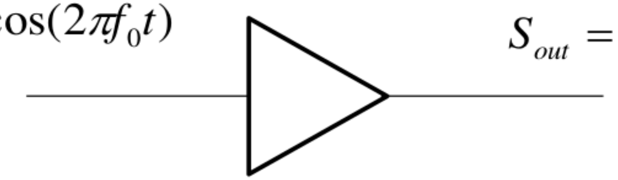
bit (0,0): $\phi_1 = 0$ bit (0,1): $\phi_2 = \frac{\pi}{2}$ bit (1,1): $\phi_3 = \pi$ bit (1,0): $\phi_4 = \frac{3\pi}{2}$

Power Amplifiers

- Power is proportional to amplitude
- To increase amplitude (hence power) the last block of the transmitter before entering the antenna is always the amplifier

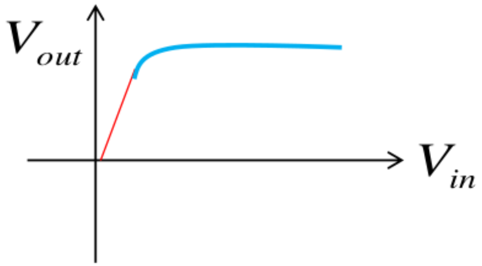
Increase of signal amplitude → Increase of Power

$$S_{in} = V_{in}\cos(2\pi f_0 t)$$



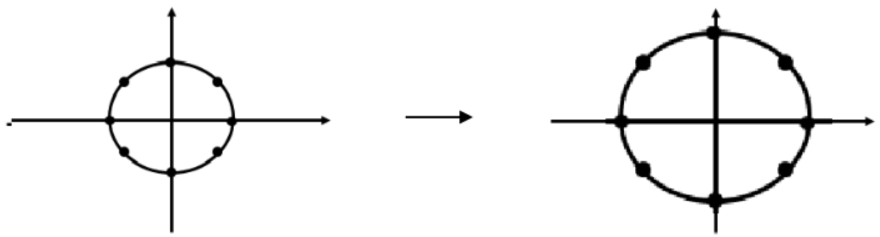
$$S_{out} = V_{out}\cos(2\pi f_0 t)$$

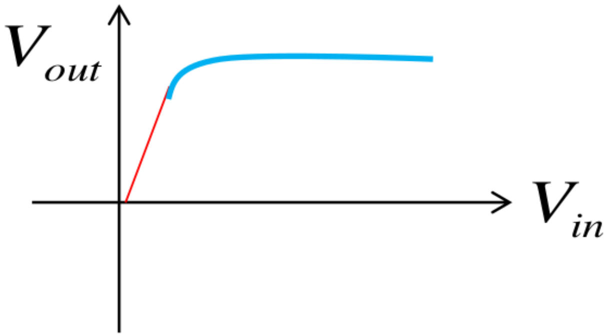
- operating point in the saturation region → maximum power transfer.
- operating point in the linear region → no maximum power transfer



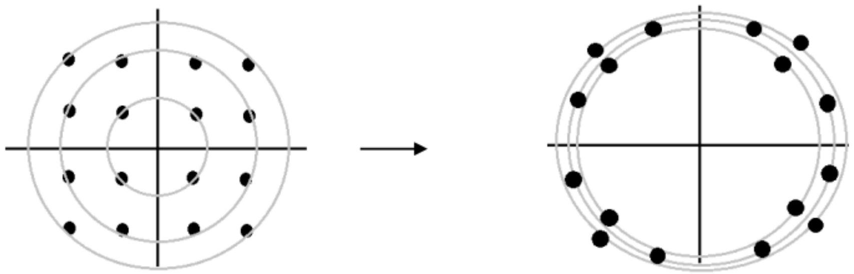
Power Amplifiers: PSK vs QAM

- **PSK**: even when working in saturation, the constellation is amplified uniformly





- **QAM**: working in the saturation zone the signal are scaled differently
  - The constellation is not ideal and its performace in terms of errors are worse



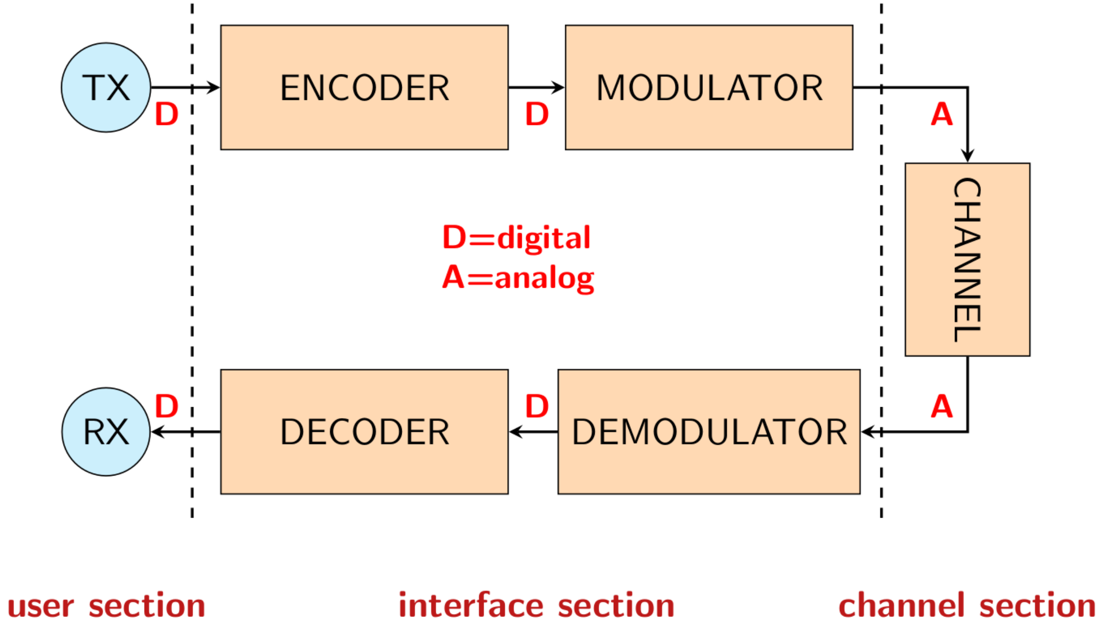
- Working in the linear zone all the circles are multiplied by the same factor.
  - The constellation is not distorted
- But the power is not maximum
  - Trade-off between **transmitted power** and **signal quality** (*input back-off*)

Contents

Challenges of the wireless medium

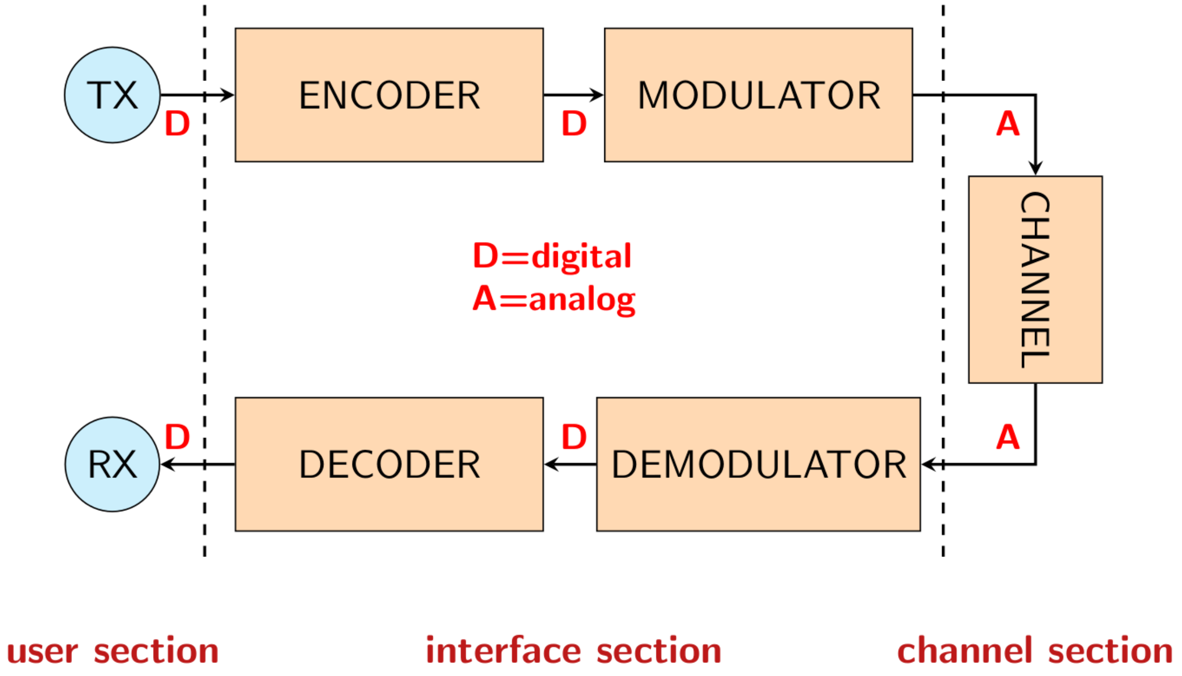
- Our goal is to communicate information (i.e. bits)
  - I.e. to transmit something that will be received correctly
- We talk binary, but we have to transmit over analog media

- Possible Challenges:
  - Share a medium (multiplexing)
  - Fight **noise** and channel **impairements**



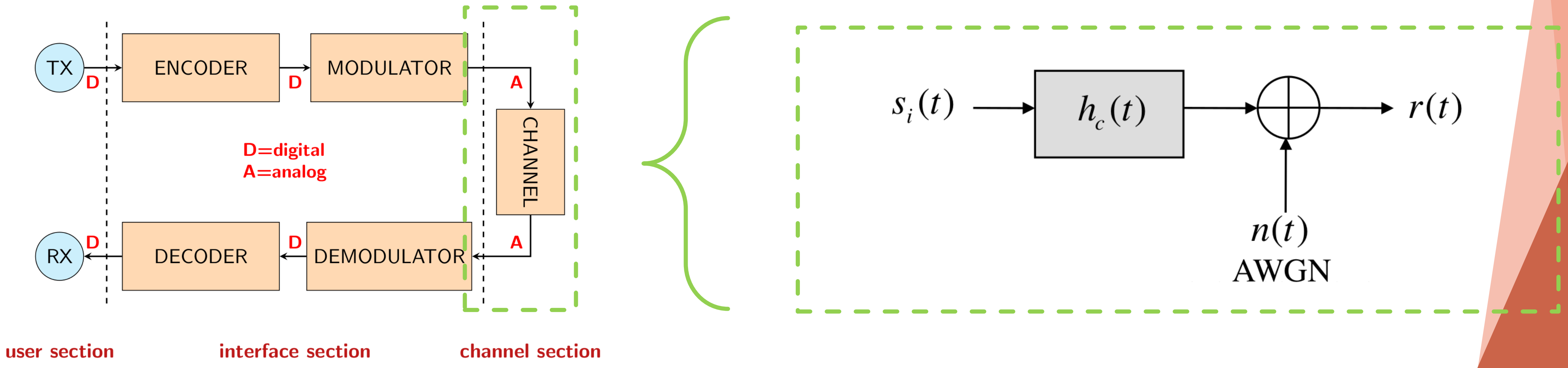
Digital Communication System: Channel

- *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



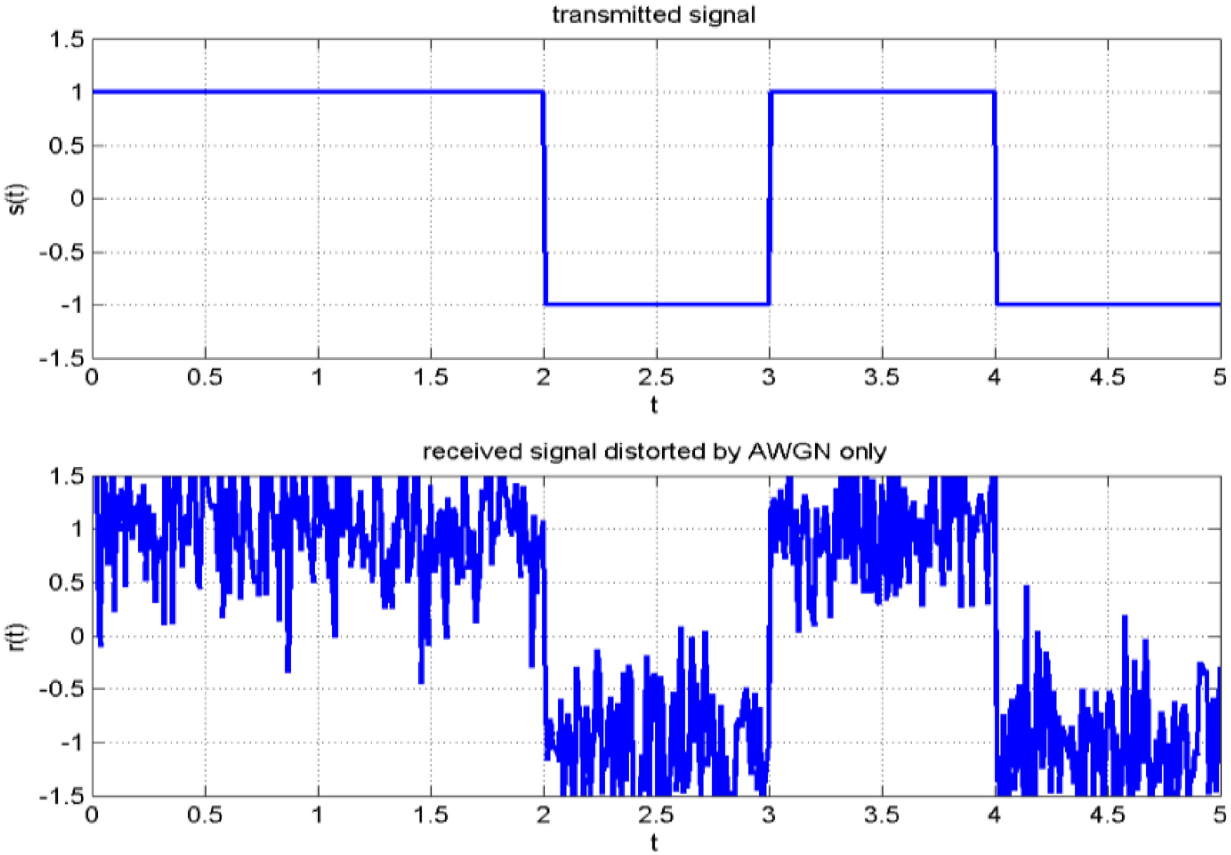
The Communication Channel

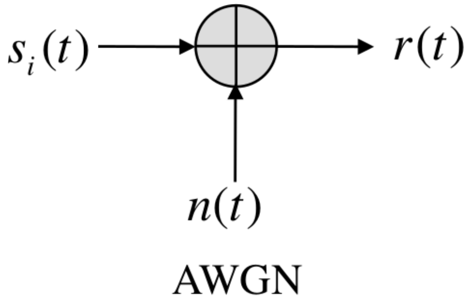
- Major sources of error:
  - *Thermal Noise (AWGN)*
    - disturbs the signal in an additive fashion (Additive)
    - has flat spectral density for all frequencies of interest (White)
    - is modeled by Gaussian random process (Gaussian Noise)
  - *Inter-Symbol Interference (ISI)*
    - Due to the filtering effect of transmitter, channel and receiver, symbols are “smeared”



Impact of the channel

- Simplifying our model, the received signal experience additive noise
- Example:

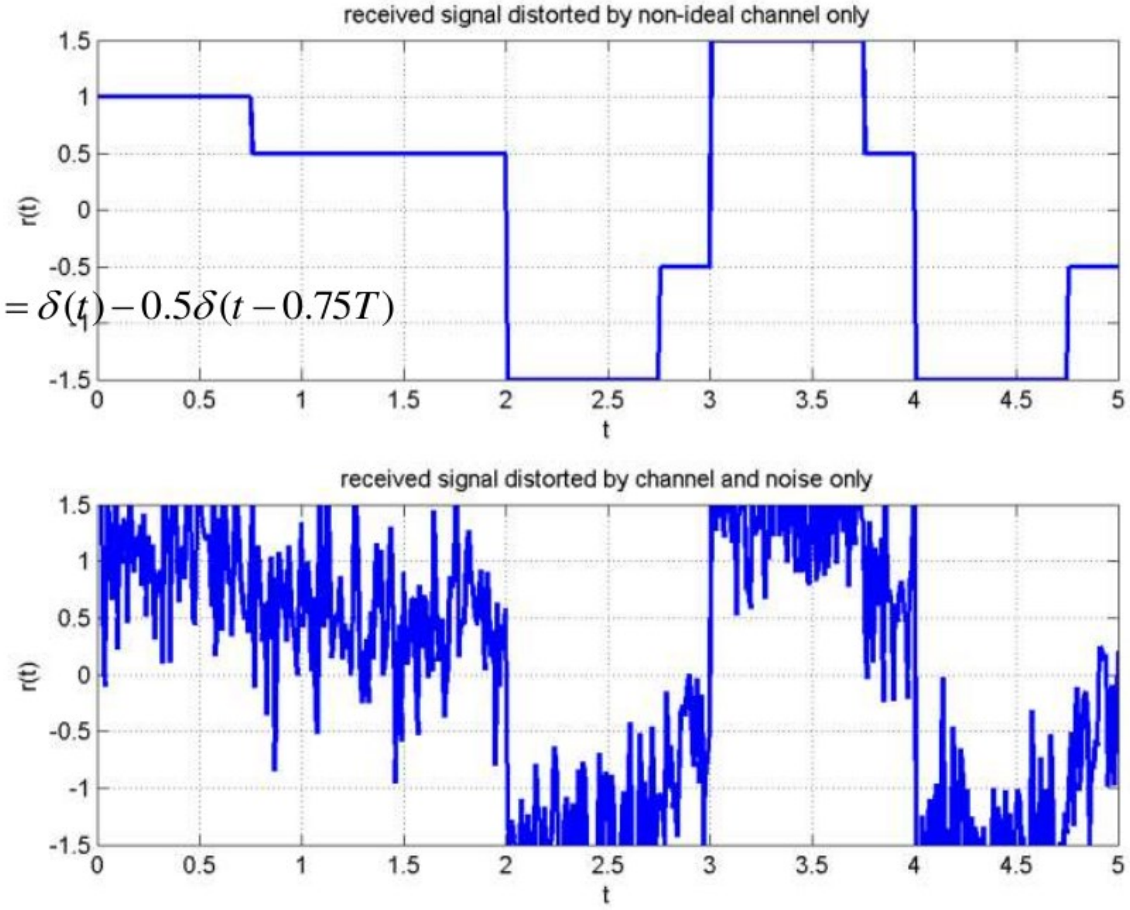




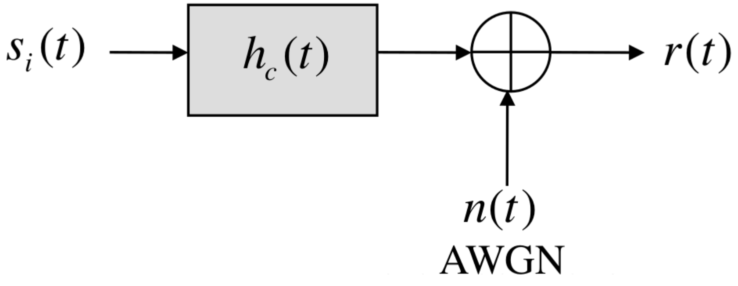
$$\boxed{r(t) = s_i(t) + n(t)}$$

Impact of the channel

- According to our model, the received signal is both filtered and noisy
- Example:



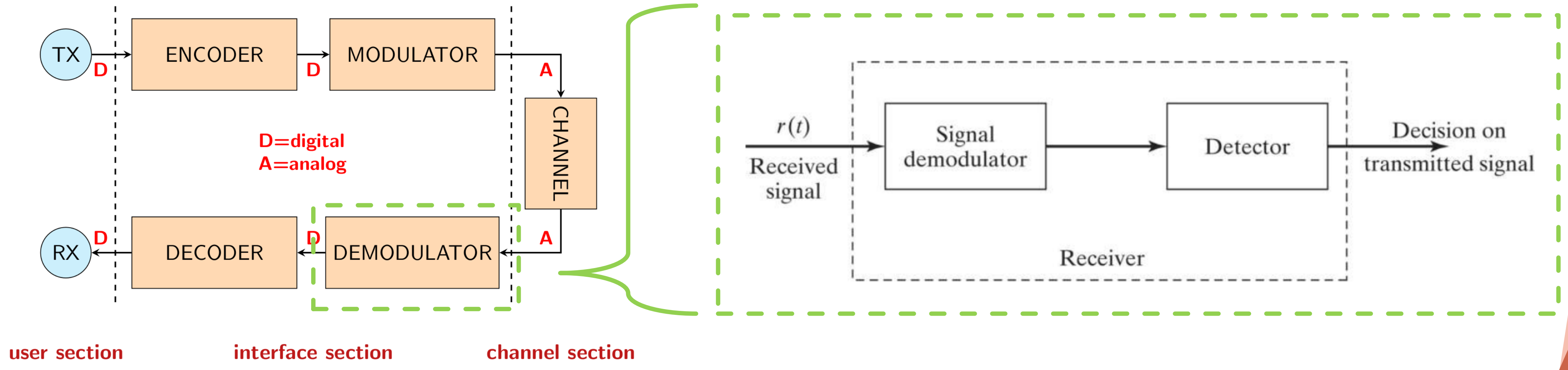
$h_c(t) = \delta(t) - 0.5\delta(t - 0.75T)$



$$\boxed{r(t) = s_i(t) * h_c(t) + n(t)}$$

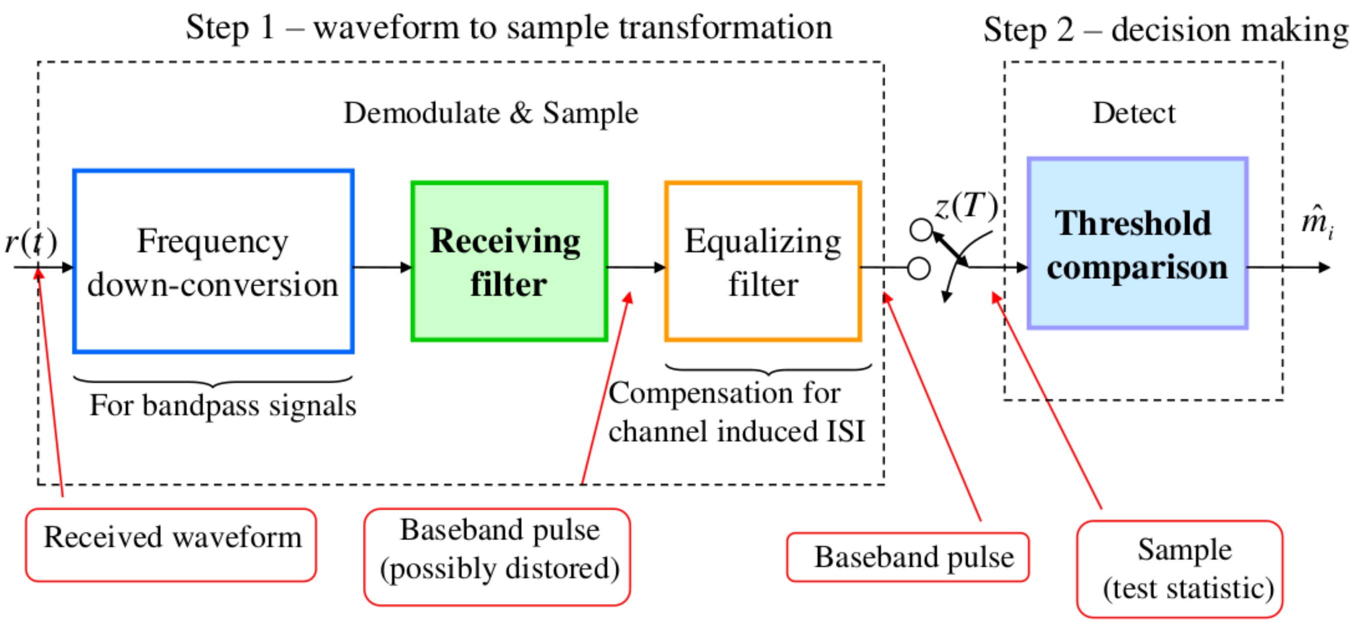
Receiver Tasks

- Demodulation and sampling
  - Waveform recovery and preparing the received signal for detection
    1. Improving the signal-to-noise ratio (SNR) using ***matched filter***
    2. Reducing ISI using ***equalizer***
    3. **Sampling** the recovered waveform
- Detection
  - **Estimate** the transmitted symbol based on the received **sample**



Receiver Tasks

- Demodulation and sampling
  - Waveform recovery and preparing the received signal for detection
    1. Improving the signal-to-noise ratio (SNR) using ***matched filter***
    2. Reducing ISI using ***equalizer***
    3. **Sampling** the recovered waveform
- Detection
  - **Estimate** the transmitted symbol based on the received **sample**



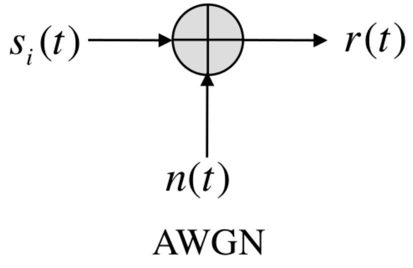
Designing the Receiver

- Find optimum solution for receiver design with the following goals:
  - Maximize SNR
  - Minimize ISI

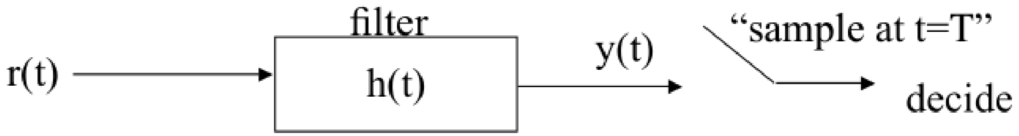
- Steps in design:
  - Model the received signal
  - Find separate solutions for each of the goals

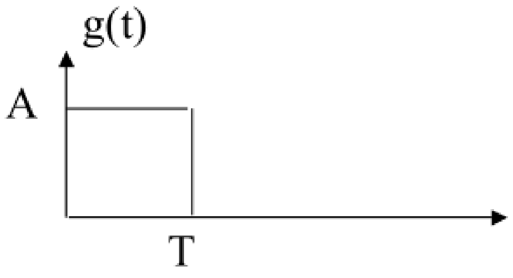
Maximize SNR

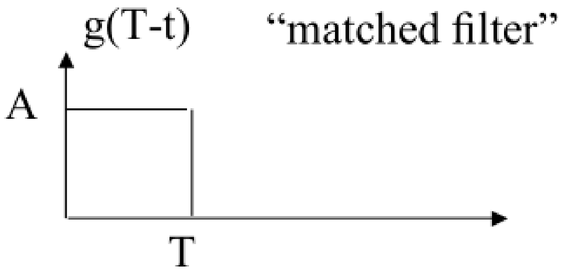
$$\boxed{r(t) = s_i(t) + n(t)}$$



- How to Maximize SNR?
- Simplified noise model
  - $n(t)$ is a random process (each "sample" of $n(t)$ is a random variable)
  - Its variance is proportional to the *noise density* N_0
- What is the filter $h(t)$ that yields the **maximum SNR at sampling**?
  - SNR is maximized by the ***matched filter*** $h(t) = g(T - t)$

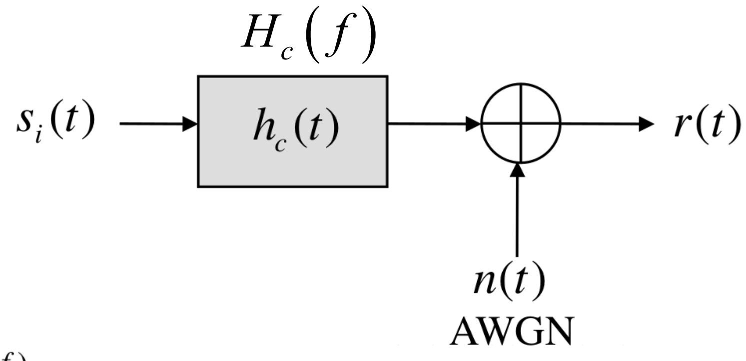






Minimize ISI

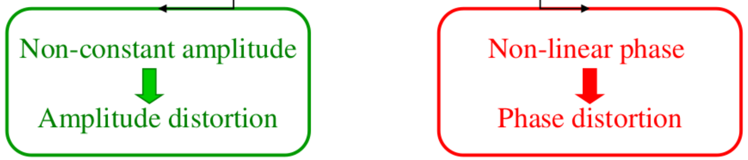
$$\boxed{r(t) = s_i(t) * h_c(t) + n(t)}$$



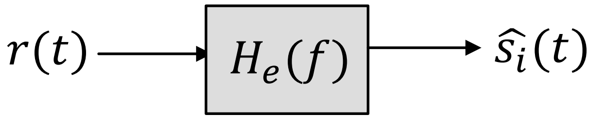
- How to minimize ISI?
- Channel impulse response must be reverted

- ISI due to filtering effect of the communications channel (e.g. wireless channels)
  - Channels behave like band-limited filters

$$H_c(f) = \underbrace{|H_c(f)|}\, e^{j\underbrace{\theta_c(f)}}$$



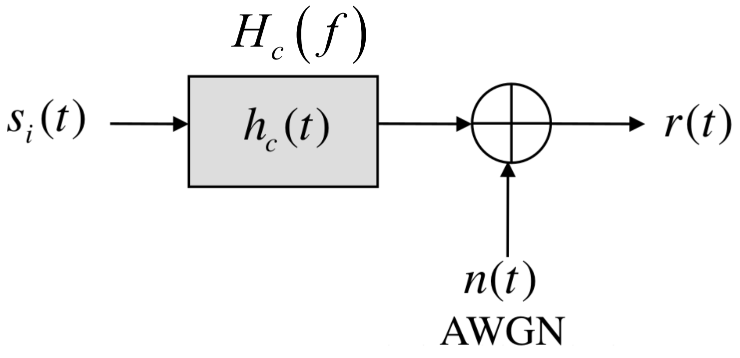
- A linear distortion can be compensated by an equalizer
  - Ideally: $H_e(f) = \frac{1}{H_c(f)}$
  - An approximation $\hat{s}_i(t)$ of the transmitted symbol is obtained



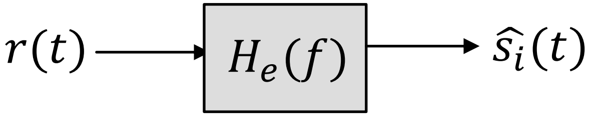
- How to know $H_c(f)$?

Minimize ISI

$$\boxed{r(t) = s_i(t) * h_c(t) + n(t)}$$



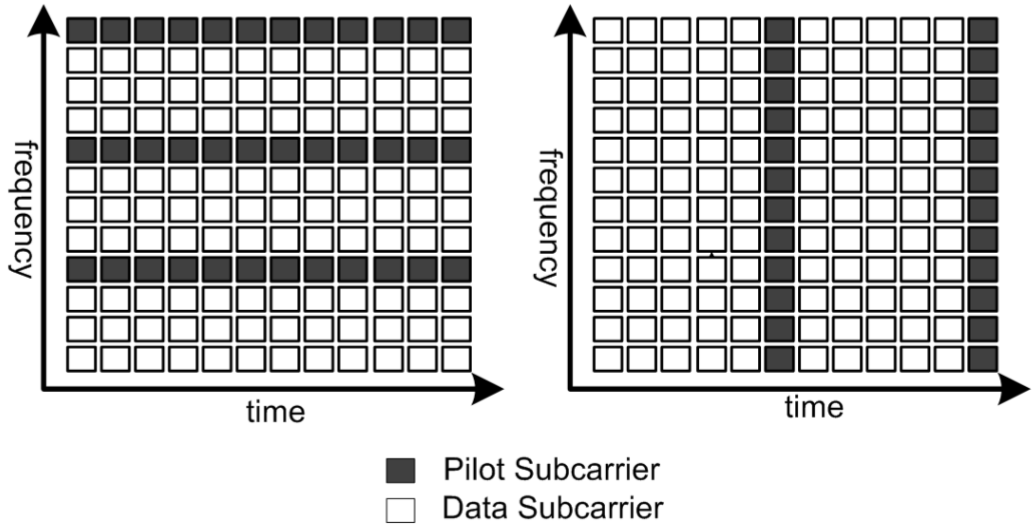
- How to know $H_c(f)$?
- *Channel Estimation* is the process that takes place before equalization in the communication system
  - The channel transfer function is estimated thanks to known signal characteristics



- Types based on the density of training symbols
  - Blind Channel Estimation
  - Semi-Blind Channel Estimation
  - Pilot Assisted Channel Estimation

Fading

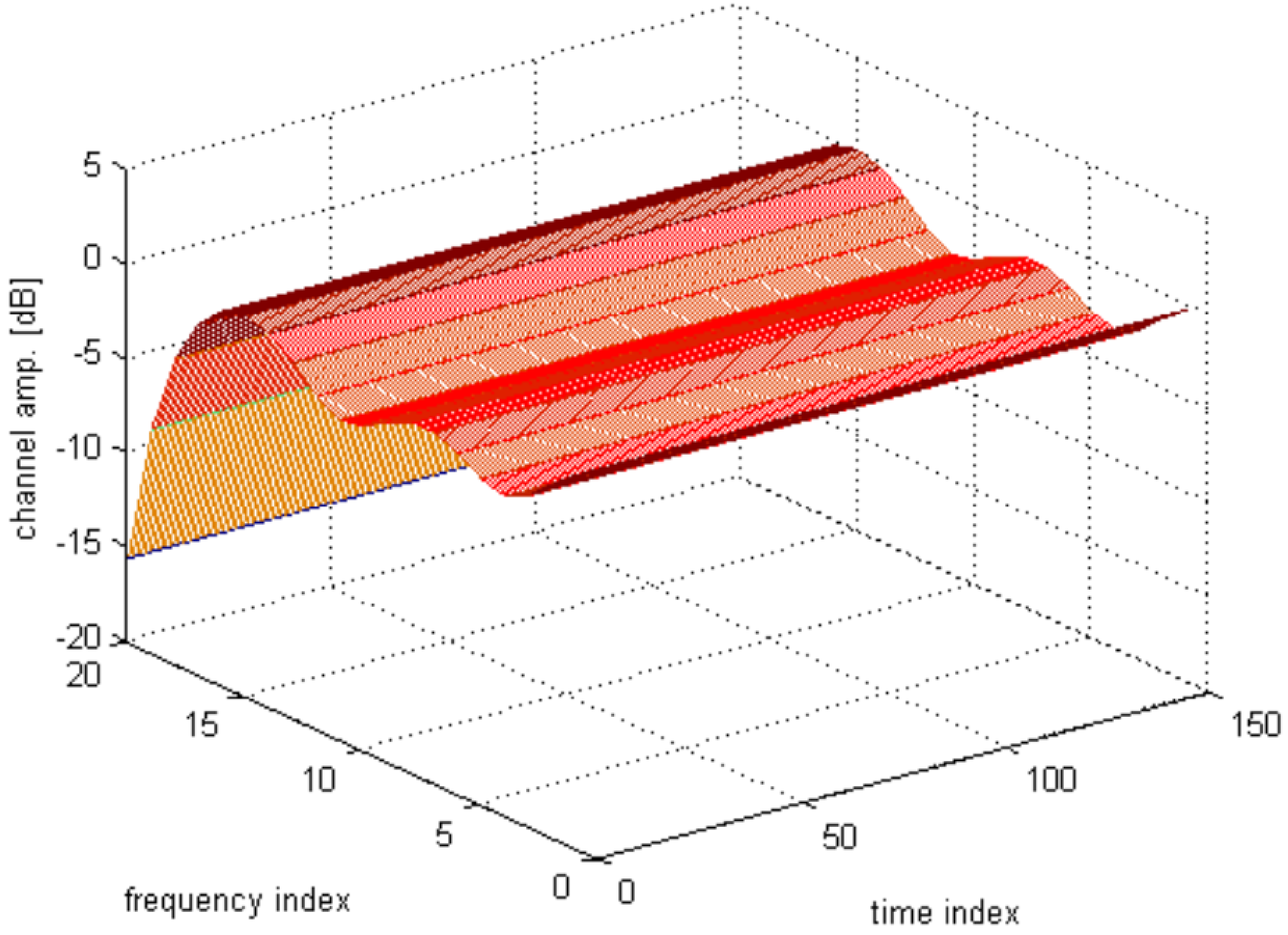
- Slow Fading Channel
  - Channel impulse response variations are slow
  - Pilot Symbols are transmitted less frequently
- Fast Fading
  - Channel Impulse response variations are fast
  - Pilot symbols are transmitted more frequently
- Examples of Pilots Arrangement for Slow and Fast Fading Channel in OFDM



(a) Comb-Type Channel Estimation (b) Block-Type Channel Estimation

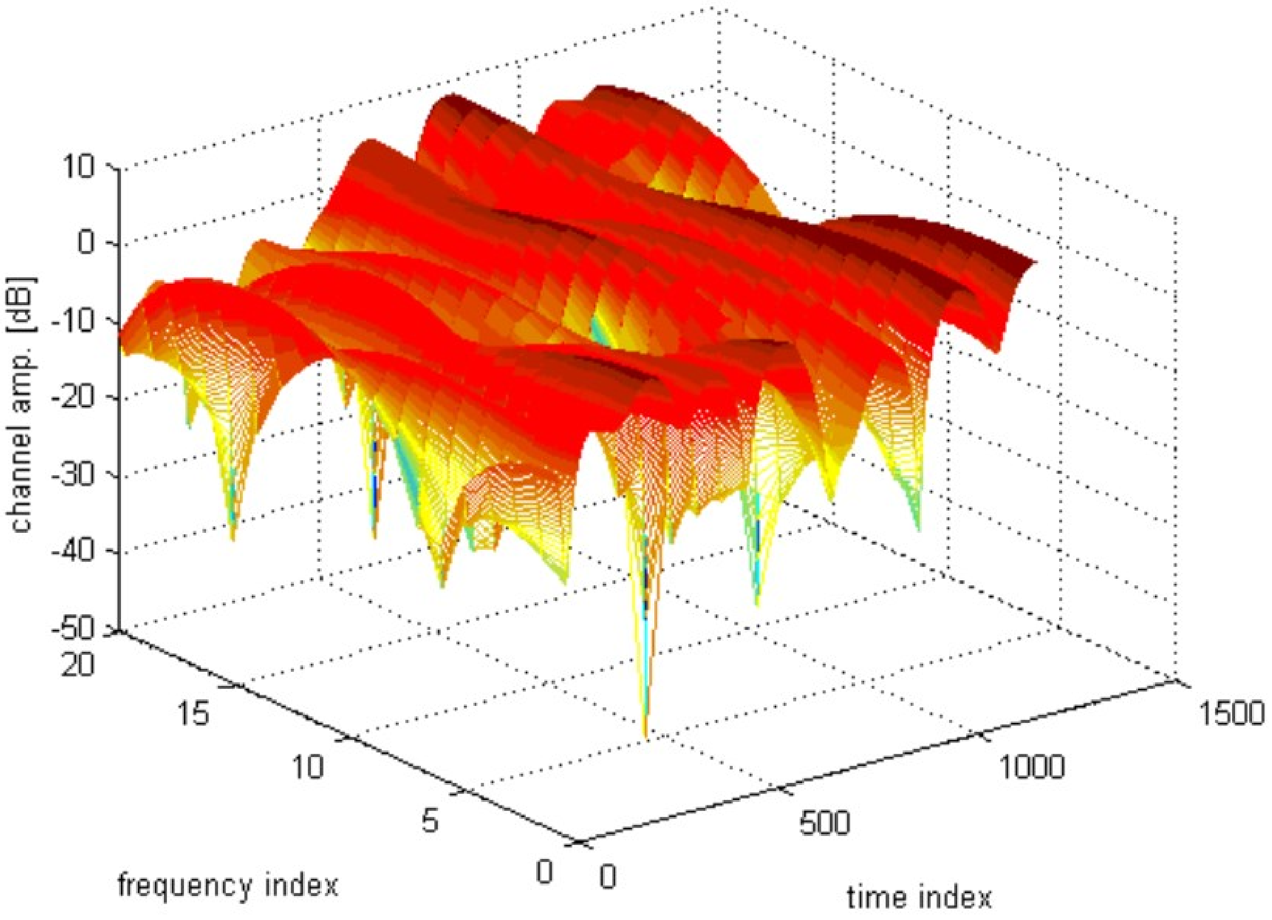
Slow Fading

- Example of a frequency selective, slowly changing (slow fading) channel for a user at 35 km/h



Fast Fading

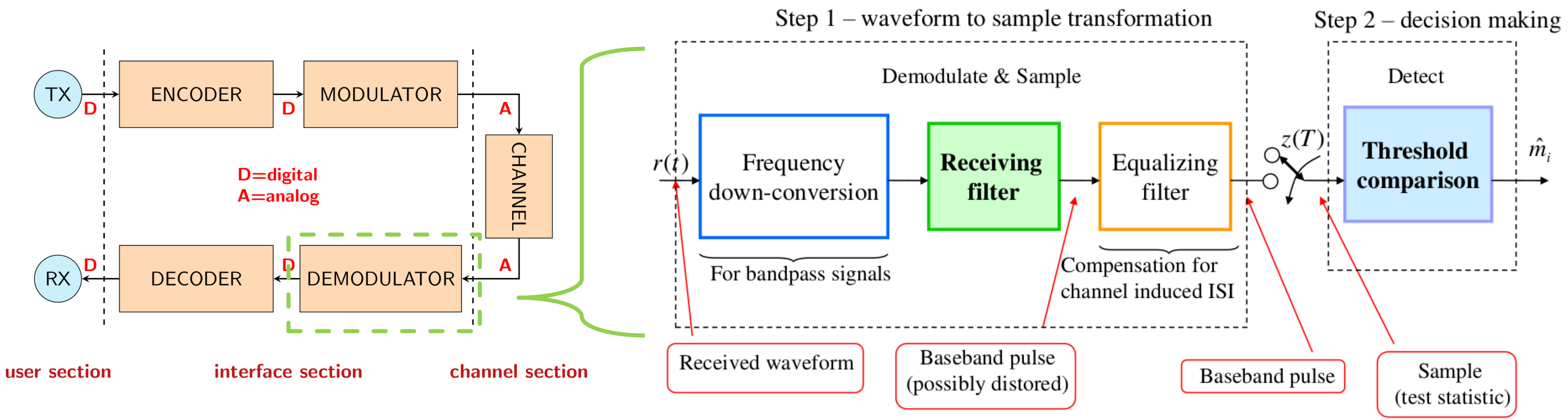
- Example of a frequency selective, fast changing (fast fading) channel for a user at 35 km/h



Contents

Symbols Detection

- After matched filtering we get $r = S_m + n$ with $S_m \in \{S_1, \ldots, S_M\}$
- How do we determine from r which of the M possible symbols was sent?
  - Without the noise we would receive what sent, but the noise can transform one symbol into another



Symbols Detection

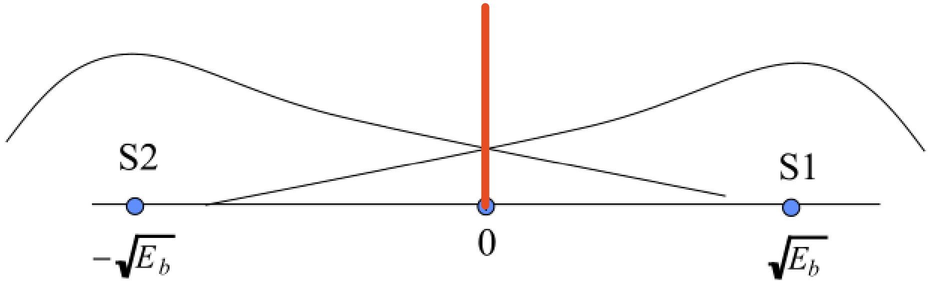
- Hypothesis testing
  - Objective: minimize the probability of a decision error
  - Decision rule: Choose S_m such that $P(S_m$ sent | r received) is maximized

- This is known as ***Maximum a posteriori*** probability (MAP) rule
- MAP Rule: Maximize the conditional probability that S_m was sent given that r was received
  - Turns out to be equivalent (under certain conditions) to **minimum distance decoding**
  - E.g. 2-PAM
    - If S_1 was sent then the received signal is $r = S_1 + n$
    - If S_2 was sent then the received signal is $r = S_2 + n$
    - Then if r > 0 decide S_1, if r < 0 decide S_2

$$d_{rS_m} = (r - S_m)^2$$

$$f_{r|s}(r \mid s1) = \frac{1}{\sqrt{\pi N_0}} e^{-(r-\sqrt{E_b})^2 / N_0}$$

$$f_{r|s}(r \mid s2) = \frac{1}{\sqrt{\pi N_0}} e^{-(r+\sqrt{E_b})^2 / N_0}$$



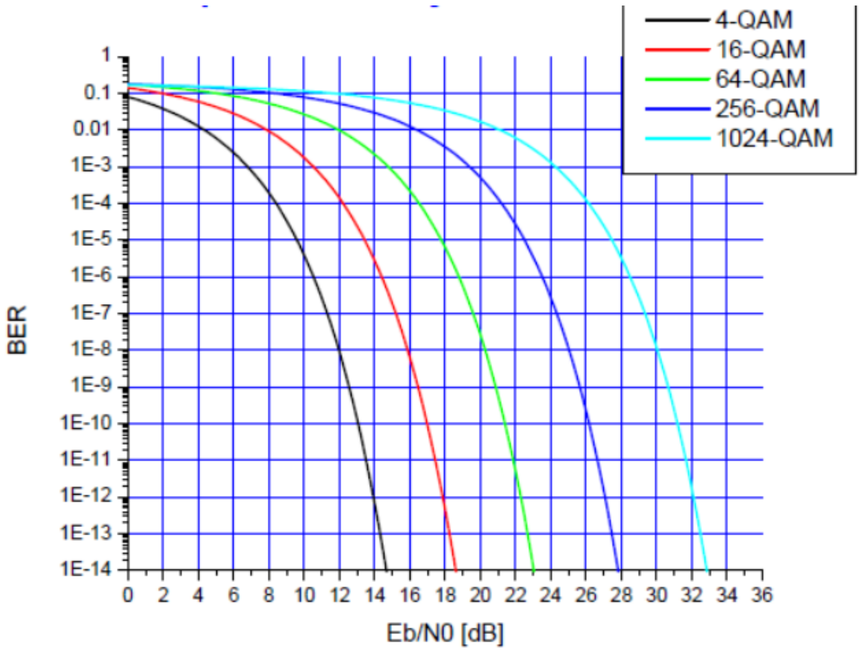
Probability of Error

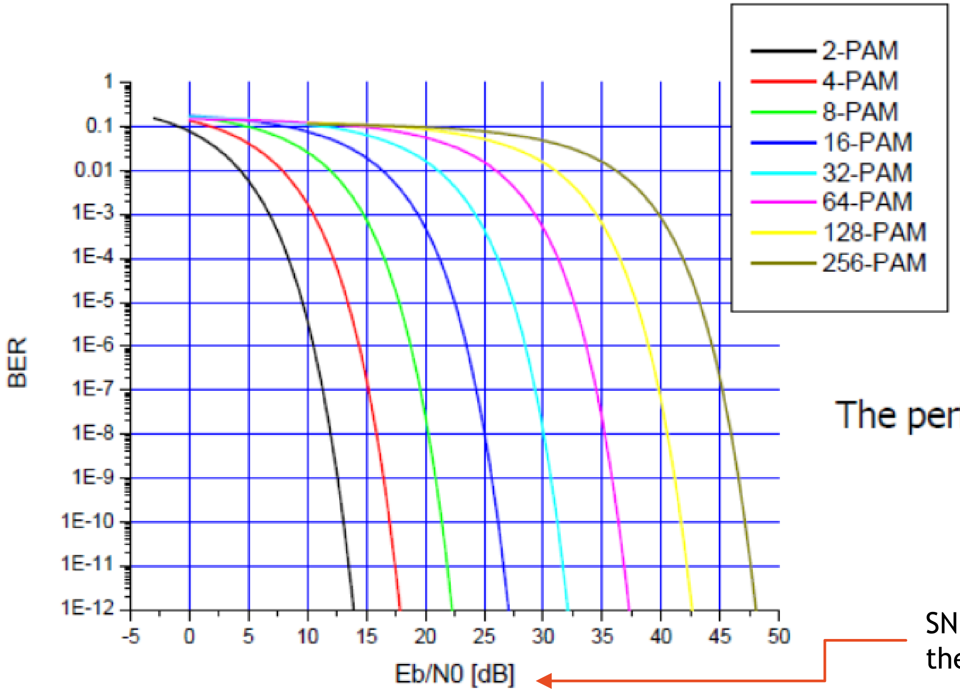
- In general, the probability of error P_e **between two symbols** separated by a **distance** *d* is given by:

$$P_e(d) = Q\left(\sqrt{\frac{d^2}{2N_0}}\right)$$

N_0 is the noise density

- Based on that, it is possible to compute a ***bit error rate*** (**BER**) for each modulation
  - Under certain conditions (e.g. gray coding) $BER = P_e / \log_2 M$





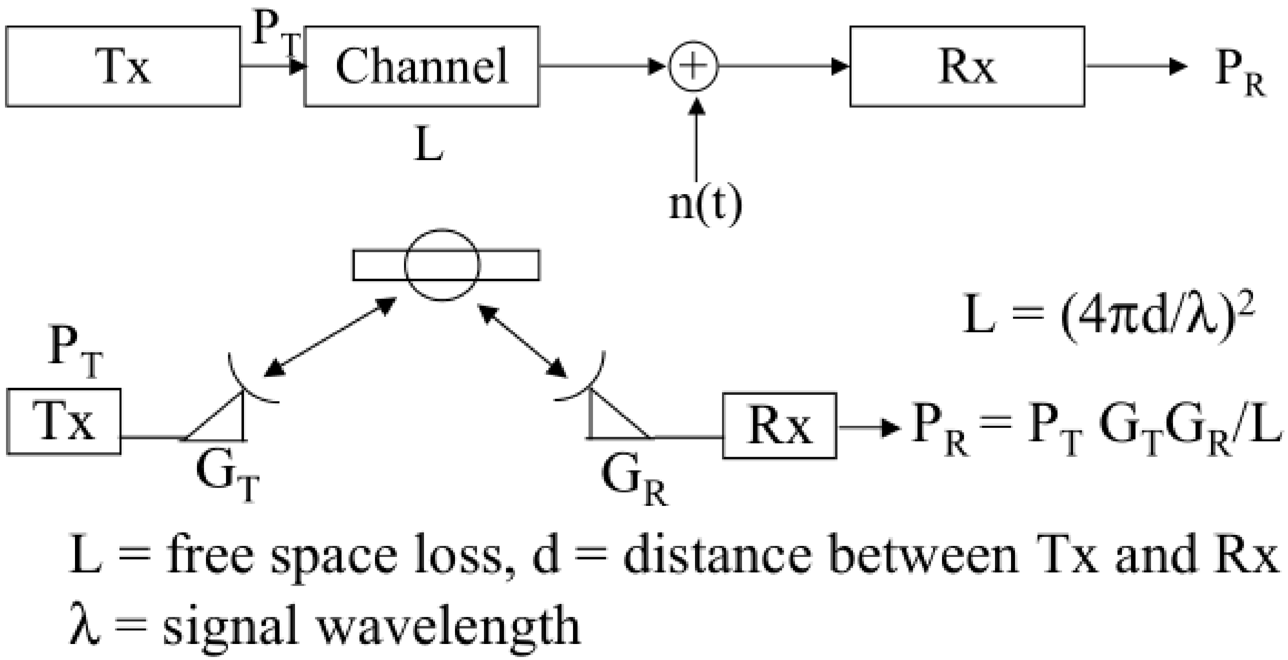
The performance decrease for increasing m

SNR is proportional to the received power

Contents

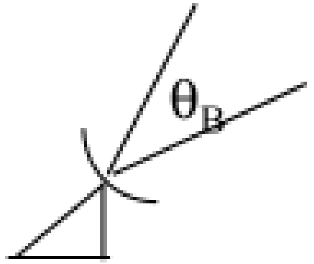
Signal attenuation

- The signal suffers an **attenuation loss** L
  - Received power: $P_R = P_T/L$
  - Received SNR: $SNR = E_b / N_0$, $E_b = P_R/R_b$
- **Antennas** are used to compensate for attenuation loss
  - Capture as much of the signal as possible



Antenna Beamwidth

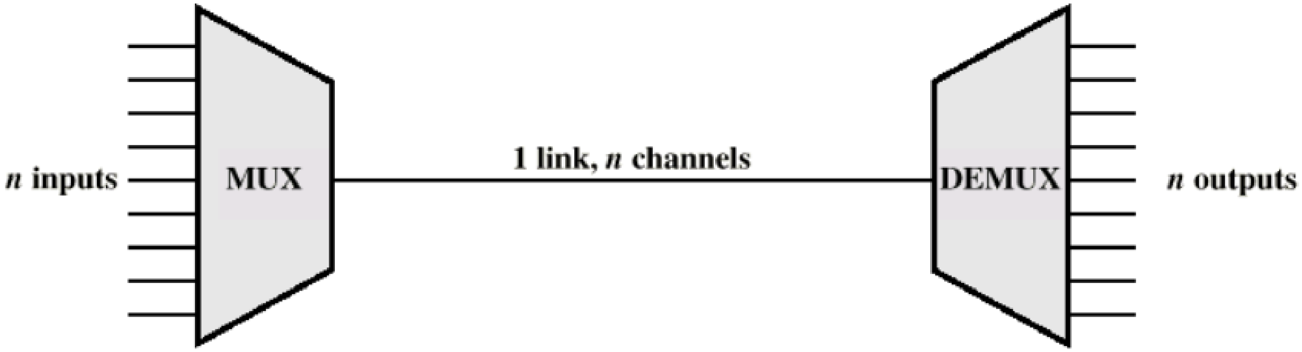
- The ***beamwidth*** θ_B is a measure of the directivity of the antenna
  - A smaller beamwidth concentrates power along a smaller area
- Free space loss assumes that power is radiated in all directions
- An antenna with a smaller beamwidth concentrates the power, hence yields a gain
  - For parabolic antenna, $\theta_B \sim 70\lambda/D$
  - Gain (G_T) is proportional to $1/\theta_B^2$
  - Hence a doubling of the diameter D increases gain by a factor of 4



Contents

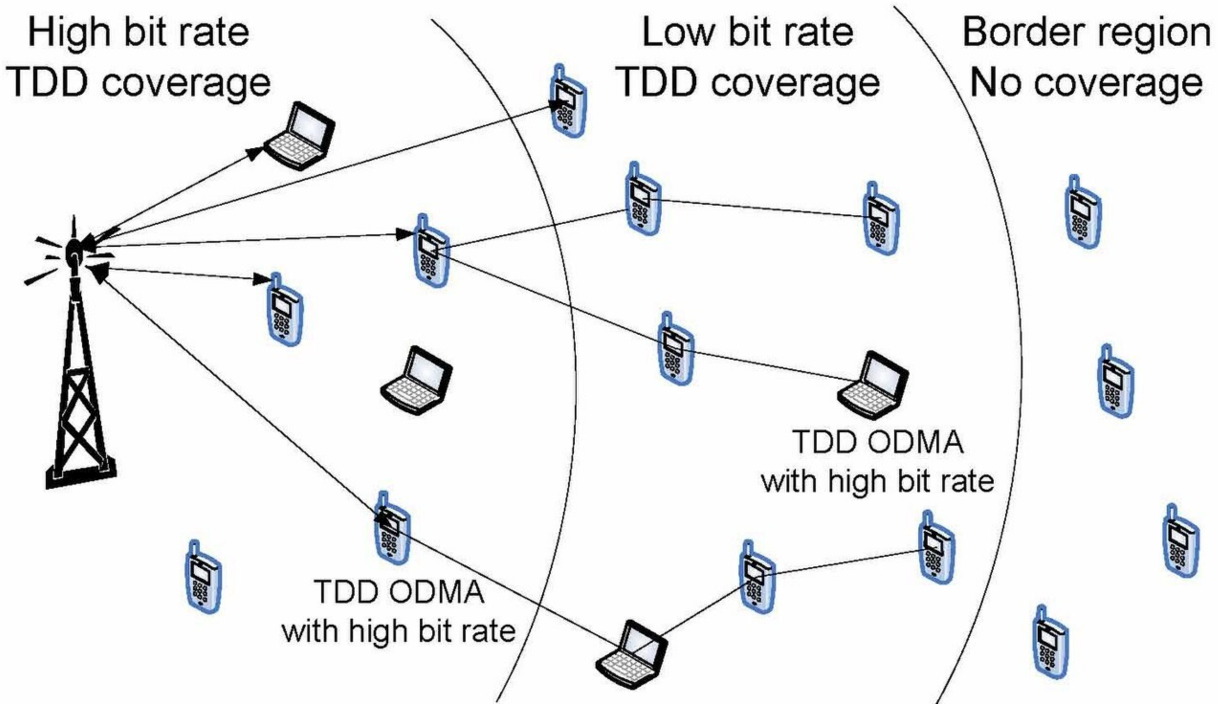
Multiplexing

- *Multiplexing* is a method by which multiple analog or digital signals are **combined into one signal** over a **shared medium**
- The multiplexed signal is transmitted over a communication channel
- The multiplexing divides the capacity of the communication channel into several **logical channels**
  - one for each message signal or data stream to be transferred.
- A reverse process, known as ***demultiplexing***, extracts the original channels on the receiver end.



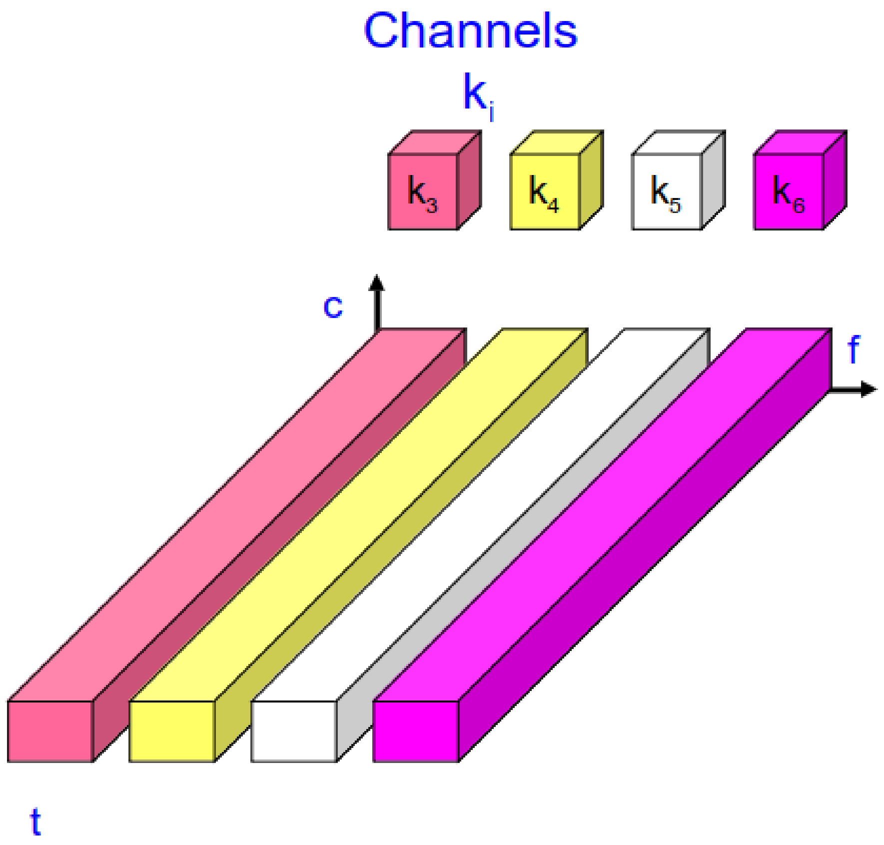
Multiple Access

- *Multiple Access* enables multiple users or devices to share a communication channel simultaneously.
- Multiplexing deals with **combining** signals, while multiple access deals with allowing **multiple users** to access and share a communication medium



Frequency Division Multiplexing /Multiple Access

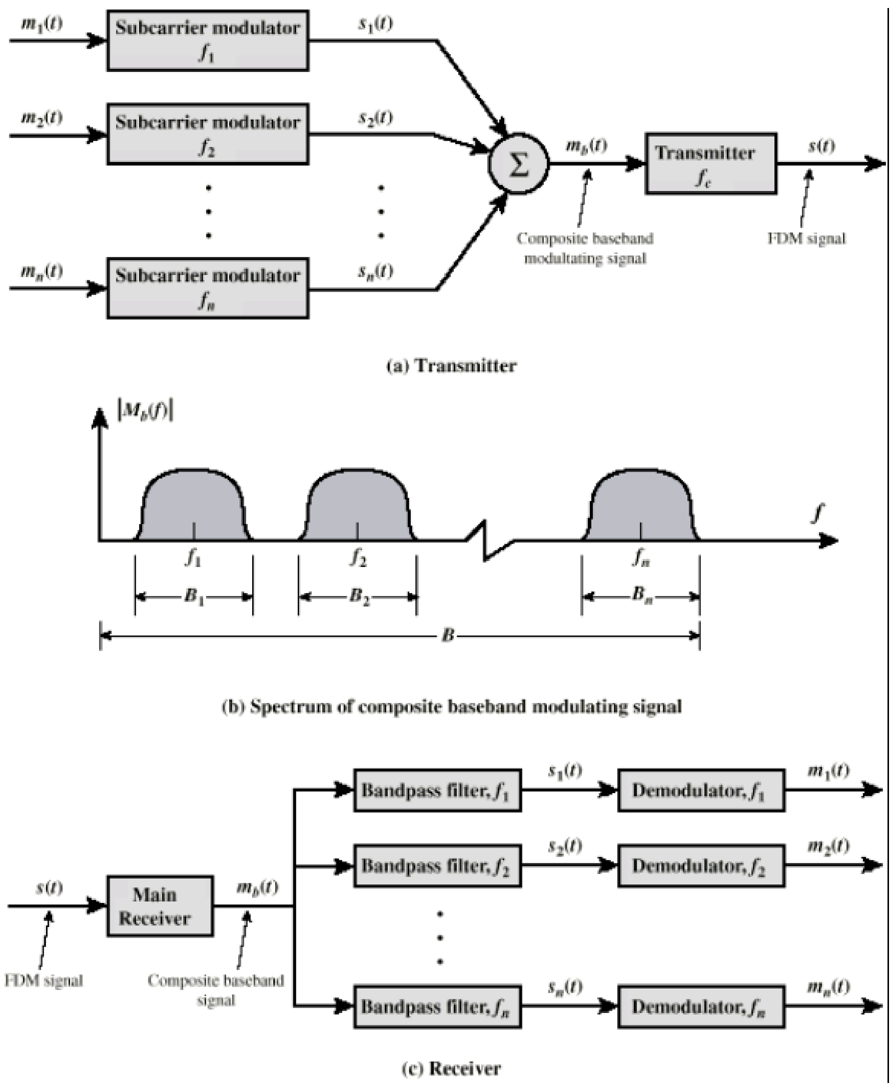
- *Frequency Division Multiplexing / Multiple Access* (FDM/FDMA)
  - Each signal is modulated to a different carrier frequency
  - Useful bandwidth of medium exceeds required bandwidth of channel
  - Carrier frequencies separated so signals do not overlap (guard bands)
  - Channel gets band of the spectrum for the whole time
    - Channel allocated even if no data



FDM/FDMA: Pro and Cons

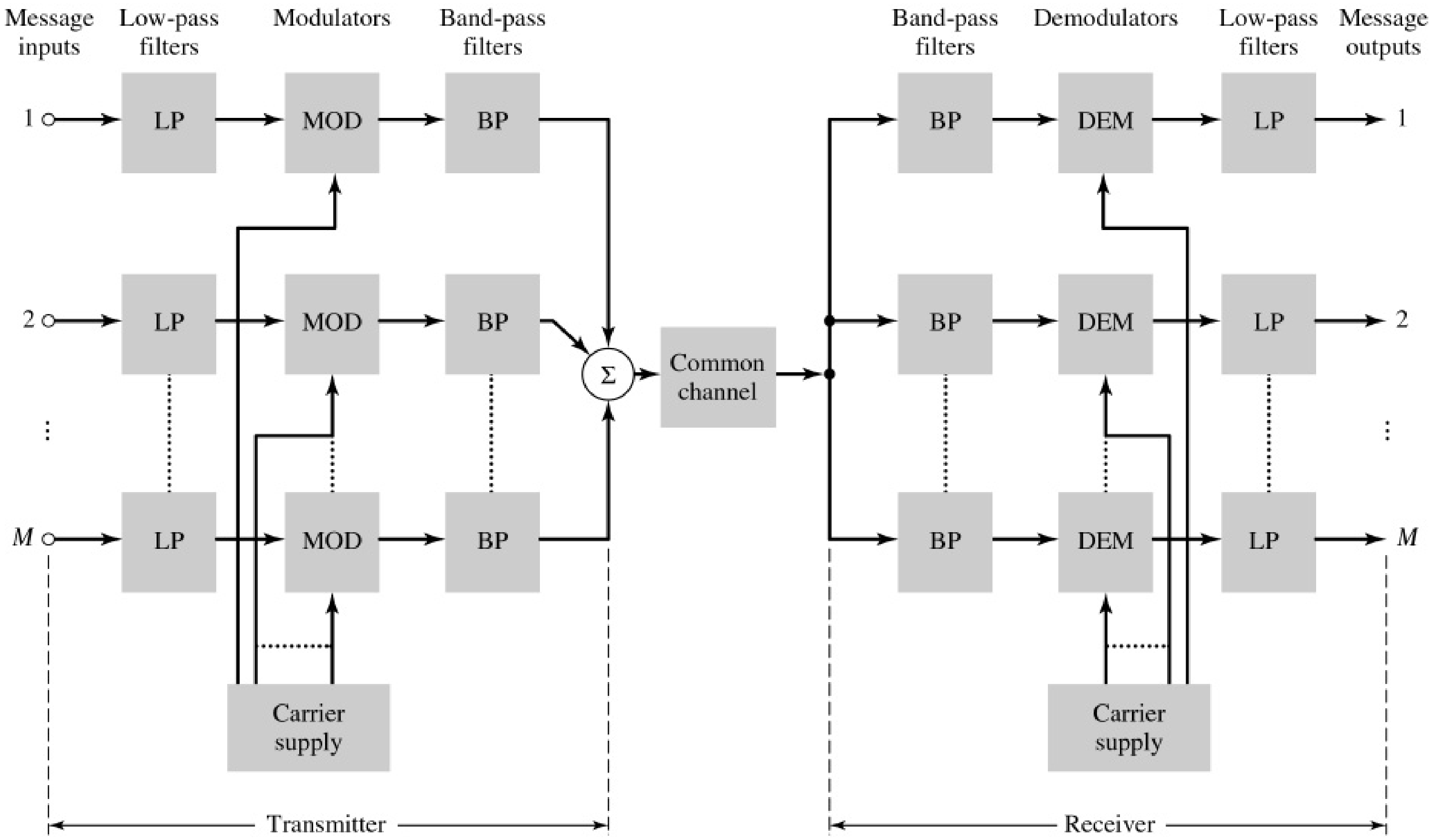
- Advantages:
  - no dynamic coordination needed
  - works also for analog signals
- Disadvantages:
  - waste of bandwidth (fixed allocation) if traffic distributed unevenly
  - guard spaces

- Applications:
  - All wireless systems basically!
  - Radio and tv broadcasting, telephone, communication satellites (uplink and downlink),DSL,…



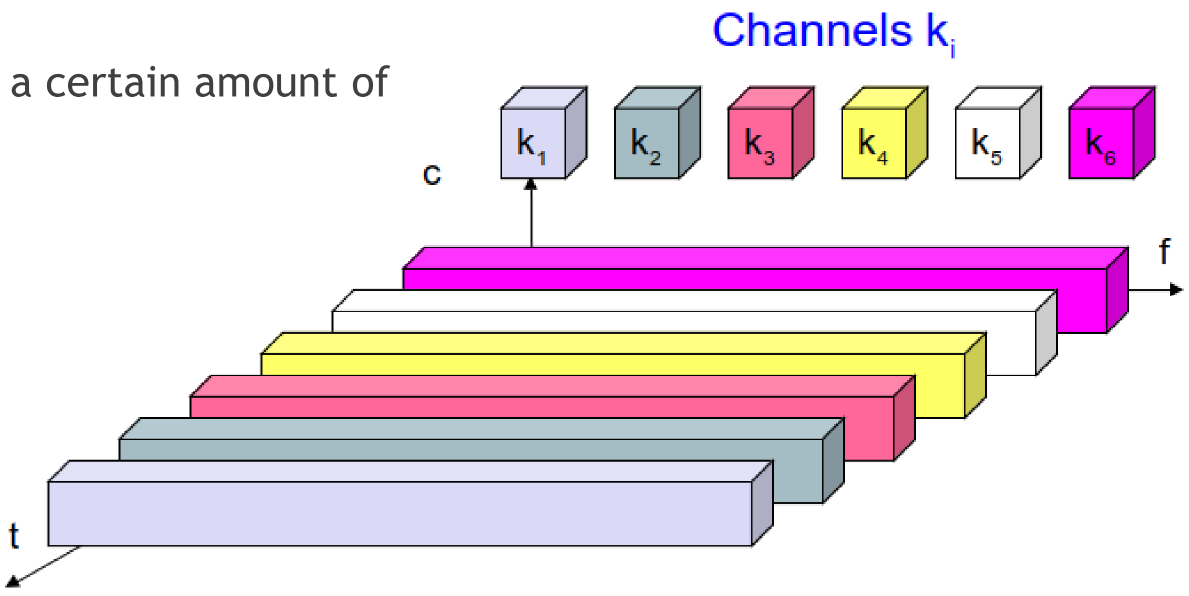
FDM: Scheme

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



Time Division Multiplexing / Multiple Access

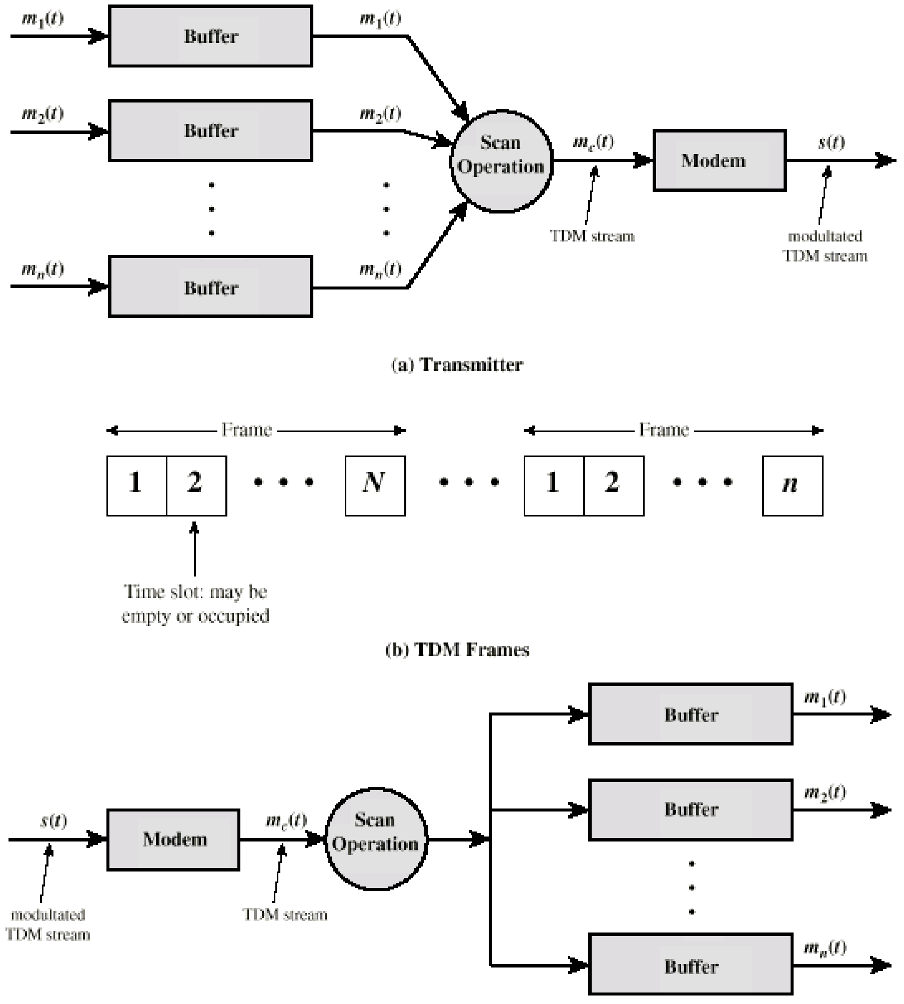
- *Synchronous Time Division Multiplexing / Multiple Access* (TDM/TDMA)
  - Multiple digital signals interleaved in time
  - Time slots preassigned to sources and fixed
    - Time slots allocated even if no data
  - Data rate of medium exceeds data rate of digital signal to be transmitted
  - Channel gets the whole spectrum for a certain amount of time



TDM/TDMA: Pro and Cons

- Advantages:
  - only one carrier in the medium at any time
  - throughput high even for many users
- Disadvantages:
  - precise synchronization necessary

- Applications:
  - Optical networks (SONET), GSM, ISDN,….



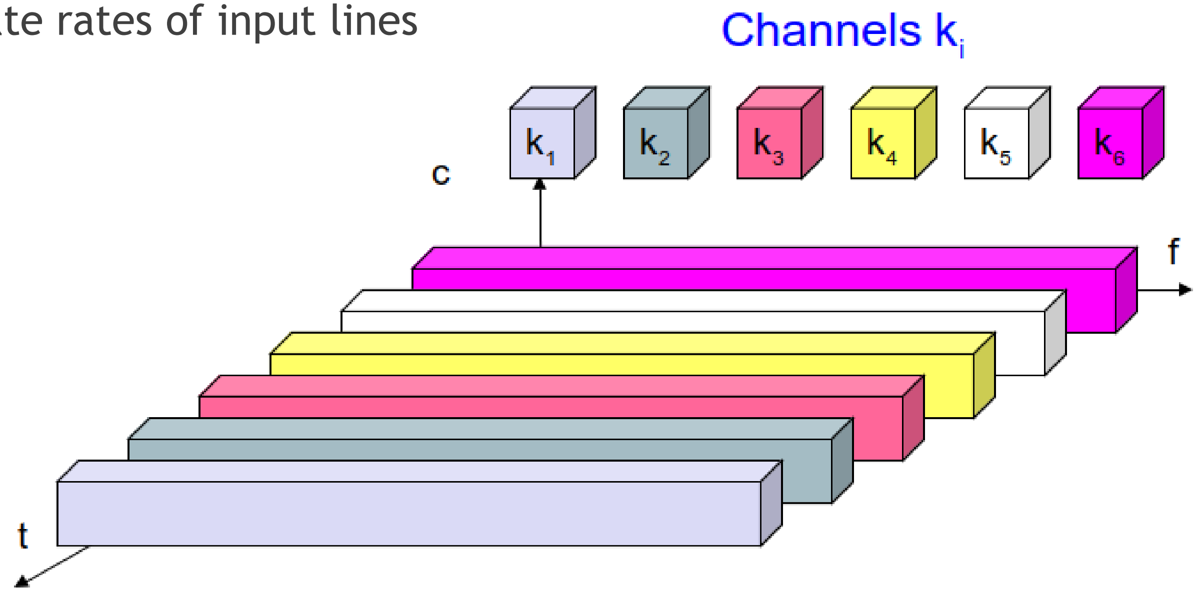
(a) Transmitter

(b) TDM Frames

(c) Receiver

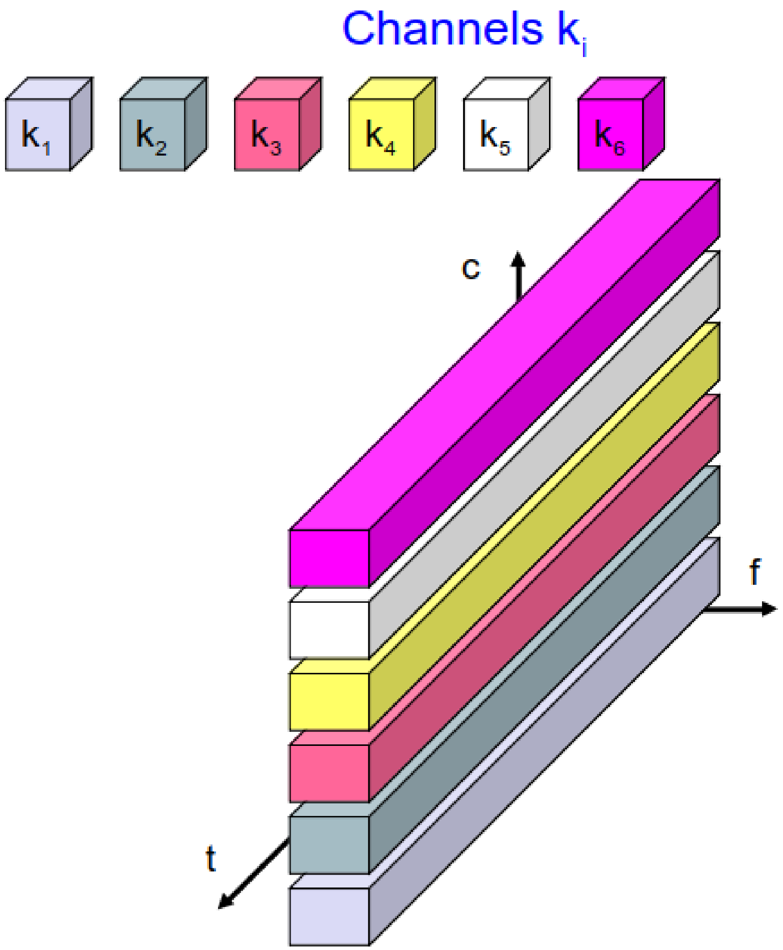
Time Division Multiplexing

- *Statistical Time Division Multiplexing*
  - In Synchronous TDM many slots are wasted
  - Statistical TDM allocates time slots dynamically based on demand
  - Multiplexer scans input lines and collects data until frame full
  - Data rate on line lower than aggregate rates of input lines
  - More advanced technique
    - It requires scheduling algorithms



Code Division Multiplexing / Multiple Access

- *Code Division Multiplexing / Multiple Access (CDM/CDMA)*
  - Each channel has unique code
  - All channels use same spectrum at same time
  - Implemented using spread spectrum technology
    - Each sender is assigned a unique binary code c_i
    - Binary codes are orthogonal vectors
    - This means that they can be summed together and separated without interference
    - MUX: sum signals after code modulation
      - $s_{mux}(t) = s_1(t)c_1 + s_2(t)c_2$
    - DEMUX performs the scalar product to get the desired signal
      - $\langle s_{mux}(t), c_1 \rangle = s_1(t)$



CDM/CDMA: Pro and Cons

- *Advantages*
  - Bandwidth efficient
  - No coordination and synchronization
  - Good protection against interference
- *Disadvantages*
  - lower user data rates
  - more complex signal regeneration

- Applications:
  - UMTS (3G), Global Navigation Satellite Systems (GPS),…

Example: GPS signal

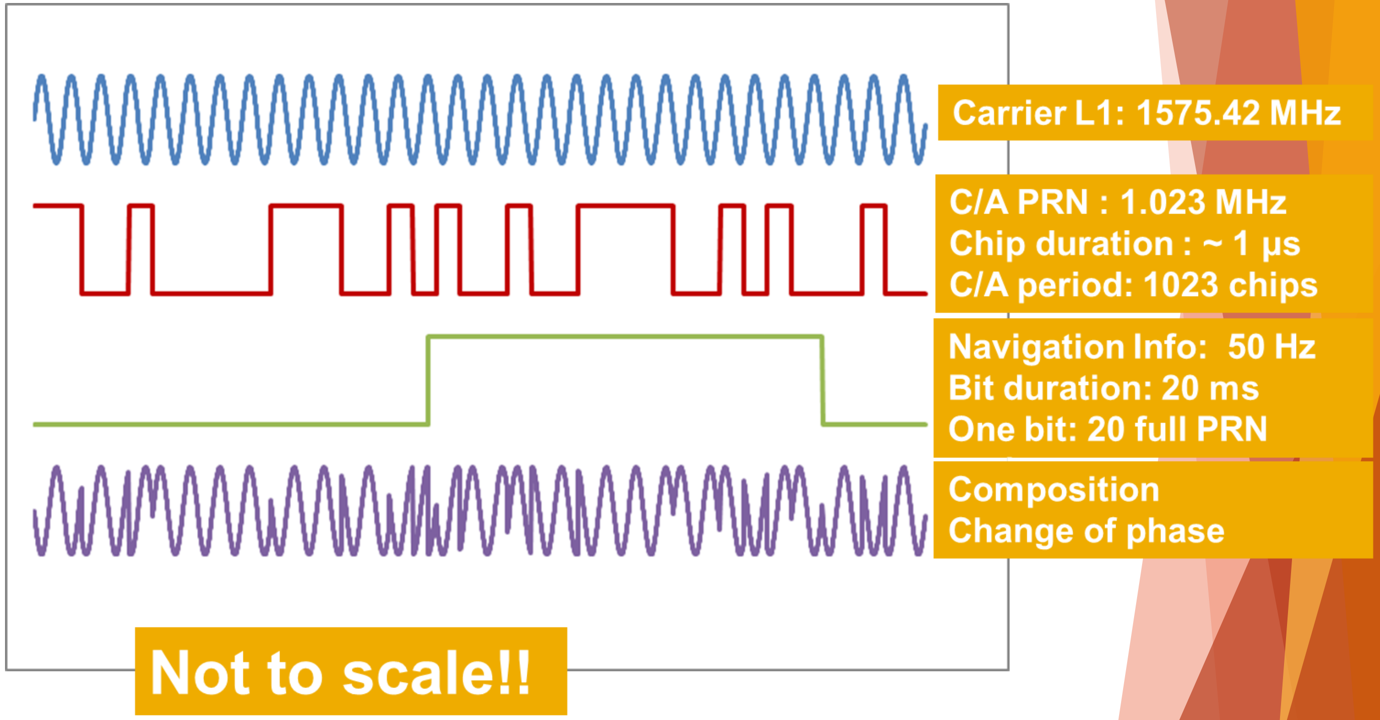
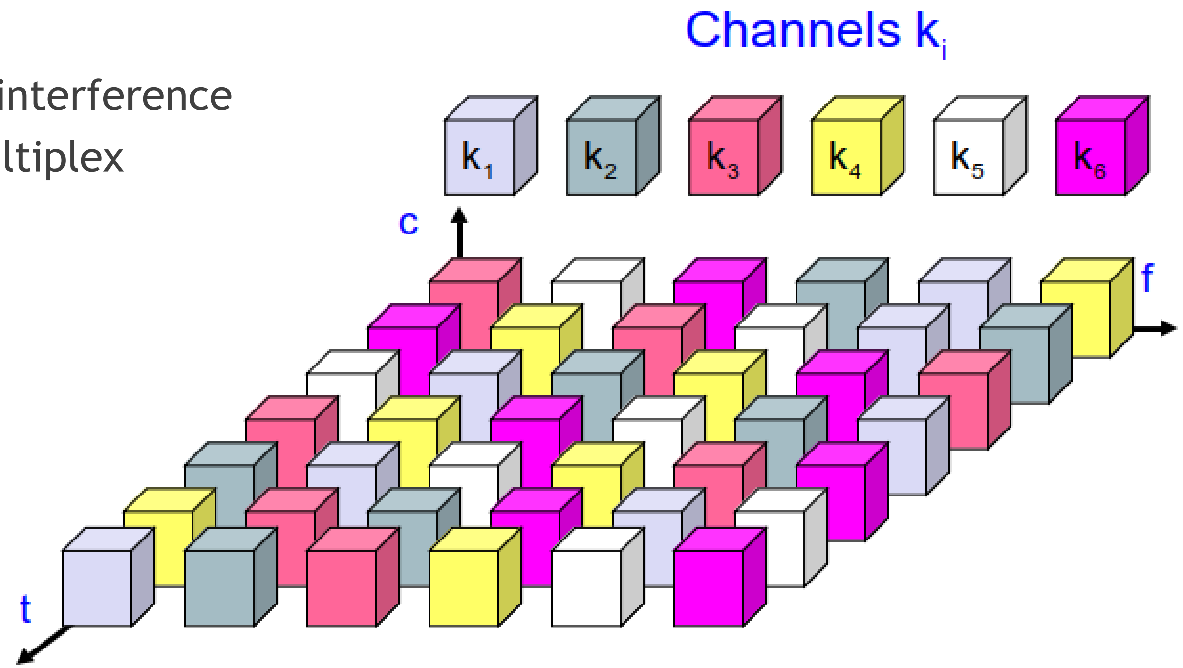


Figure: "GPS signals" by José Caro Ramón is licensed under CC BY-SA 3.0

TDM/A + FDM/A

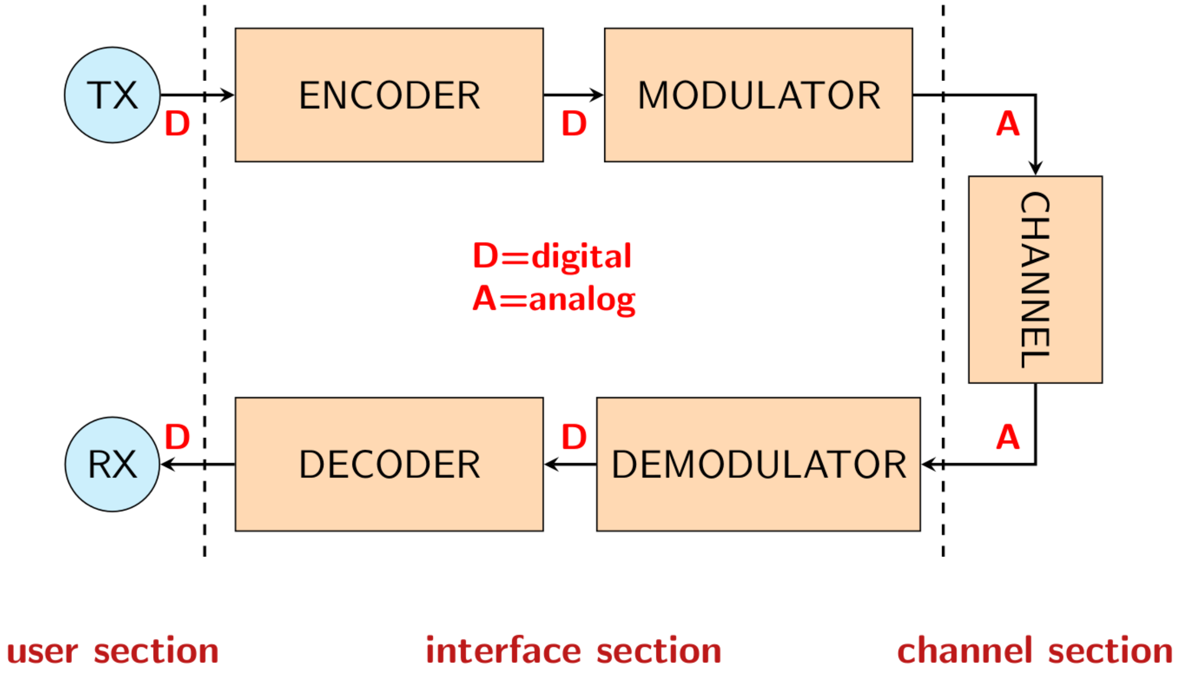
- *Time and Frequency Division Multiplexing*
  - A channel gets a certain frequency band for a certain amount of time (e.g. GSM)
- *Advantages:*
  - better protection against tapping
  - protection against frequency selective interference
  - higher data rates compared to code multiplex
  - Precise coordination required



Contents

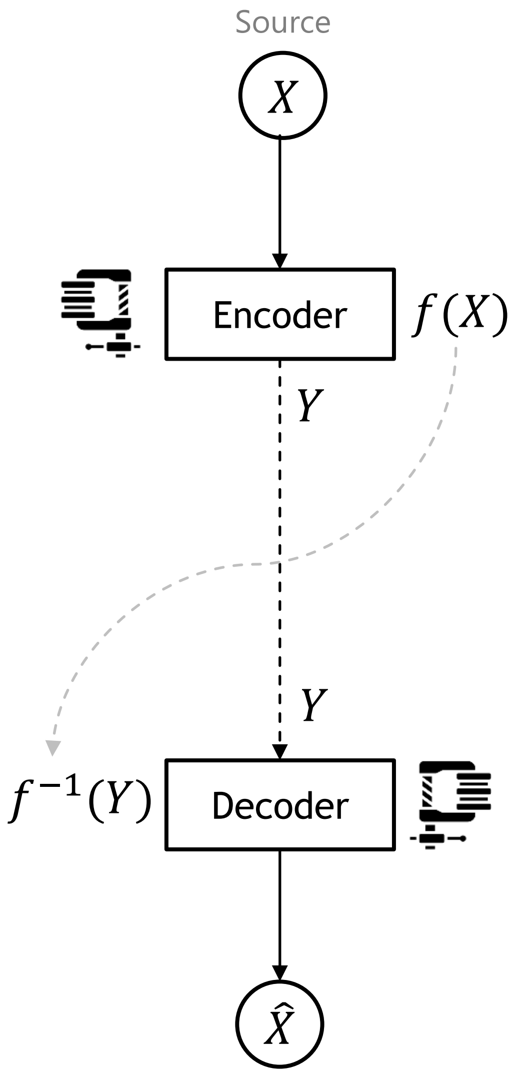
Digital Comm. System: Encoder/Decoder

- *Encoder*
  - Implements **source encoding** to limit the amount of transmitted data
  - Implements **channel encoding** to limit the effects of channel disturbances
- *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



Encoding/Decoding

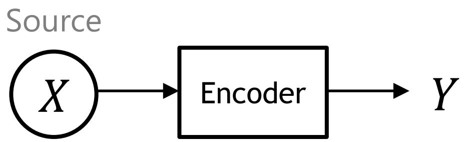
- *Encoding*
  - It aims to generate a compressed representation Y, starting from the input data X.
- *Decoding*
  - It aims to reconstruct the input data, generating a version $\hat{X}$ starting from the compressed sequence Y



Source Coding

- ***Source coding***, also known as data **compression**, aims to represent information or data in a more compact form to reduce redundancy and **save storage** space or **transmission bandwidth**
- The primary goal is to eliminate or **minimize redundancy** in the data, as many real-world datasets exhibit patterns or **repetitions** that can be efficiently encoded
  - E.g. Variable-length coding assigns shorter codes to more frequent symbols and longer codes to less frequent symbols. This reduces the average number of bits needed to represent the data.

Symbol	Frequency	Variable length Code	Fixed length Code
A	6	0	00
B	3	10	01
C	2	110	10
D	1	111	11



AAAABBBCCDAA

000010101011011011100 **Variable Length**

000000000101011010110000 **Fixed Length**

Compression Types

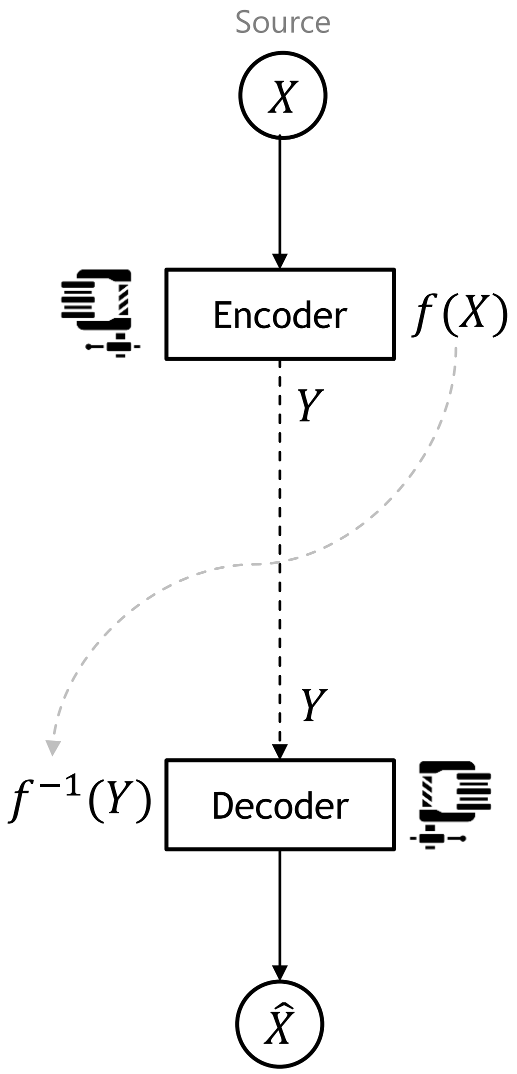
Compression classes for source encoding

Loseless

- Ensures that the original data can be perfectly reconstructed from the compressed version. Examples include ZIP and PNG.
- $\hat{X} = X$

Lossy

- Sacrifices some data accuracy for higher compression ratios. Commonly used in multimedia compression, as in JPEG and MP3
- $\hat{X} \approx X$



- There are no universal compression formats. The fidelity requirements ($\hat{X} \approx X$) of the application and the nature of the data define the specifications
  - Reducing the size of transmitted data preserving the **perceived information**
- Trade-off: compression efficiency vs. computational complexity
  - Advanced algorithms may provide higher compression but require more processing power

Source Encoding: Examples

Source coding aim at efficiently **reducing the size of transmitted data** preserving the perceived information

Data

- Text Files
- Digitalized Signals
- Scientific data
- Telemetry data
- Measurements
- IP frames

Audio/Speech

- Phone calls (realtime)
- Music Tracks
- Recorded Tracks
- Environmental sounds

Static Images

- Stored pictures
- Scientific figures
- Camera captures

Video

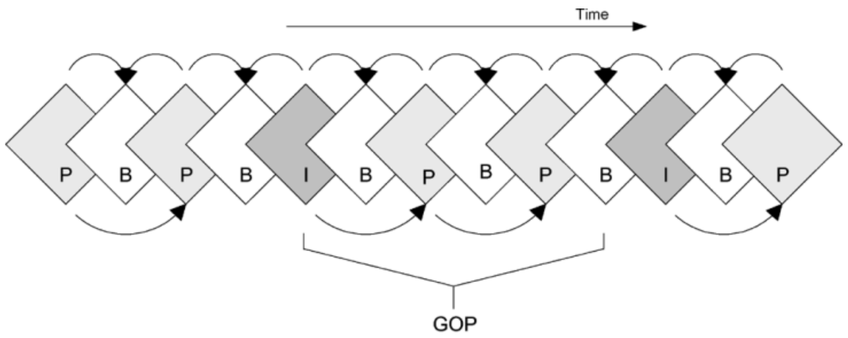
- TV contents
- Surveys
- Surveillance

Perceptual Compression

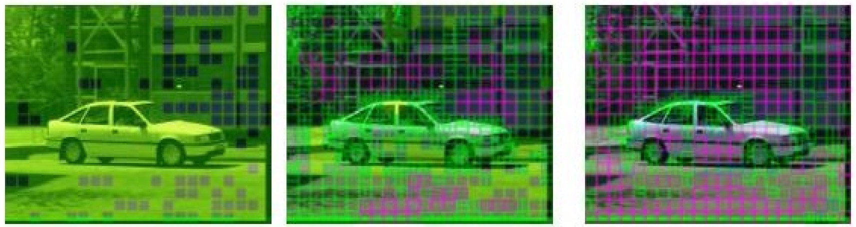
Source Encoding: Examples

Differential Video Encoding

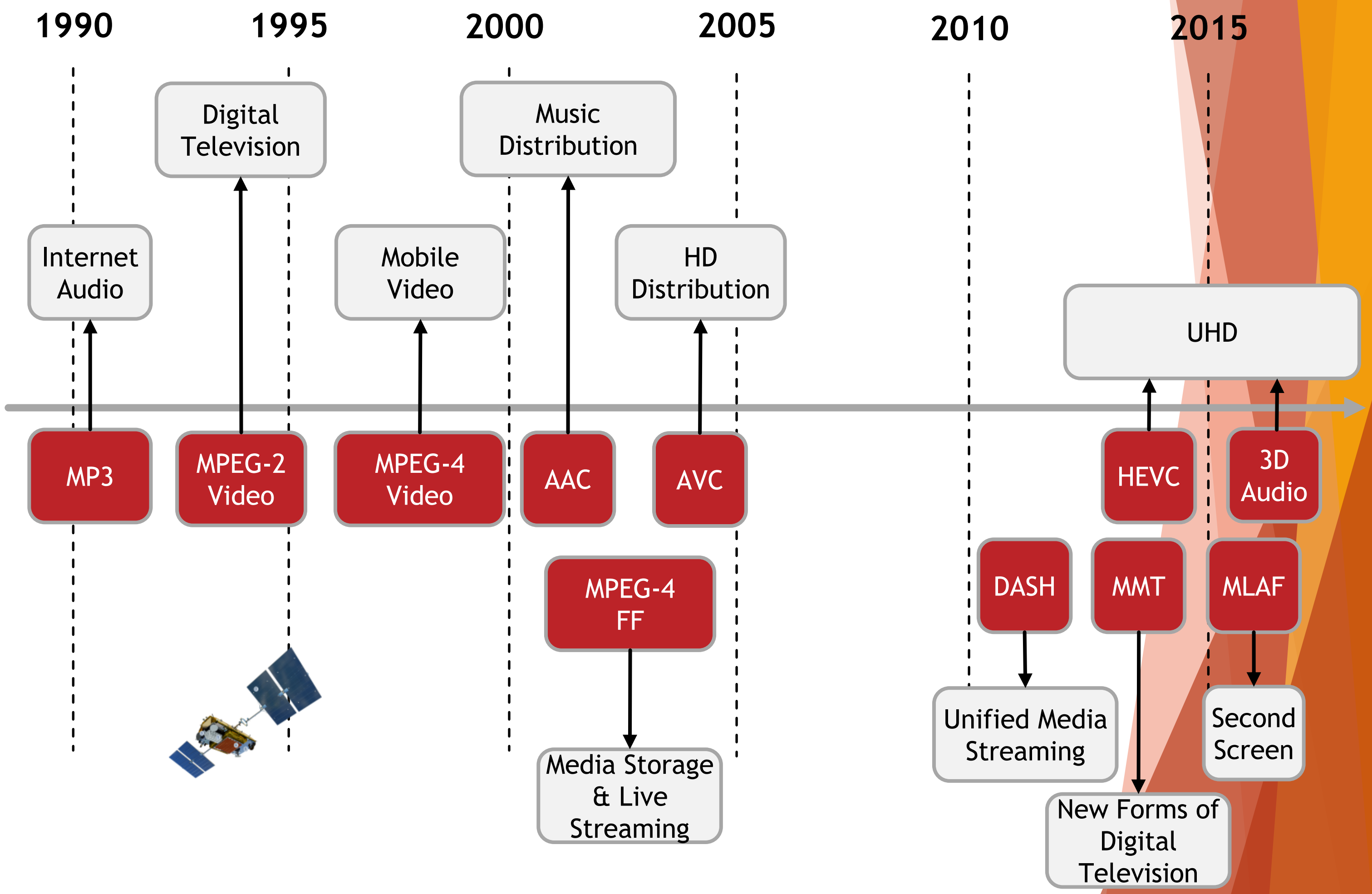
Video compression takes advantage of static image compression and frame time redundancy



Conventional MPEG GOP structure

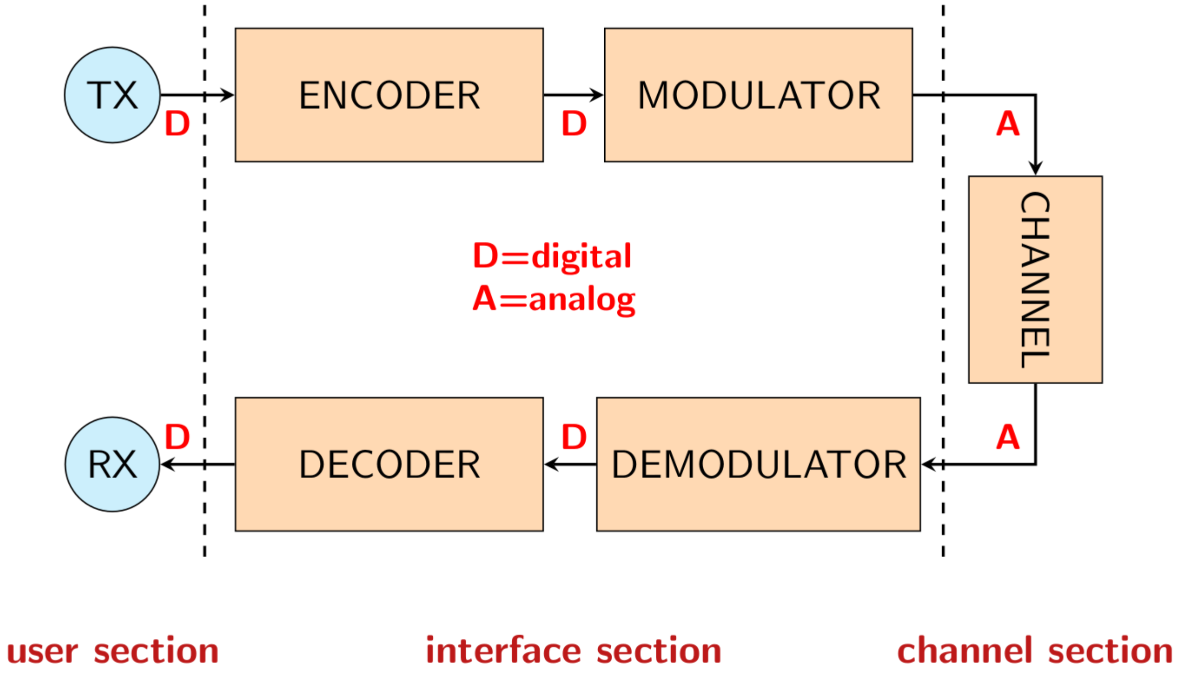


Intraframe (I), predicted frame (P) and bi-directionally predicted (B) frame



Digital Comm. System: Encoder/Decoder

- *Encoder*
  - Implements **source encoding** to limit the amount of transmitted data
  - Implements **channel encoding** to limit the effects of channel disturbances
- *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



Error Detection and Correction

- After **source coding**, bits should be received **unaltered**
- Goal: reliable delivery of digital data over unreliable communication channels
- *Error detection* techniques allow detecting such errors, while *error correction* enables reconstruction of the original data
- All error-detection and correction schemes add some ***redundancy*** (i.e., some extra data) to a message, which receivers can use to check consistency of the delivered message and to recover corrupted data

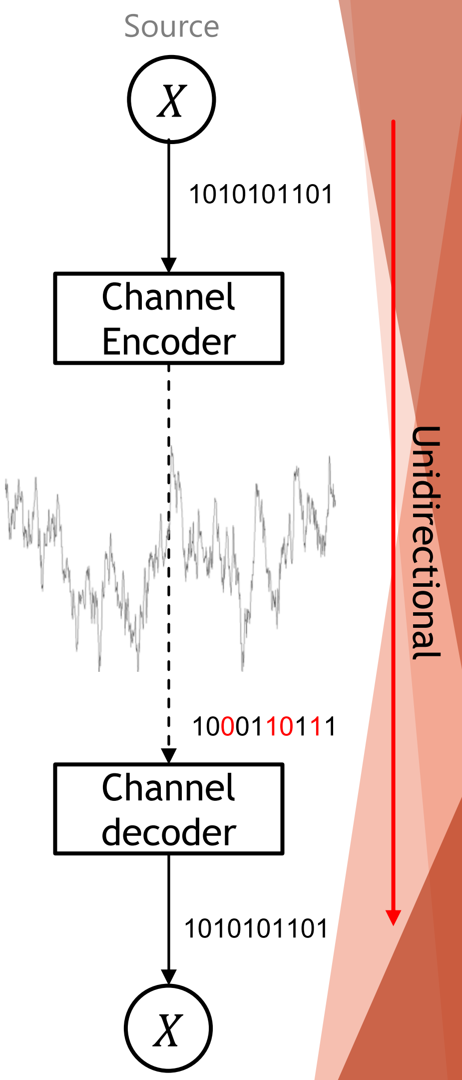
APPROACHES

Automatic repeat request (ARQ)

- It uses **acknowledgements** (messages sent by the receiver indicating that it has correctly received a message) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission
- Protocol perspective, needs a backward channel
- Examples: Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ

Forward error correction (FEC) / Channel coding

- It is a process of adding **redundant** data to a message so that it can be recovered by a receiver even when some errors (up to the capability of the code being used) are introduced
- No need for a backward channel, unidirectional communication
- Examples: Block codes, convolutional codes



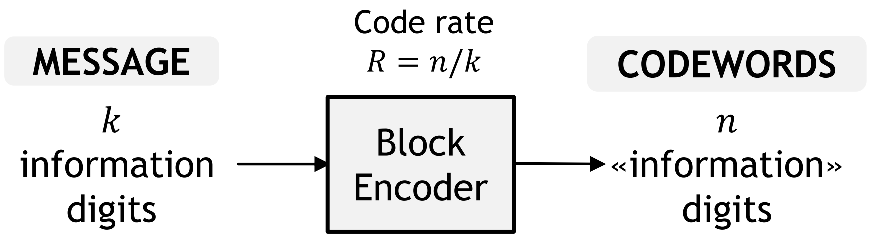
Channel Coding

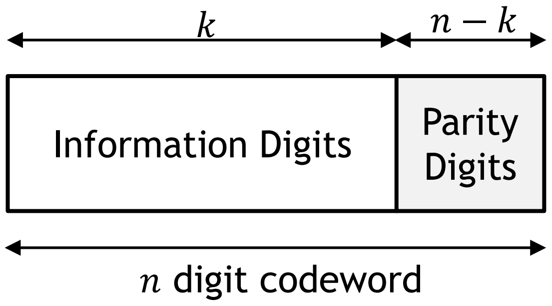
- ***Channel coding*** aims to detect and correct errors that may occur during transmission
  - It adds redundant bits to the original message, creating a coded message that contains extra information for error detection and correction
  - Used in various communication systems, including wireless communication, satellite communication, digital television, and data storage
- The effectiveness of a channel code is often measured by its **error correction capability**, indicating the maximum number of errors that can be corrected within a codeword.
- There is a **trade-off** between the amount of redundancy added (which affects bandwidth efficiency) and the level of error correction provided.

- **Block Codes:** Divide the data into fixed-size blocks, and error correction is performed independently on each block.
- **Convolutional Codes:** Process the data as a continuous stream, on a bit-by-bit basis, and error correction is based on the convolution of the input data with a code. Optimally decoded through Viterbi Algorithm.

Block Codes

- A block code acts on block of k bits of input data to produce n bits of output data (n, k)





Linear Block Codes

- Reed–Solomon
- Hamming
- Hadamard
- Expander
- Golay codes
- Reed–Muller

- A simple example: *Repetition code*
  - Each bit is repeated 3-times.
  - Each codeword of $n = 3$ digits is decoded to the most common bit in it