Faculty of Electrical Engineering and Communication
BRNO UNIVERSITY OF TECHNOLOGY

COMMUNICATION SYSTEMS

prof. Ing. Aleš Prokeš, Ph.D.

Vytvořeno za podpory Studium moderní a rozvíjející se techniky VUT (SMART VUT) CZ.02.2.69/0.0/0.0/18_056/0013325.

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

References

[1] SKLAR, B. Digital Communications: Fundamentals and Applications. Prentice Hall, 2009.

[2] COUCH, L. W. Digital and Analog Communication Systems. Prentice Hall, 2000.

[3] DESURVIE, E. Wiley Survival Guide in Global Telecommunications: Signaling Principles, Protocols, and Wireless Systems. John Willey & Sons, 2004.

[4] DESURVIE, E. Wiley Survival Guide in Global Telecommunications: Broadband Access, Optical Components and Networks, and Cryptography. John Willey & Sons, 2004.

[5] GARCIA, L. Communications Networks Fundamental Concepts and Key Architectures. McGraw Hill 2004.

Content

1. History
2. Digital communication system architecture
3. Formatting and source coding
4. Cryptography
5. Channel coding
6. Pulse modulation
7. Band-pass modulation
8. Multiple access
9. Wireless interface
10. Synchronization
11. Wired communication systems
12. Wireless communication systems
13. Computer networks

1. HISTORY

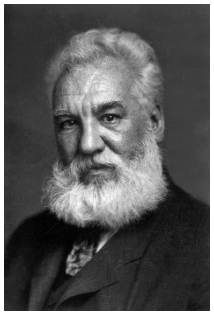
3000BC	Picture language (hieroglyphic), Egypt
800	Arabic number system (adopted from India)
1440	Movable metal type, (letterprint), *Johanes Guttenberg*
1752	Demonstration that lightning is electricity, *Benjamin Franklin*
1827	Ohm law formulation, *Georg Simon Ohm*
1834	Building of telegraph, *William F. Cooke and Sir Charles Wheatstone*
1842	Connection over 65 km using *Morse* telegraph
1850	Kirchhoff circuit laws, *Gustav Robert Kirchhoff*
1858	Transatlantic cable laying (failed after 26 days)
1864	Prediction electromagnetic radiation, *James C. Maxwell*
1876	Development and patenting of the telephone, *A. Graham Bell*
1883	Discovery of a flow of electrons in a vacuum, *Thomas A. Edison*
1901	Wireless signal transmission across Atlantic (3500 km), *Guglielmo Marconi*
1904	Invention of the thermionic two-electrode valve (diode), John A. Fleming
1906	Invention of the vacuum-tube (triode) amplifier, *Lee De Forest*
1915	U.S. transcontinental telephone line completion, *Bell System*
1918	Super-heterodyne receiver circuit, *Edwin H. Armstrong*
1920	First scheduled radio broadcasts in Pittsburg (U.S.)
1926	Demonstration of television, *J. L. Baird and C. F. Jenkins*
1927	Negative-feedback amplifier, *Harold Black*

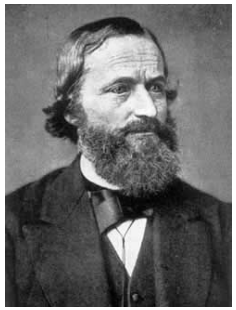
1. HISTORY

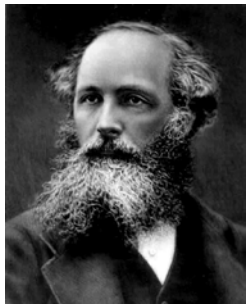
1933	Invention of frequency modulation (FM), *Edwin H. Armstrong*
1935	First practical radar design, *Robert A. Watson-Watt*
1938	First television broadcast, *British Broadcasting Corporation (BBC)*
1940s	Using the spread spectrum technique for military anti-jam applications
1946	First mobile telephone service, *St. Louis, U.S., AT&T*
1947	Invention of transistor, *W. H. Brattain, J. Bardem, and W. B. Shockley*
1948	Publication of information theory, *Claude Elwood Shannon*
1950	Application of Time-division multiplexing (TDM) to telephony
1950	Development of Microwave telephone and communication links
1953	Introduction of NTSC color television, United States
1953	Lay of the first transatlantic telephone cable (36 voice channels)
1957	Launch of the fist Earth satellite, *Sputnik* (USSR)
1958	Publication of the laser principles, *A. L. Schawlow, C.H. Townes*
1958	Production of the first silicon IC, *Robert Noyce (Fairchild)*
1961	Stereo FM broadcasting, United States
1962	The first active satellite relaying TV signals between the U. S. and Europe
1963	Use of error-correction codes and adaptive equalization for HS comm
1965	Launch of the first commercial communications satellite, *Early Bird*
1968	Development of cable television systems

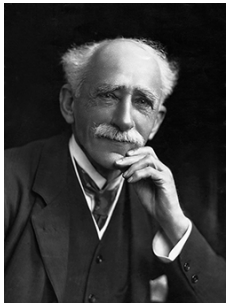
1. HISTORY

1971 Fist single-chip microprocessor, *Intel*
1972 Demonstration of cellular telephone, *Motorola*
1976 Development of personal computer
1980 Development of the FT3 fiber-optic communication system
1981 Nordic Mobile Telephone (NMT) 450
1989 Global positioning system (GPS)
1991 Global System for Mobile Communication (GSM)
2000 IMT2000 (International Mobile Telecommunication 2000)
2001 First commercial Universal Mobile Telecomm. System (UMTS), *Telenor*
2001 First commercial WCDMA 3G mobile network, *NTT DoCoMo*
2002 First GSM/EDGE 3G mobile phone, *Nokia*
2005 Demonstration of 9 Mbps with WCDMA, HSDPA phase 2, *Ericsson*
2009 First publicly available LTE (4G) service, *TeliaSonera Stockholm*

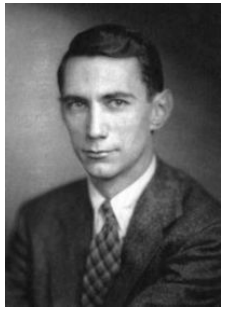

G. S. Ohm


G. R. Kirchhoff


J. C. Maxwell


J. A. Fleming


W. B. Shockley


C. E. Shannon


R. Noyce

2. DIGITAL COMMUNICATION SYSTEM ARCHITECTURE

2.1 Classification of communication systems

- Analog vs digital
- Bi-directional vs Single-directional (duplex vs. simplex)
- Fixed vs mobile
- Cellular vs other
- Public vs private

Definitions:

An analog information source produces messages that are defined on a continuum (microphone, thermometer, …).

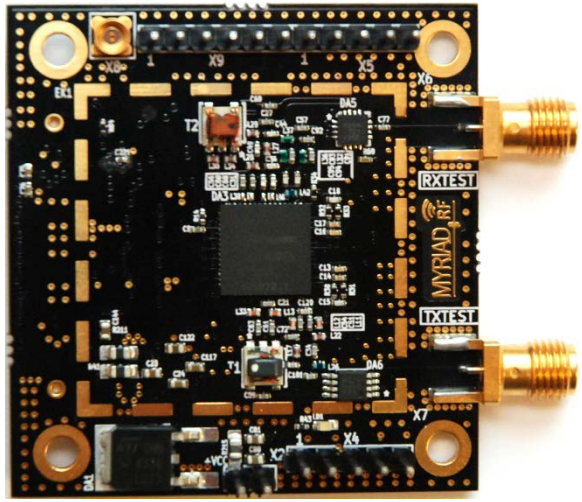
A digital information source produces a finite set of possible messages (typewriter, teleprinter, telegraph…).

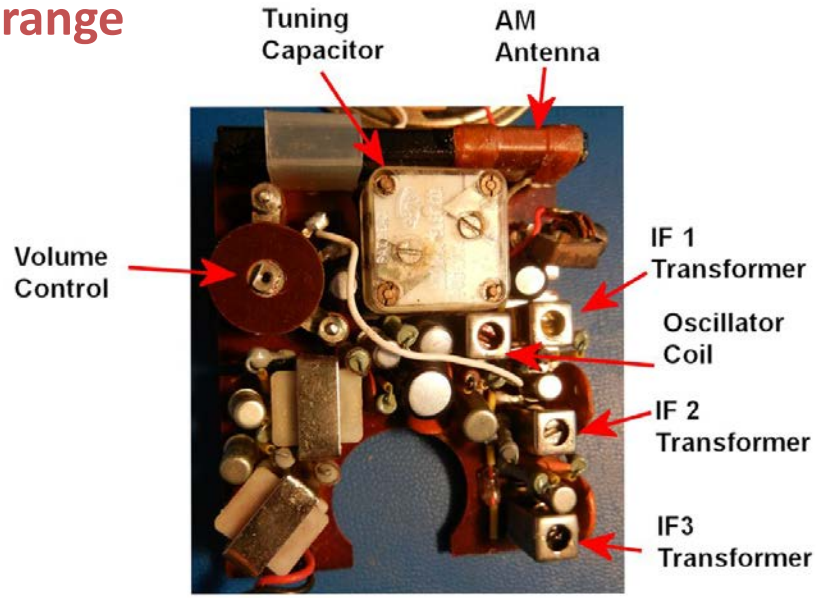
Digital communication system transfers an information from a digital information source to an end user.

Analog communication system transfers an information from an analog information source to an end user.

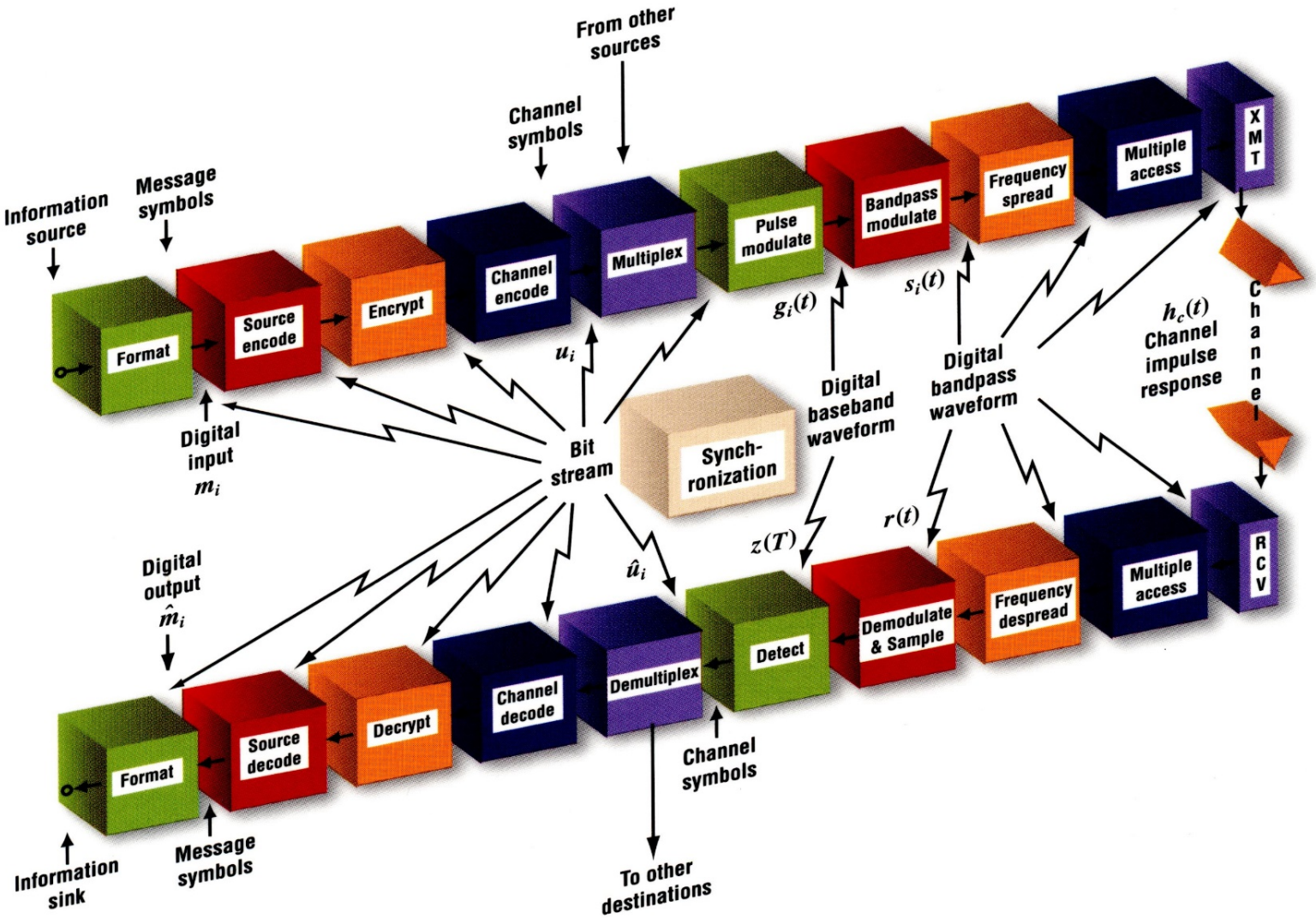
2.2 Digital communication system yes or not?

+ Relatively cheap electronic circuits
+ Confidentiality of information using cryptography
+ Large dynamic range
+ Multiplexing of data from different sources
+ Easy data signal regeneration
+ Possible fading suppression and data error correction
+ Flexible implementation
- Necessity of synchronization
- Nongraceful degradation
- Requirement of a wide frequency range





2.3 Digital communication system architecture



2.3 Digital communication system architecture

Transmitter branch

- ✓ **Format**: sampling followed by uniform or non-uniform quantization, pulse code modulation (PCM), character coding.
- ✓ **Source encode**: speech, audio, video and data coding. Lossy compression (MPEG, JPEG), loss-less compression (Huffman code, LZH, ARJ, …).
- ✓ **Encrypt**: data protection against an abuse. Asymmetric and symmetric cryptography. Block and data stream encryption (ciphering).
- ✓ **Channel encode**: data error protection. Error detection and correction codes. Block, convolutional, and turbo codes.
- ✓ **Multiplex**: multiplexing of data streams from a few sources.
- ✓ **Pulse modulate**: PCM waveforms (line codes), non-return-to-zero (NRZ), RZ. Equalization, filtering for inter-symbol interference (ISI) suppression.
- ✓ **Band-pass modulate**: baseband to pass-band signal transformation using carrier wave. Coherent and non-coherent modulation. Phase shift keying (PSK), frequency shift keying (FSK), amplitude shift keying (ASK), continuous phase modulation (CPM), etc.

2.3 Digital communication system architecture

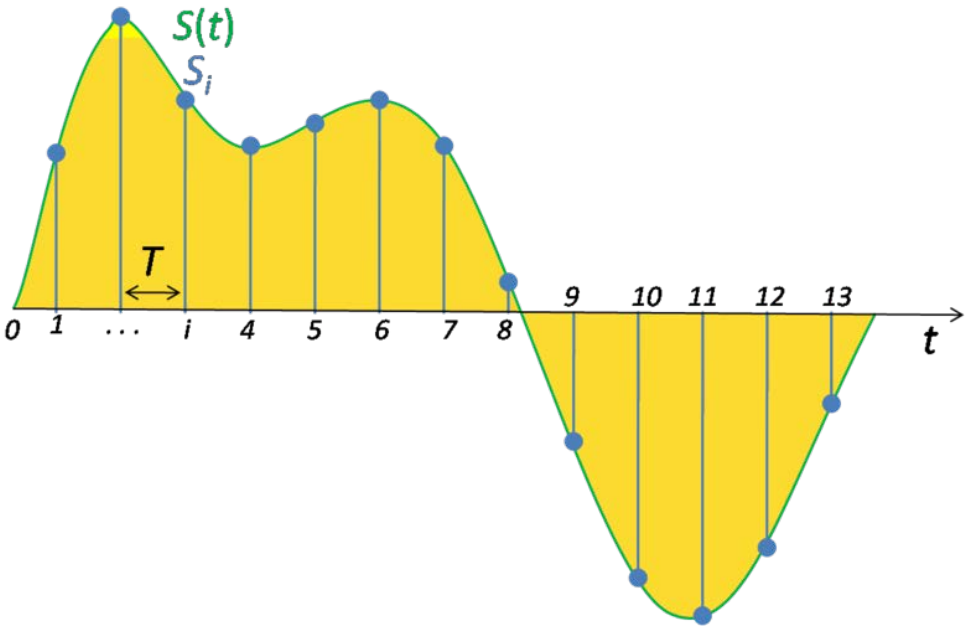
- ✓ **Frequency spread: frequency band spreading for fading elimination, data security,…). Direct sequencing (DS), frequency hopping (FH), time hopping (TH).**
- ✓ **Multiple access: channel allocation to individual users. Frequency division multiplexing (FDM/FDMA), time division (TDM/TDMA), code division (CDM/CDMA), space division (SDMA), polarization division (PDMA). …**
- ✓ **XMT: transmitter. Power amplification of a RF signal and filtering.**
- ✓ **Synchronization: carrier recovery, symbol and bit timing recovery, frame timing recovery, …**
- ✓ **Channel: time delay, phase shift, time dispersion, interference, attenuation. …**
- ✓ **RCV: receiver. Low noise amplification of RF signal and filtering. …**

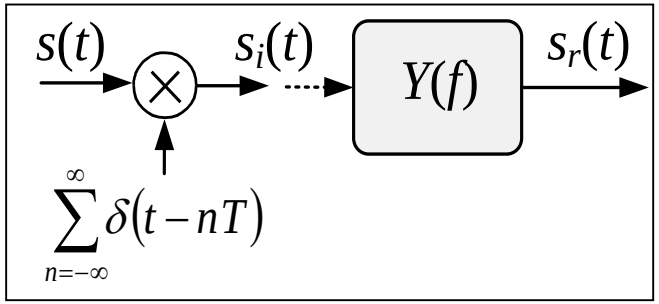
Receiver branch - inverse operations

- ✓ **Demodulate & sample: signal conversion to baseband, equalization and sampling at the appropriate times given by the synchronization circuit.**
- ✓ **Detect: detection of symbols corrupted by a noise and by an interference depending on the modulation type.**
- ✓ **… … inverse operations … …**

3. FORMATTING AND SOURCE CODING
3.1 Sampling

Sampling: conversion of a continuous signal to a discrete signal.
Impulse sampling: multiplying the signal with series of *Dirac* pulses.



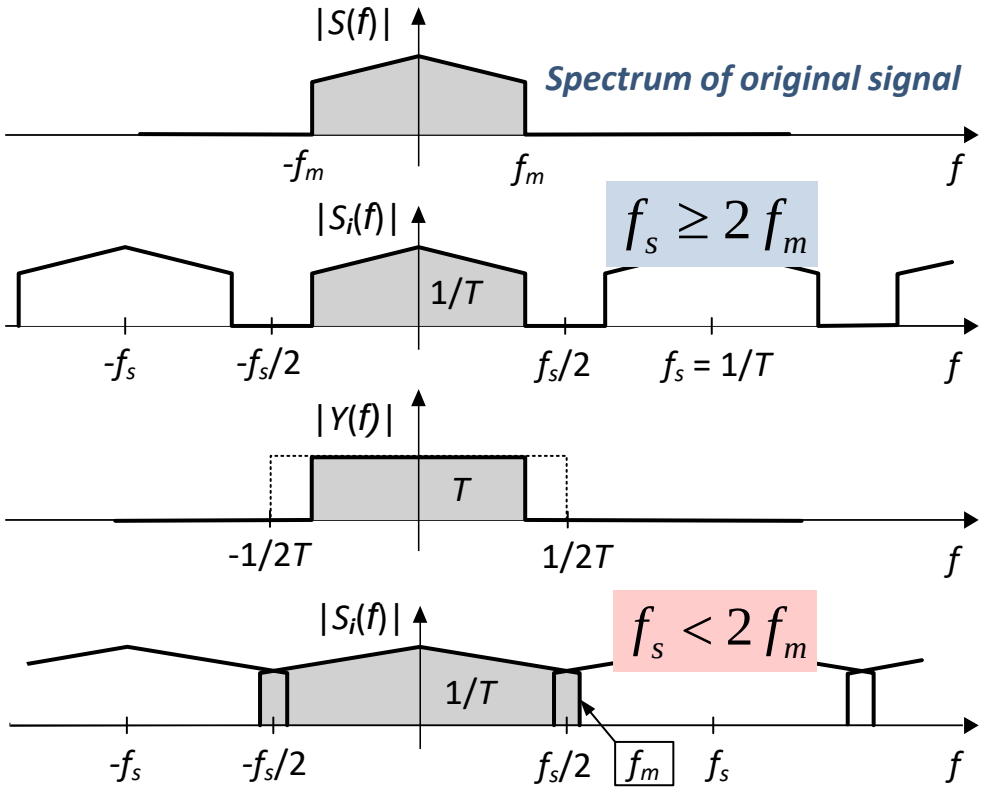


$$s_r(t) = s(t)\underbrace{\sum_{n=-\infty}^{\infty}\delta(t-nT)}_{sampler} * y(t)$$

T: sampling period, $f_s = 1/T$: sampling frequency

3.1 Sampling

Spectrum of sampled signal



Spectrum of sampled signal

$$S_i(f) = \frac{1}{T}\sum_{k=-\infty}^{\infty} S[2\pi(f - kf_s)]$$

Reconstruction function:

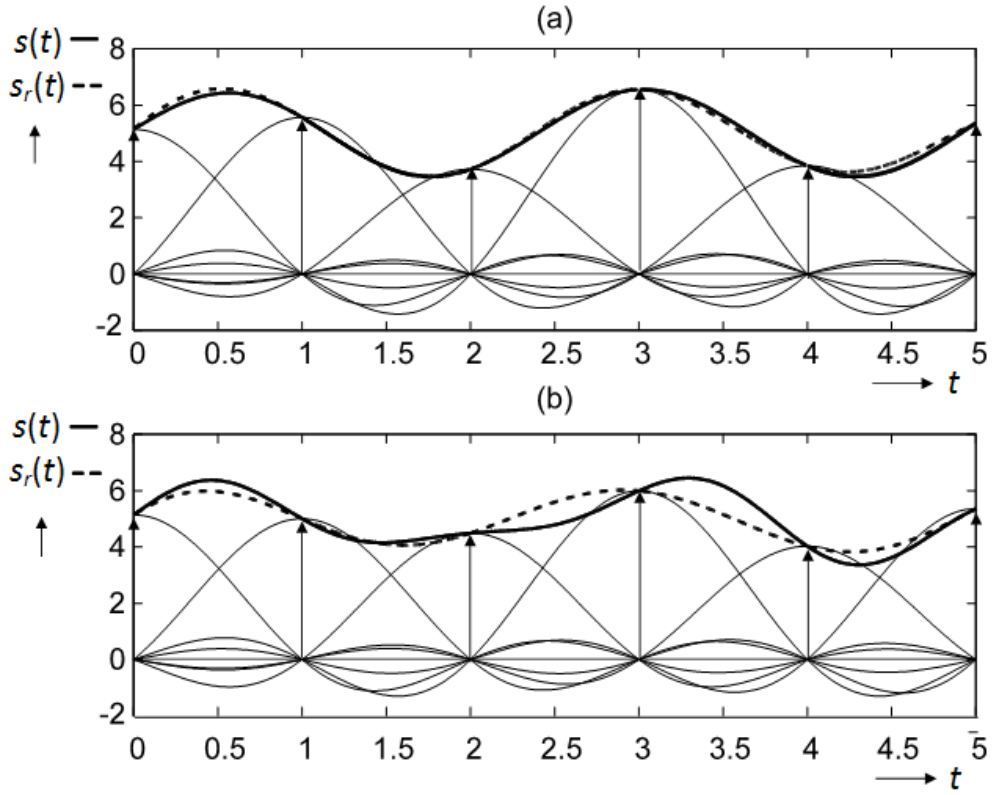
$$s_r(t) = \sum_{n=-\infty}^{\infty} s(nT)\,\mathrm{sinc}\frac{\pi}{T}(t - nT)$$

Aliasing: overlapping of spectrum components.

Nyquist – Shannon sampling theorem: A band-limited signal having no spectral components above f_m (cut-off frequency in Hertz) can be determined uniquely by values sampled at uniform intervals with frequency:

$$f_s \geq 2 f_m$$

3.1 Sampling



← Sampling theorem is fulfilled

$$f_s \geq 2 f_m$$

← Sampling rate is low

$$f_s < 2 f_m$$

Natural sampling: multiplying the signal with series of rectangular pulses of the width υ (*sample & hold* (SH)). Magnitude of spectrum drops according to the function:

$$\operatorname{sinc}\left(2\pi f \frac{\vartheta}{2}\right)$$

3.2. Source coding

Definitions:

Redundancy: amount of symbols or bits, which can be removed from a message without loss of information. Removal of redundancy = **loss-less compression.**

Irrelevancy: unsubstantial (waste) information, which can be suppressed in a message (voice or video) so that required quality of a signal is maintained. Removal of irrelevancy = **lossy compression.**

Speech coding (300 Hz - 3.4 kHz)

- **Waveform coding** using uniform and non-uniform quantization (PCM linear and nonlinear, DPCM, DM, ADM).
- **Parametric source coding (vocoders)** - **lossy compression.**
- **Hybrid coding - lossy compression.**

3.2. Source coding

Audio compression (10 Hz - 20 kHz)

Removal of inaudible sound components caused by masking effect of human auditory system - lossy compression

- **Source coding MPEG1 (*Moving Picture Experts Group*) (layer 1, 2, and 3), MPEG2, MPEG4.**

Image and video compression (DC - 6 MHz)

Removal of space and time redundancy and suppression of irrelevant components - lossy compression

- **Transformation coding – JPEG (*Joint Photographic Experts Group*).**
- **DPCM and predictive coding.**
- **Hybrid coding** (transformation coding, predictive coding, motion vectors) – **MPEG.**

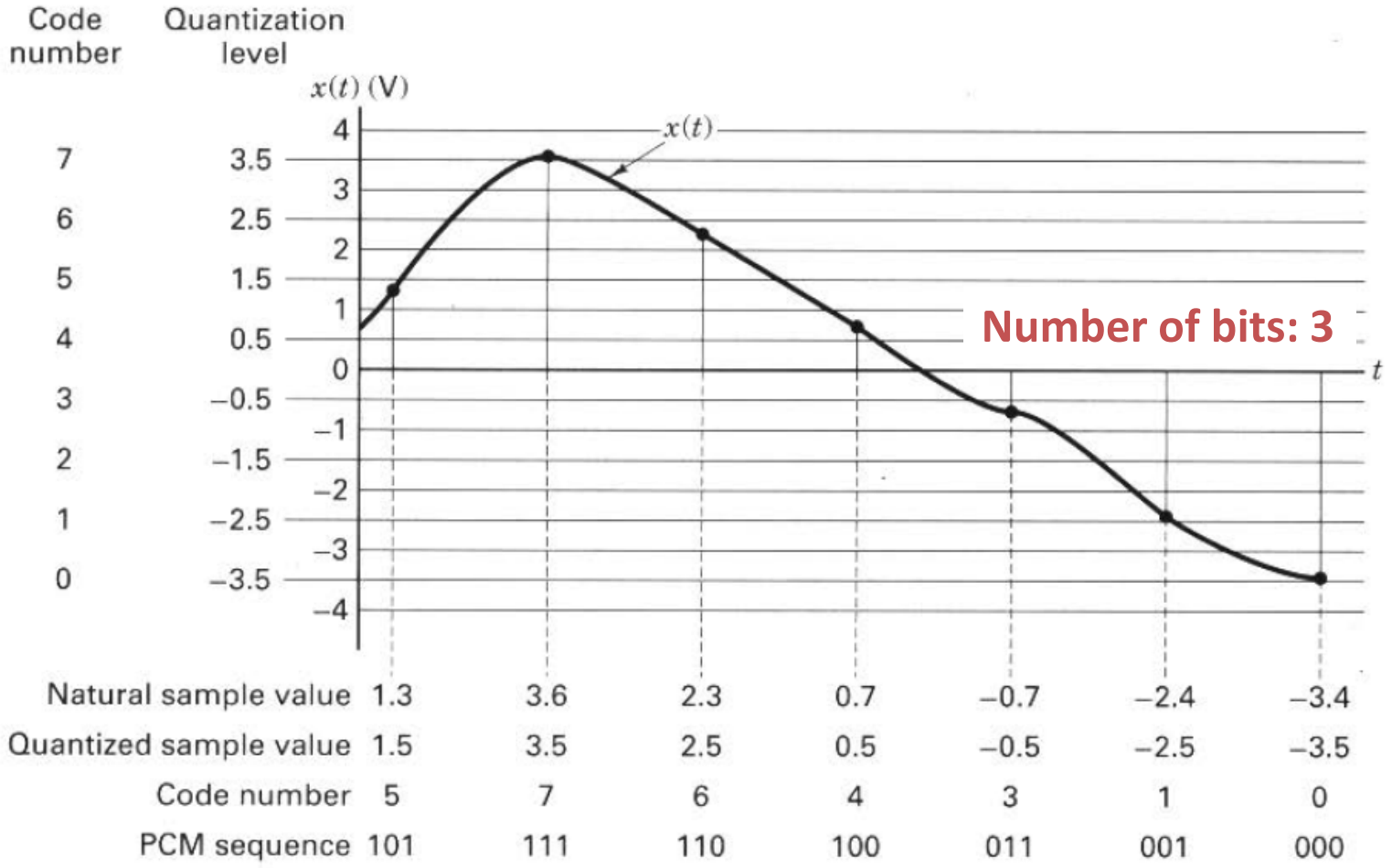
3.2. Source coding

Source coding for digital data

- **Non-adaptive entropy encoding** (predefined dictionary): ***Huffman* coding – VLC (variable-length code), prefix-free codes.**
- **Adaptive encoding** (dynamically generated dictionary): **LZW (*Lempel – Ziv – Welch*) (GIF, TIFF, ARJ).**

3.2.1 Waveform coding

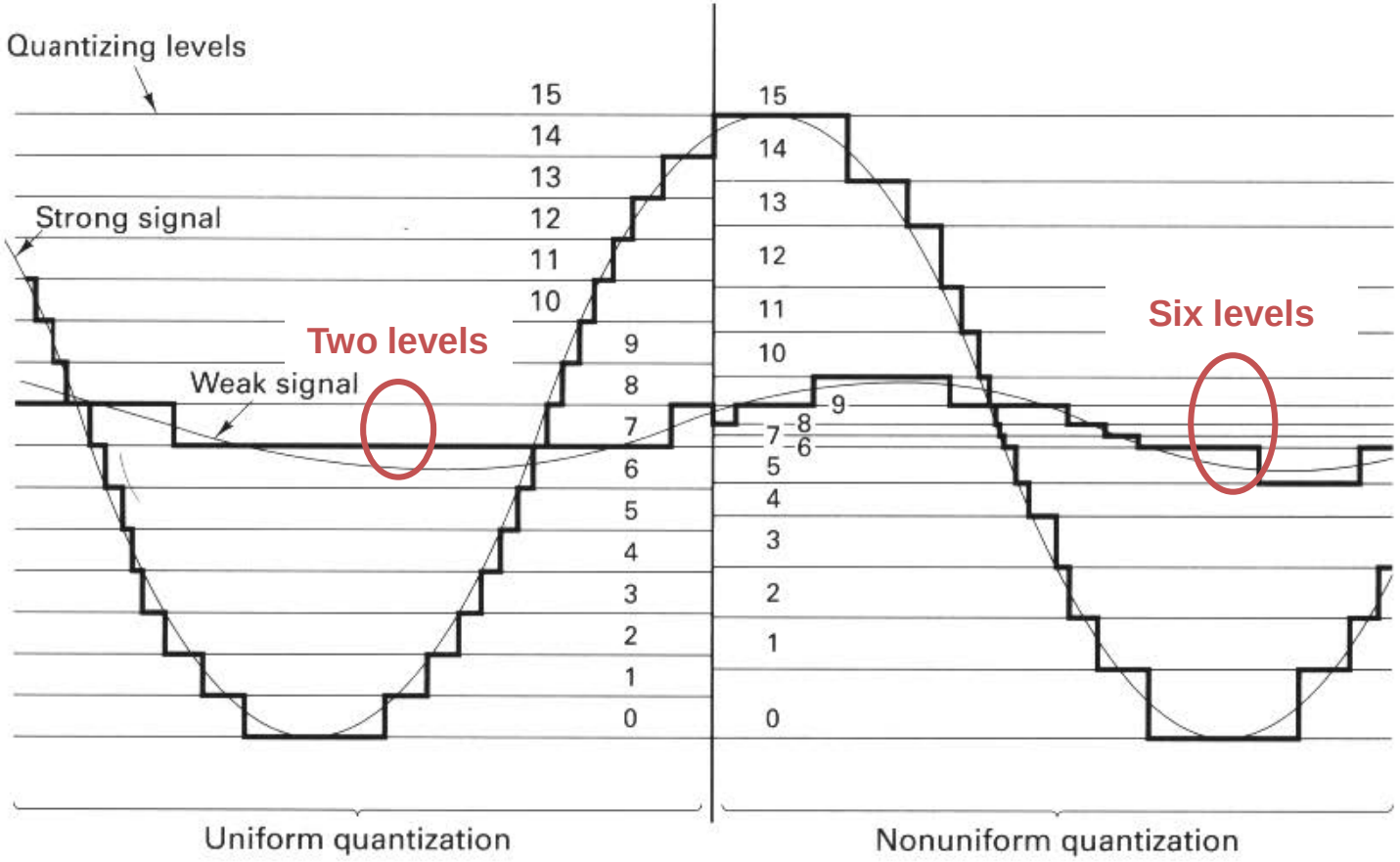
PCM (*Pulse Code Modulation*): Analog to Digital Converter (ADC).



Each sample is assigned to one of eight levels or a 3-bit PCM sequence.

3.2.2 Uniform and nonuniform quantization

In human speech very low speech volumes predominate, large amplitude values are relatively rare.



Non-uniform quantization advantage: fine quantization of the weak signals and coarse quantization of the strong signals.

3.2.2 Uniform and nonuniform quantization

The μ – law nonlinearity

$$|y_\mu(t)| = \frac{\ln(1+\mu|x(t)|)}{\ln(1+\mu)}$$

Typically: $\mu = 255$

The A – law nonlinearity

$$|y_A(t)| = \begin{cases} \dfrac{|x(t)|A}{1+\ln A} & 0 \le |x(t)| \le \dfrac{1}{A} \\ \dfrac{1+\ln(|x(t)|A)}{1+\ln A} & \dfrac{1}{A} \le |x(t)| \le 1 \end{cases}$$

Typically: $A = 87.6$

The calculation of nonlinear functions is difficult ⇒
approximation of nonlinearities by polyline.

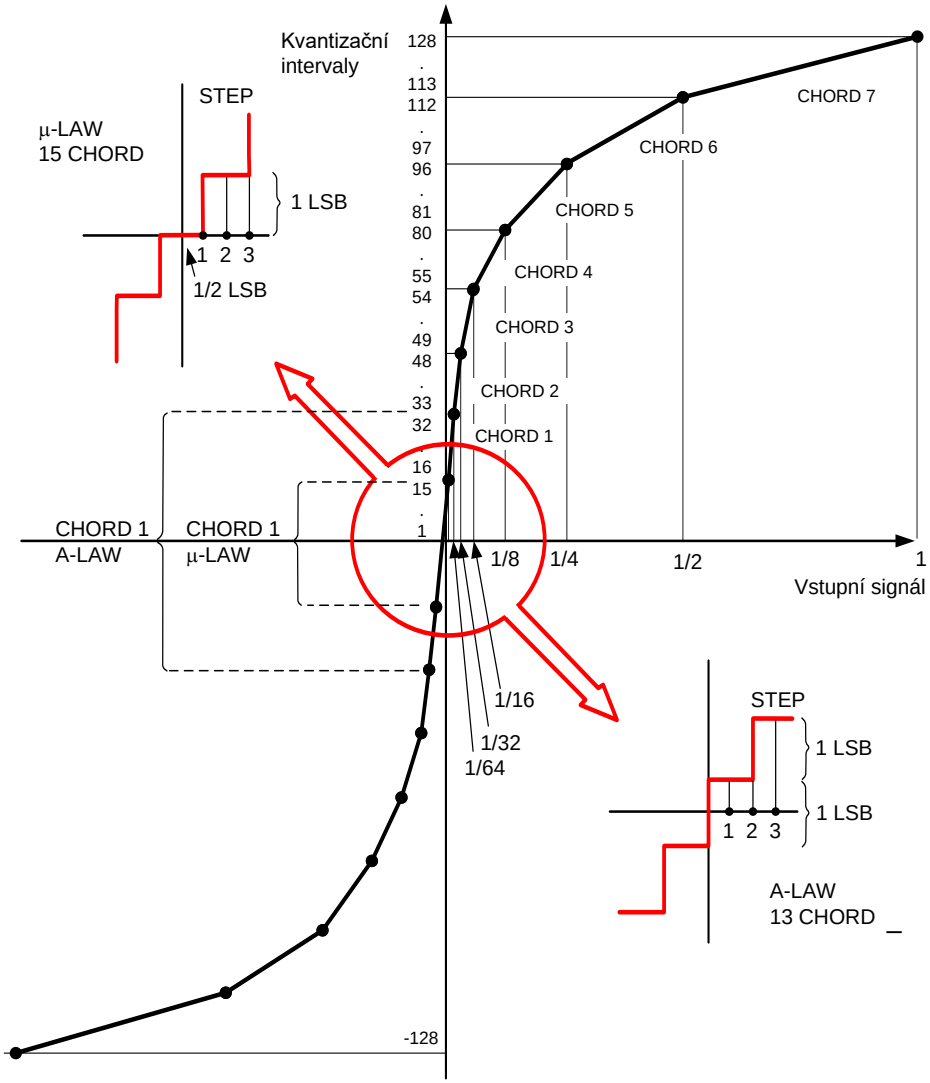
Sign	Chord			Step			
x	x	x	x	x	x	x	x

x = log 0 or log 1

ADC = coder, DAC = decoder ⇒ ADC + DAC = codec.

3.2.2 Uniform and nonuniform quantization

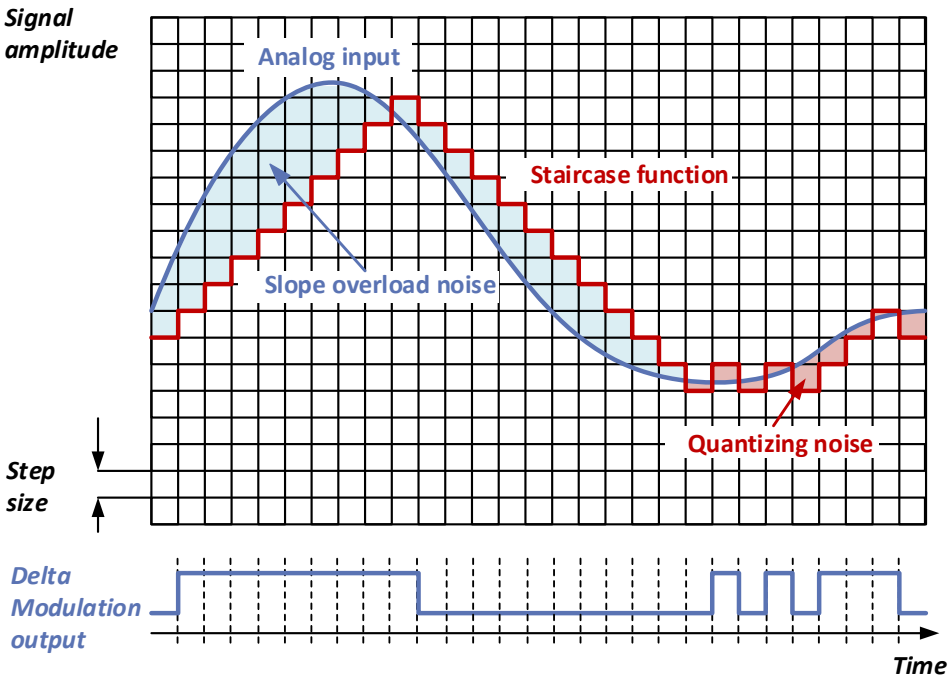
Codecs with non-linear quantization of A law and μ law type (8 bits (1+3+4))

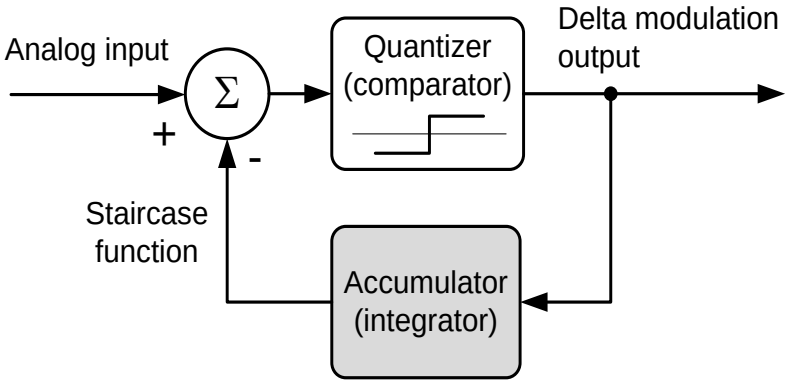


3.2.2 Uniform and nonuniform quantization

Utilization: telephone central offices. Different quantization nonlinearities: *A*-law in Europe, μ - law in USA.

3.2.3 Delta modulation (DM)





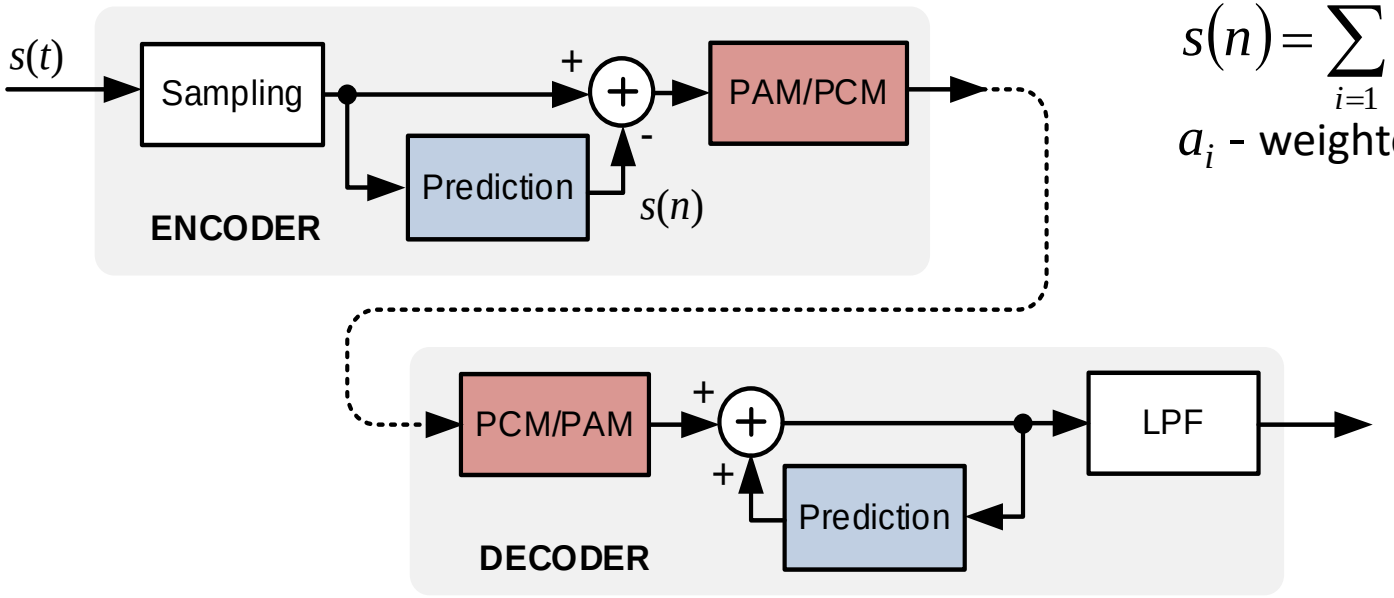
DM or *Δ*-modulation: conversion technique applicable for transmission of voice where quality is not of primary importance.

3.2.4 Adaptive delta modulation (ADM)

ADM: continuously variable slope delta modulation in which the step size varies according the change rate of the voice signal (to avoid slope overload).

3.2.5 Differential Pulse Code Modulation (DPCM)

DPCM calculates the difference between the predicted and instant value and quantizes it.



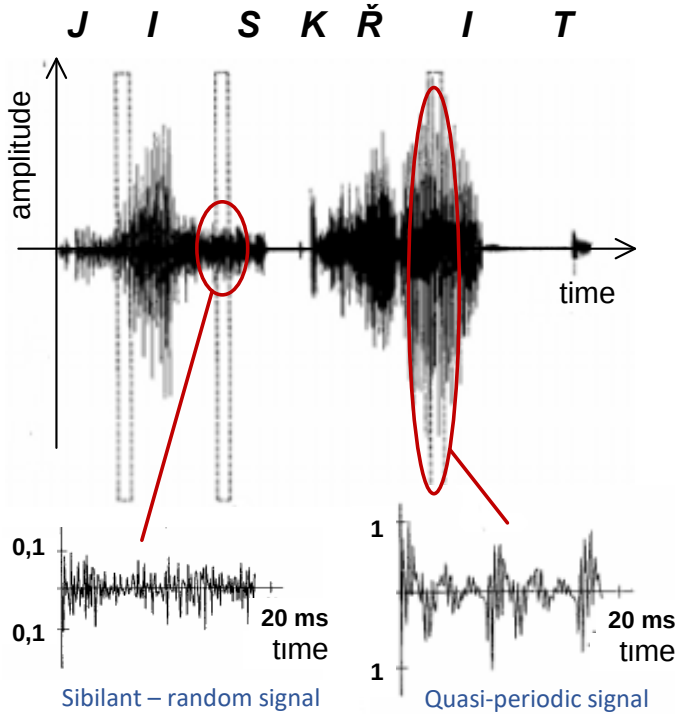
$$s(n) = \sum_{i=1}^{N} a_i s(n-i)$$

a_i - weightenning coefficient

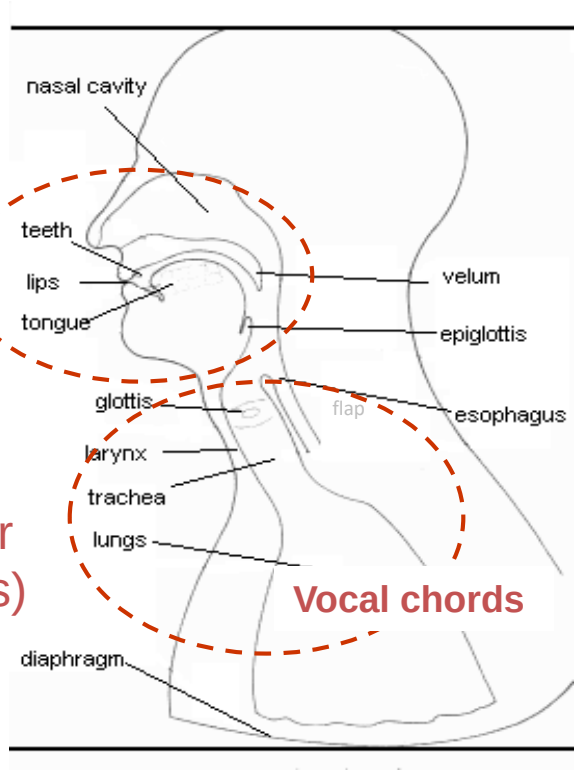
Compression ratio: 2 to 4 (if differences are subsequently entropy coded).

3.2.6 Parametric source coding

Voice record



The organs of speech



Filter

Generator (together with lungs)

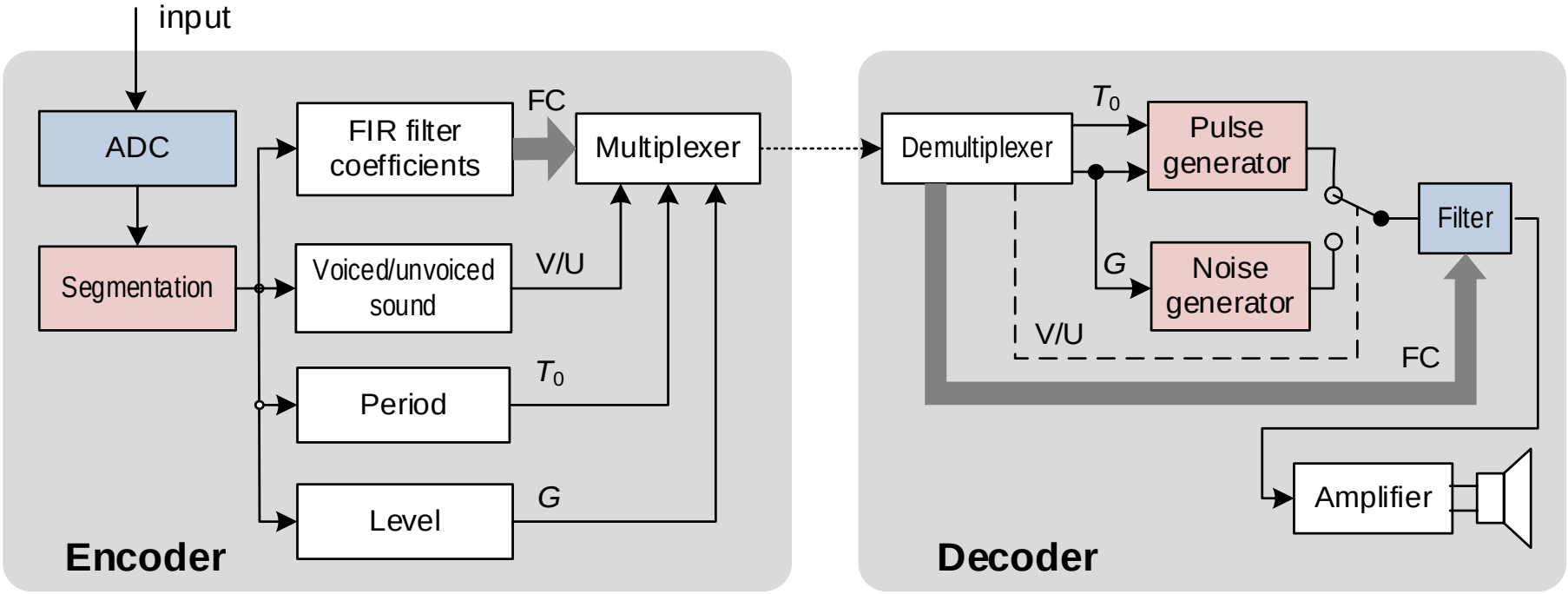
Generation of voiced sounds: **by opening and closing of the glottis which produces a periodic waveform with a lot of harmonics and by filtering by the nose and throat.**

Generation of unvoiced and plosive sounds: **by the mouth in different fashions.**

3.2.6 Parametric source coding

Vocoder: **examines speech and determines filter coefficients, voiced or unvoiced sound, period of a quasi-periodic signal and sound level.**

Vocoder block diagram



Speech segmentation: **identification of the boundaries between phonemes in spoken voice. Division voice into segments of 10-30 ms duration (parameters of human voice organs are *stationary*).**

Hybrid source coding

The speech signal is represented by the filter response to the excitation signal, however, it is generated in a more complex way.

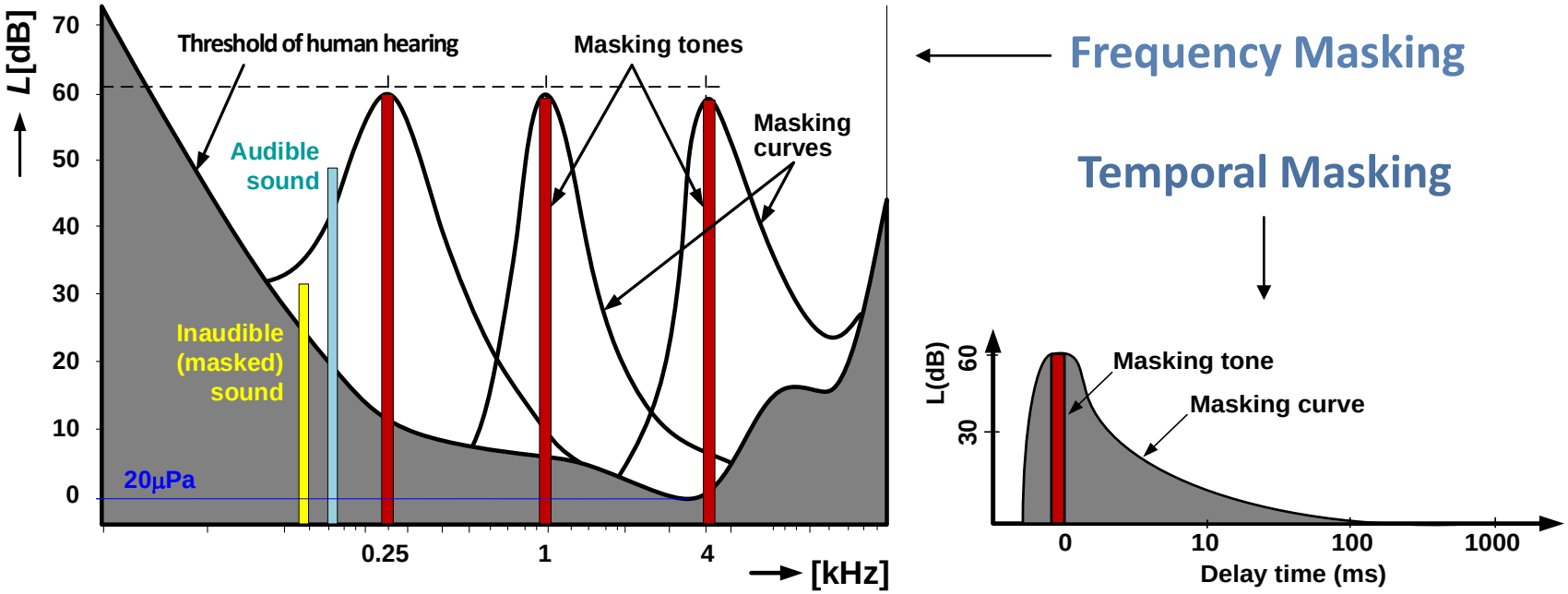
- **There is no distinction between voiced and unvoiced sounds.**
- **A multi-pulse excitation (pulses with unequal spacing) is used.**
- **The encoder includes a decoder generating a differential error which is minimized, transmitted through the channel and used to set the excitation generator in the receiver.**

The pulse excitation methods include:

- ***Multi Pulse Excitation* (*MPE*): individual pulse distances and amplitudes, bitrate: 8-16 kbps.**
- ***Regular Pulse Excitation* (*RPE*). Pulse position is given, amplitudes are individual, bitrate: 8-16 kbps.**
- ***Code Excited Linear Prediction* (*CELP*)**
  A set of the typical sound segments are represented by the pulse sequences stored in the "book". Only the sequence address is transferred. Bitrate: 4 kbps and lower.

3.2.7 Audio compression (10 Hz - 20 kHz)

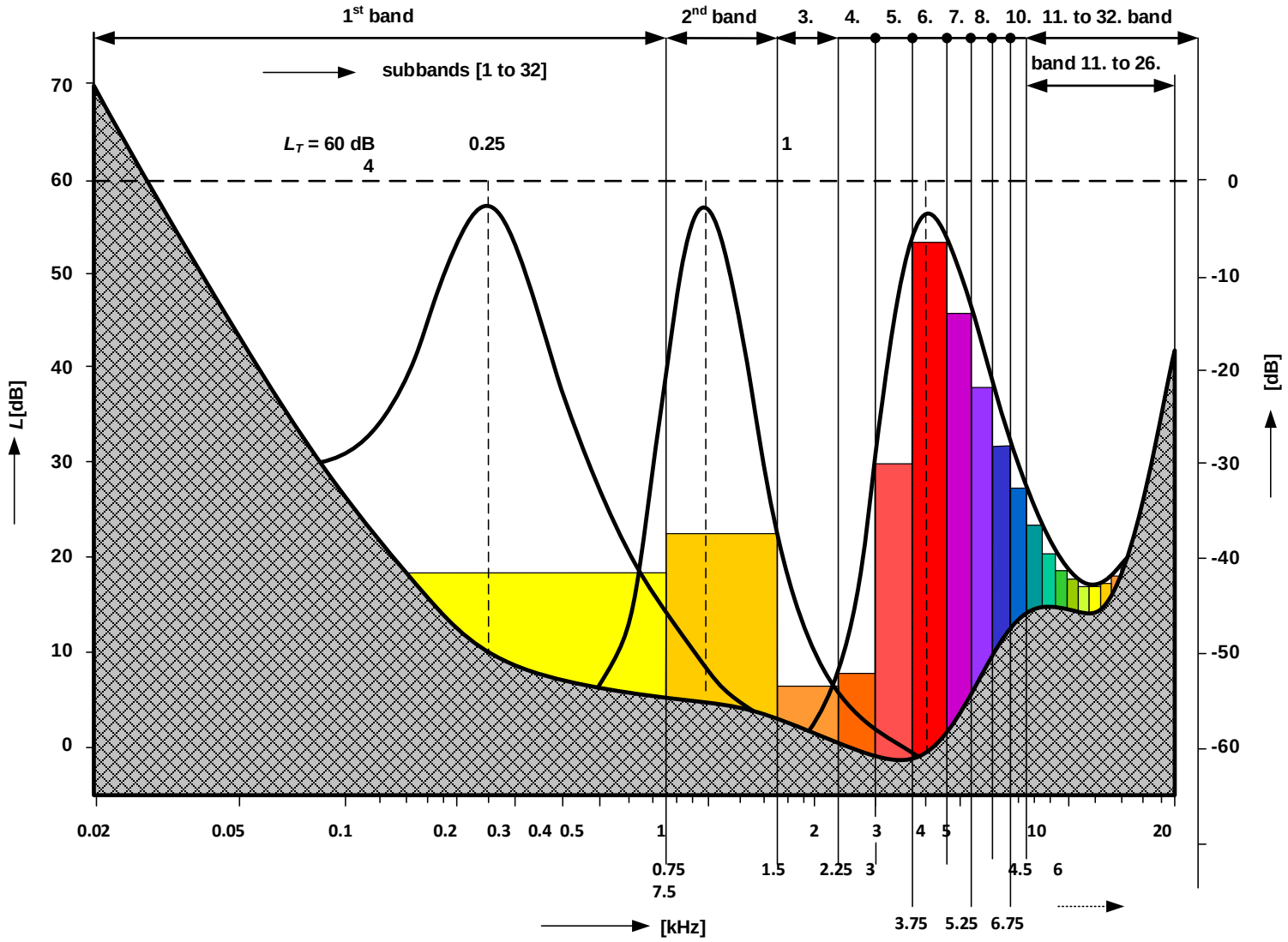
- **Source coding MPEGx: based on temporal and frequency masking effect of human auditory system.** A lower tone can effectively mask a higher tone.



- **Frequency Masking Curves: determines how particular pure tone affects human ability to hear tones nearby in frequency.**
- **Temporal Masking: any loud tone will cause the hearing receptors in the inner ear to become saturated and require time to recover.**

3.2.7 Audio compression (10 Hz - 20 kHz)

Subband coding



3.2.7 Audio compression (10 Hz - 20 kHz)

MPEG audio coding overview

1. Applying a filter bank to split the sound into 32 frequency sub-bands.
2. Signal level analysis in all sub-bands.
3. In parallel, applying a psychoacoustic model to the data (for bit allocation block ≈ 8 ms).
4. Calculation of the number of the quantization bits for all sub-bands.
5. Quantization of the allocated bits from the filter bank – providing the compression.

MPEG 1 variants:

- Layer-1
- Layer-2 (DAB)
- Layer-3 (MPEG3 players)

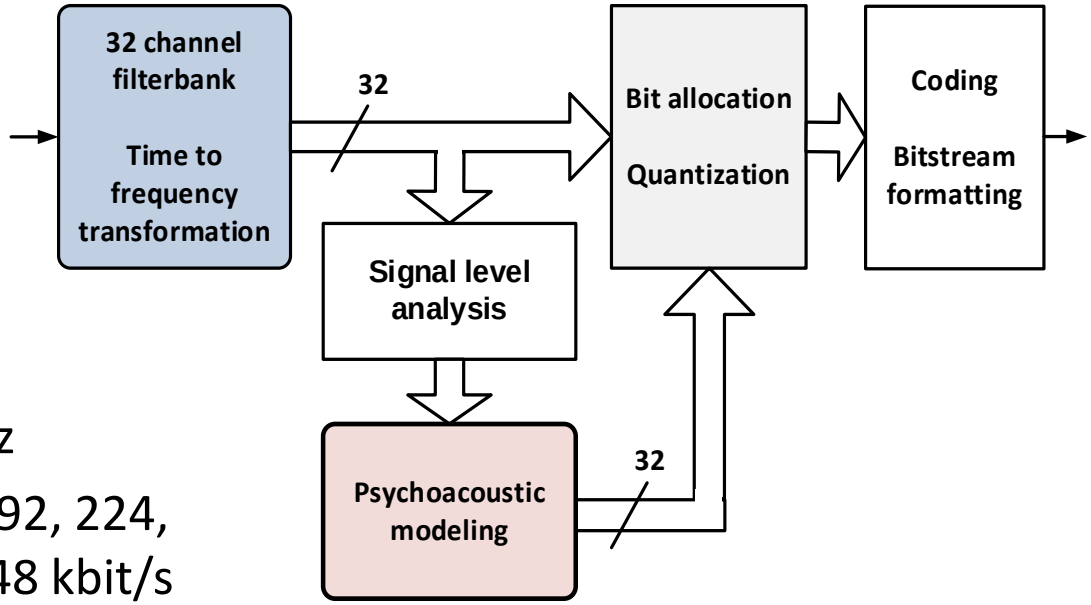
MPEG 2: DVB

MPEG 4: multimedia

Sampling rates: 32, 44.1, 48 kHz

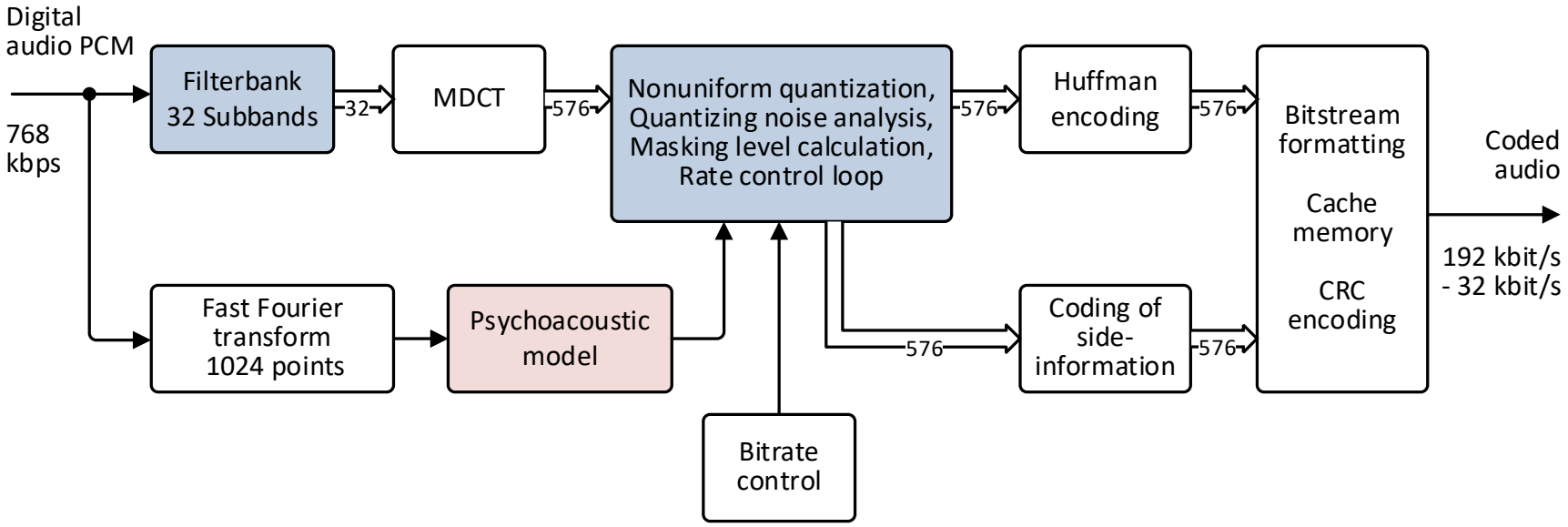
Bitrates: 32, 64, 96, 128, 160, 192, 224, 256, 288, 320, 352, 384, 416, 448 kbit/s

MPEG-layer 1



3.2.7 Audio compression (10 Hz - 20 kHz)

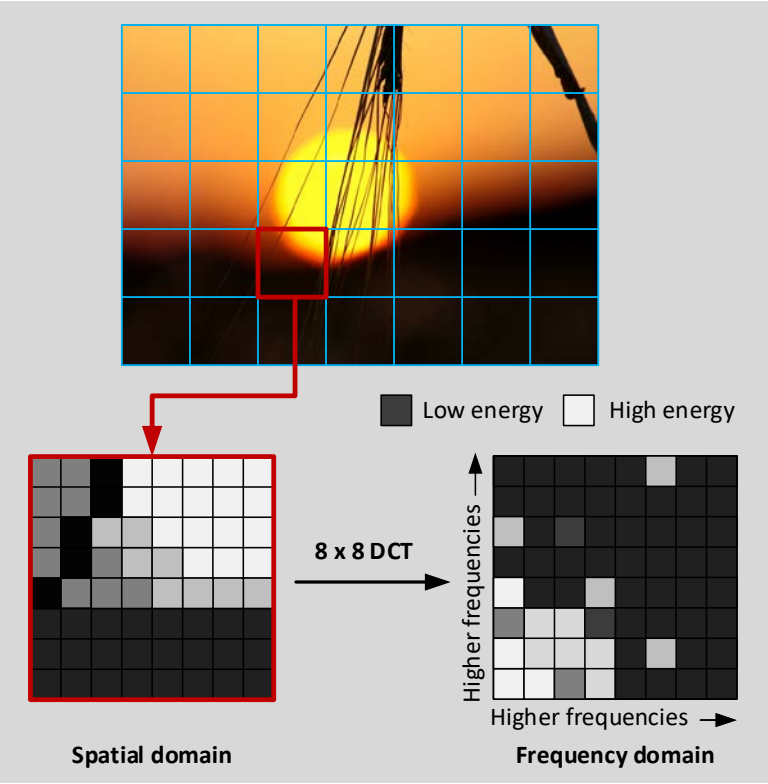
MPEG 1 Layer-3



- ✓ **Part 1 divides the audio signal into frames. An MDCT (*Modified Discrete Cosine Transform*) filter is then applied on the output to get 576 subchannels.**
- ✓ **Part 2 passes the sample into a 1024-point FFT, and then the psychoacoustic model is applied.**
- ✓ **Part 3 quantifies and encodes each sample. This is also known as noise allocation. The noise allocation adjusts itself in order to meet the bit rate and sound masking requirements.**
- ✓ **Part 4 formats the bitstream into an audio frame. An audio frame is made up of 4 parts, The Header, Error Check, Audio Data, and Ancillary Data.**

Static picture standard JPEG – compression algorithm:

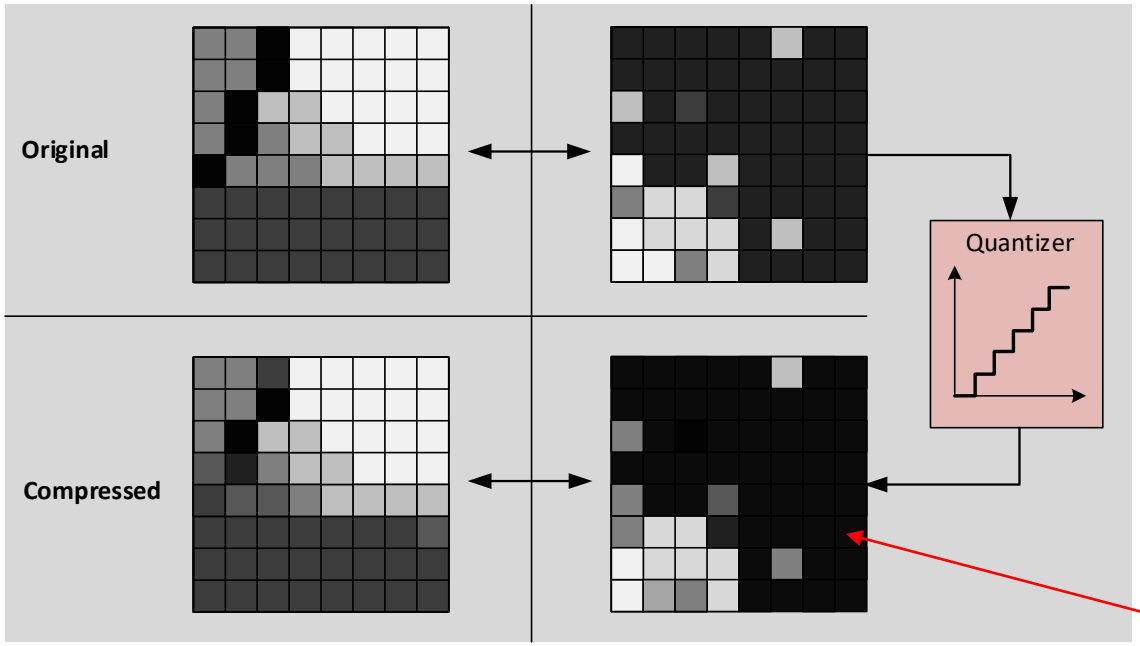
1. **Conversion of RGB values to Y, R-Y, B-Y color space** (Y: luminance signal - brightness information, R and B: chrominance signals - color information).
2. **Split frame into 8 × 8 blocks**.
3. **Application 2- dimensional** Discrete Cosine Transform (DCT) on each block - loss-less transformation from the spatial to the frequency domain.



- **Low frequencies** - large features in the image.
- **High frequencies** - small features.
- The human eye is more sensitive to the information contained in low frequencies ⇒ low-frequency coefficients are encoded with a higher precision than the high-frequency ones.

3.2.8 Image and video compression (DC - 6 MHz)

4. **Quantization of DCT coefficients:** dividing the coefficients by quantization matrix ***Q*** and rounding the results.



Low frequencies

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Large values. Why?

Zero power coefficients

Quantization discards many bits. For example, a 12-bit coefficient may be rounded to the nearest of 32 predetermined values $\Rightarrow$ five-bit symbols.

3.2.8 Image and video compression (DC - 6 MHz)

5. **Run length and entropy coding:** grouping consecutive zero-valued coefficients (a "run") using a zig-zag scanning (see page 36) and encoding the number of coefficients (the "length") instead of encoding the individual zero-valued coefficients.
6. **Variable-length coding (VLC):** frequently occurring symbols are represented using short code words (containing only a few bits), while less common symbols are represented with longer code words.

JPEG total compression ratio ≈ 10:1

Motion picture standard MPEG – hybrid coding

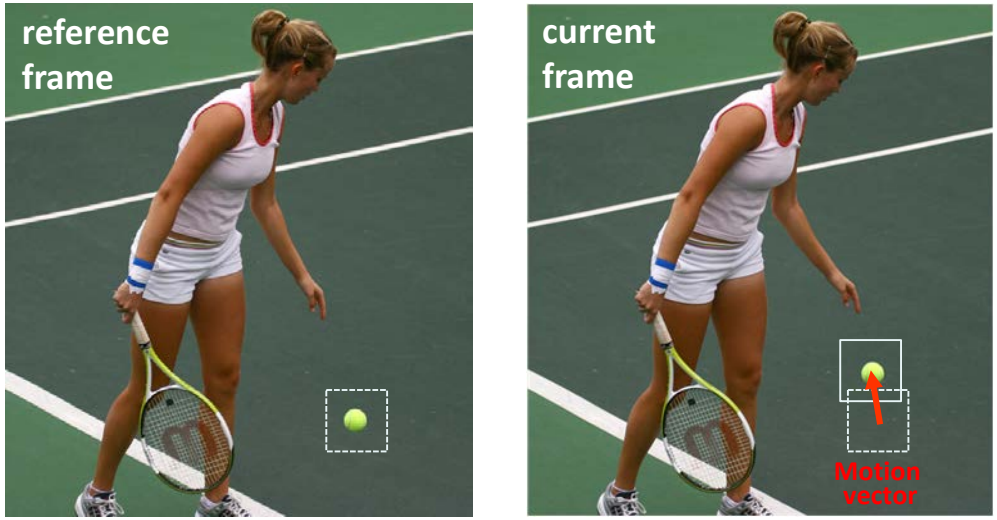
- **Applies compression techniques used in the still-image compression (JPEG).**
- **Takes advantage of the similarities (correlation) between successive video frames and uses video-specific compression techniques such as**
  - **BMA (*Block Matching Algorithm*),**
  - **DPCM (*Differential PCM*),**

  to achieve better compression ratios ≈ 200:1.

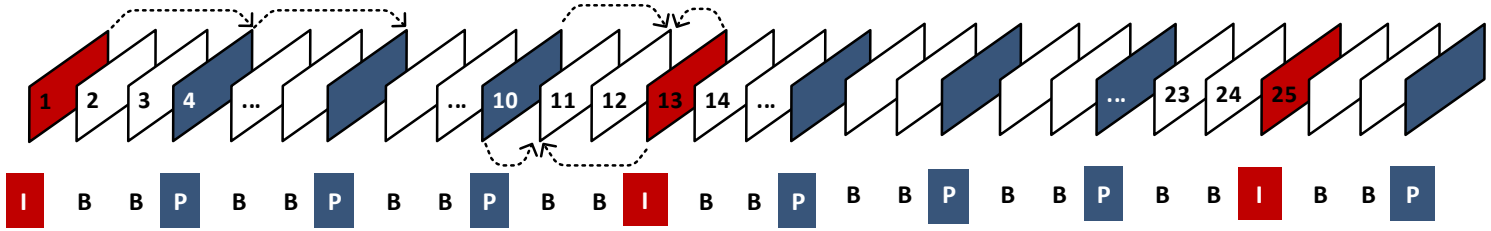
3.2.8 Image and video compression (DC - 6 MHz)

General idea: use **motion vectors** (macroblock motion estimation) to specify how a 16x16 macroblock is translated between the **reference frame** and **current frame** using BMA, then code difference using DPCM between reference and actual block.

Motion estimation



1. **Creation** **Group of Pictures (GOP):** set of consecutive frames that can be decoded without any other reference frames.



3.2.8 Image and video compression (DC - 6 MHz)

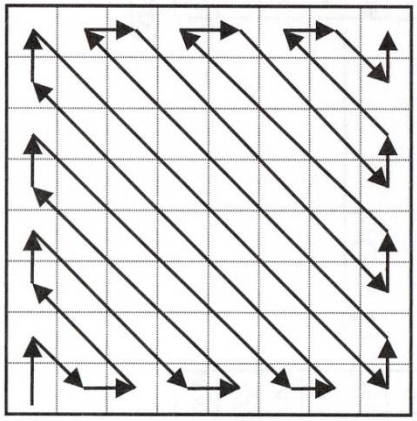
Frame types:

- **I-frame** (intra-coded): DCT coded without reference to other frames
- **P-frame** (predictive-coded): coded with a reference to a previous reference frame (either I or P) see below.
- **B-frame** (bi-directional predictive-coded): coded with reference to both previous and future reference frames (either I or P) see bellow.

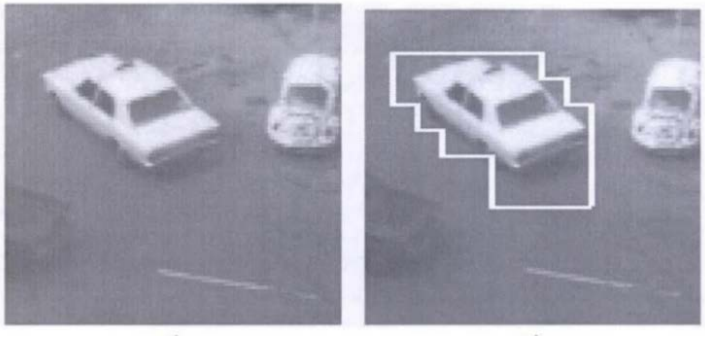
2. **Estimation of motion vectors:** each reference frame macroblock is searched in the current frame using BMA. For each macroblock found, the motion vector is calculated.
3. **Calculation of DPCM:** differential frames P or B are obtained by subtraction of a current frame and a reference frame (I or P) created using motion vectors (by applying of shifted macroblocks)
4. **Transformation of differential frames into frequency domain** using DCT…
5. **Run length and entropy codding** of all frames using zig-zag and VLC Huffman algorithms (see JPEG).
6. **Multiplexing** of frequency domain coefficients and motion vector coordinates.

3.2.8 Image and video compression (DC - 6 MHz)

Zig-zag scanning



BMA example



Newer algorithm H.264

Supports the CAVLC (*context-adaptive VLC*) , CABAC (*context-adaptive arithmetic coding*), multi frame prediction, adaptive macroblock size, deblocking filter and other techniques.

- CABAC compresses data more efficiently than CAVLC but requires considerably more processing to decode.
- Deblocking filter helps prevent the blocking (quantization) artefacts resulting in better visual appearance and compression efficiency.

3.2.9 Data compression

The goal is to encode a sequence of symbols of the source alphabet (usually binary) so that the length (number of bits) of the symbols of the code alphabet is as low as possible and the sequence is uniquely decodable.

Example: $P(a)=0.73$, $P(b)=0.25$, $P(c)=0.02$

symbol	Code 1	Code 2	Code 3	Code 4	Code 5	Code 6
a	00	0	1	1	00	1
b	01	1	10	00	01	01
c	10	11	100	01	1	11
c b a b	**10010001**	**11101**	**10010110**	**0100100**	**1010001**	**1101101**
Length	**8**	**5**	**8**	**7**	**7**	**7**
Uniquely d.	**yes**	**no**	**yes**	**yes**	**yes**	**no**
Prefix-free code	**yes**	**no**	**no**	**yes**	**yes**	**no**

A sufficient condition of unambiguous decodability: no symbol is a prefix of another symbol.

Average number of bits: $\overline{n} = \sum_i n_i P(X_i)$

n_i: code-word length
$P(X_i)$: probability of code-word occurrence

3.2.9 Data compression

Huffman coding

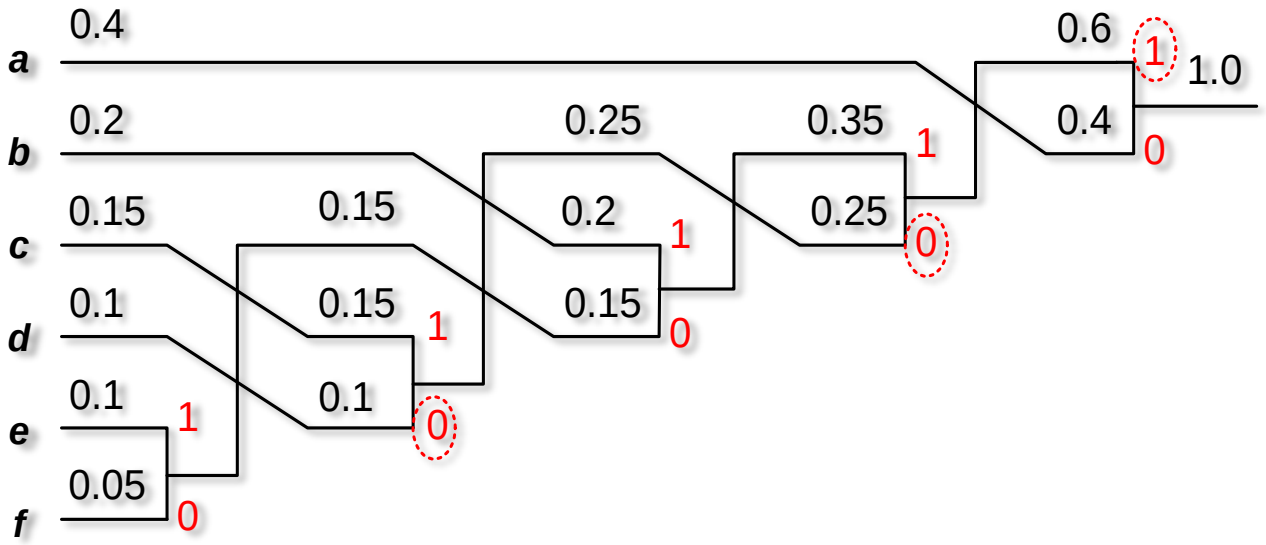
- **Non-adaptive entropy encoding** (predefined dictionary coding).
- **VLC (*variable-length code*).**
- **Prefix-free code.**
- **Shortest average length code.**
- **Encoding requires knowledge of the relative frequency (probability) of input symbol (alphabet) occurrence.**

Encoding guide:

1. List the input alphabet along with their probability (relative frequency) in descending order↓.
2. Assign symbol 0 to a last branch and symbol 1 to the next to last branch.
3. Merge the two branches with lowest probability and form new branch with their cumulative probability.
4. Reorder (if necessary) branches with descending probability of occurrence.
5. Until only two branches with the cumulative probability equal to 1 remain, repeat points 2 to 5.

3.2.9 Data compression

Example:



Input alphabet	*Probability of occurrence*	*Code symbols*
a	0.4	0
b	0.2	111
c	0.15	101
d	0.1	100
e	0.1	1101
f	0.05	1100

Adaptive LZW (*Lempel – Ziv – Welch*) encoding

Data is encoded by looking through the existing dictionary (containing already-coding segments) for a match to the next segment in the sequence being encoded. If a match is found the code references the location of the segment sequence (library address) and then appends the next symbol.

Example of the *Lempel–Ziv LZ78 algorithm*:

Let we have a set of input alphabets: [*a* | *b* | *a a* | *b a* | *b b* | *b b b* | *b b a* | *b b b b* | *b a*]

LZ78 code packet (symbol): ⟨library address, next symbol⟩.

code packet	⟨0,a⟩	⟨0,b⟩	⟨1,a⟩	⟨2,a⟩	⟨2,b⟩	⟨5,b⟩	⟨5,a⟩	⟨6,b⟩	⟨4,-⟩
address	1	2	3	4	5	6	7	8	
content	*a*	*b*	*aa*	*ba*	*bb*	*bbb*	*bba*	*bbbb*	

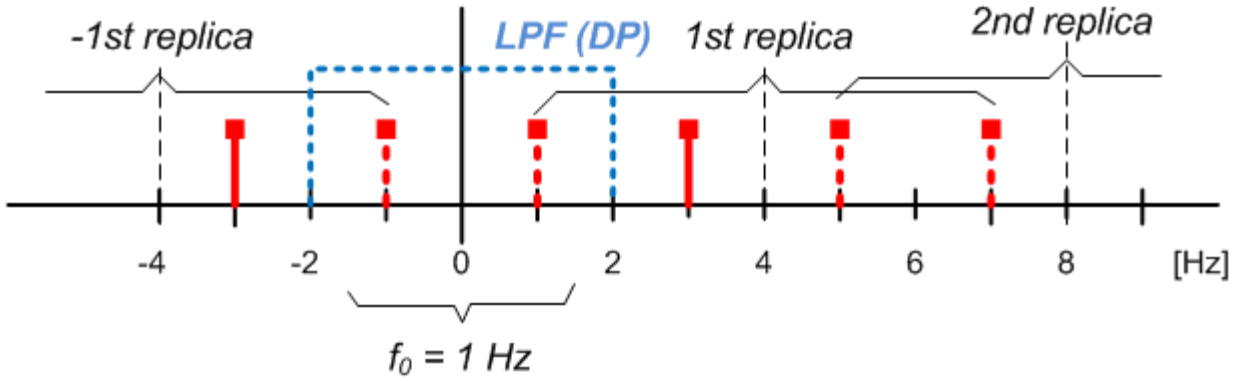
Problems

1. *Harmonic signal* $s(t) = 10 \times \cos(6\pi t + \pi/2)$ *is sampled by the rate* $f_s = 4$ *Sa/s and then fed to the low-pass filter with the cut-off frequency of* $f_m = 2$ *Hz. Evaluate the signal frequency at the filter output.*
2. *Voltage* $V_i = 0.31V$ *is applied to the input of a non-uniform quantizer working with A-law characteristics. Specify the code word at the output if the input voltage range of the quantizer is ±2V.*
3. *The message contains only alphabets a – f. Relative frequencies (probabilities) of alphabet occurrence are:* $P(A) = 0.35$, $P(B) = 0.16$, $P(C) = 0.10$, $P(D) = 0.08$, $P(E) = 0.25$ *a* $P(F) = ?$ *Encode them using the Huffmann code and decode the message* 1 1 0 1 0 0 1 1 0 1 0.
4. *Signal parameters of the MPEG1 encoder are: sampling rate 48kSa/s, number of quantization bits 16. Subchannel number (into which the signal is split) 32. Determine the sample rate in each channel, segment duration (in ms) and number of samples per segment in each channel, if the segmentation is performed by 384 samples.*
5. *Encode sequence of numbers M =* 1001 0001 0001 1001 1100 1110 0010 0010 *using the Lempel-Ziv algorithm LZ78.*

Problems

As for 1

$s(t) = 10\cos(6\pi t + \pi/2) \rightarrow f = 3$ Hz
$f_s = 4$ Hz
$f_m = 2$ Hz



Problems

As for 2

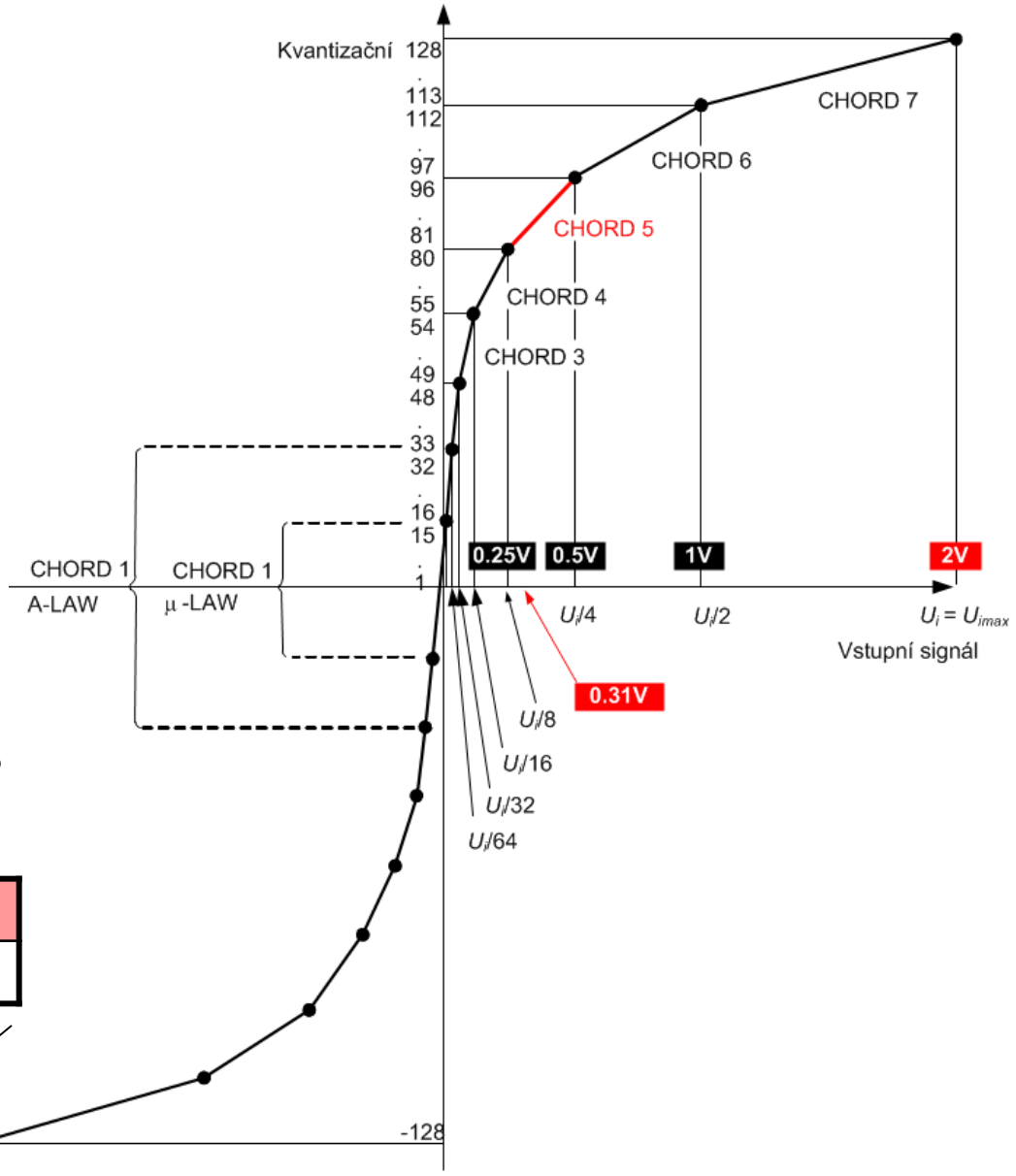
$U_i = 0.31\text{V}$
$U_{imax} = \pm 2\text{V}$
Nonlinearity: A-law

$$0.25 + k\Delta U_5 = 0.31$$

$$\Delta U_5 = \frac{0.5 - 0.25}{2^4} = 0.015625$$

$$k = floor\left(\frac{0.31 - 0.25}{0.015625}\right) = floor\,(3.84) = 3$$

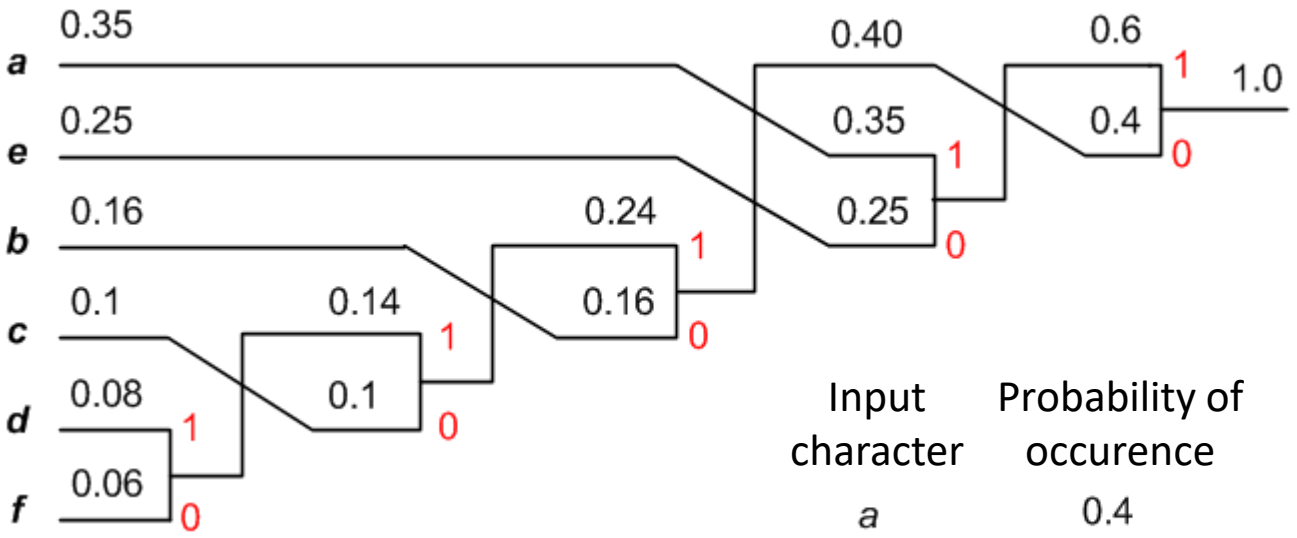
Polarity	Chord			Step			
+(1), - (0)	1	0	1	0	0	1	1
		5			3		



Problems

As for 3 *P(A) = 0.35, P(B) = 0.16, P(C) = 0.10, P(D) = 0.08, P(E) = 0.25 a P(F) = ?*
Encoding: Hufmann

P(F) = 1- P(A) - P(B) - P(C) - P(D) – P(E) = 1 - 0.35 - 0.16 - 0.1 - 0.08 - 0.25 = 0.06



Input character	Probability of occurence	Code word
a	0.4	11
b	0.16	00
c	0.10	010
d	0.08	0111
e	0.25	10
f	0.06	0110

1 1 | 0 1 0 | 0 1 1 0 | 1 0
A *C* *F* *E*

Problems

As for 4

Sampling frequency: f_s = 48kSa/s,
Number of quantization bits: N = 16.
Number of subchannels: M = 32.
Number of samples per segment: K = 384 Sa

Sampling frequency in subchannels: f_{ss} = 48/M = 48/32 = 1.5 kSa/s,
Number of samples in subchannels: K_s = 384/M = 384/32 = 12 Sa

Segment duration: $T_s = K_s / f_{ss}$ = 12/1500 = 8 ms
Check (using input data): $T_s = K/f_s$ = 384/48000 = 8 ms

Problems

As for 5

M = 1001 0001 0001 1001 1100 1110 0010 0010
Algorithm: *Lempel-Ziv LZ78*

code packet	⟨0,1⟩	⟨0,0⟩	⟨2,1⟩	⟨2,0⟩	⟨3,0⟩	⟨4,1⟩	⟨1,0⟩	⟨3,1⟩	⟨7,0⟩
address	1	2	3	4	5	6	7	8	9
content	1	0	01	00	010	001	10	011	100

code packet	⟨1,1⟩	⟨9,0⟩	⟨11,0⟩	⟨2,-⟩					
address	10	11	12	13					
content	11	1000	10001	0					

4 CRYPTOGRAPHY
4.1 Cryptography concepts

Reasons for using cryptosystems in communications:

1. **Privacy: to prevent unauthorized persons from extracting information transferred through the channel (eavesdropping).**
2. **Authentication: to prevent unauthorized persons from injecting an unwanted information into the channel (spoofing).**

- **Cryptography: transformation of a plain message into an unintelligible message (ciphertext).**
- **Key: set of symbols or characters which determines a specific encryption transformation.**
- **Cryptanalysis: estimation of the plaintext by analyzing the ciphertext in the channel, without benefit of the key.**
- **Cipher break: disclosure of the ciphering algorithm using the cipher-text-only attack (brute-force) or the known plaintext attack.**

4.1 Cryptography concepts

Encryption strategies:

1. **Block encryption:** segmentation of a plaintext into blocks of fixed size, each block encryption independently from the others.
2. **Stream encryption:** similar to a convolutional coding. There is no fixed block size.

Aims of cryptosystems:

1. To provide an inexpensive and easy means for encryption and decryption of information to all authorized users in possession of the appropriate key.
2. To ensure difficult and expensive the cryptanalyst's effort of producing an estimate of the plaintext without benefit of the key.

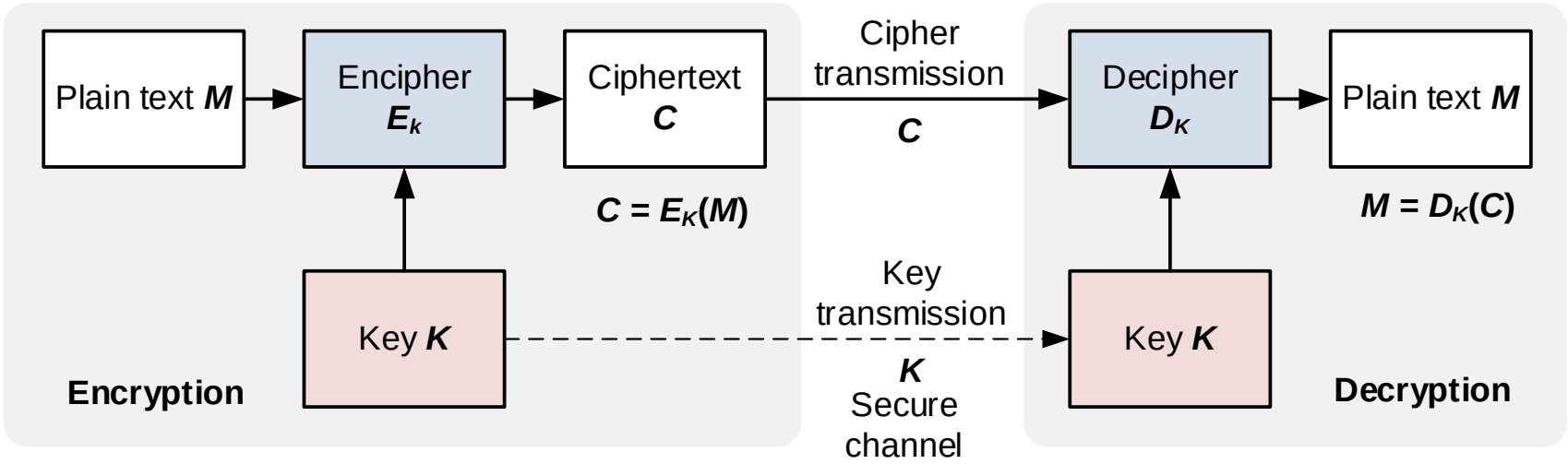
4.1 Cryptography concepts

Encryption categories:

1. Conventional cryptosystems – The same key is used for both encryption and decryption. Encryption algorithm can be revealed because the security of the cryptosystem depends on a safeguarded key.
2. Public key cryptosystems – utilizes two different keys. One (public) for encryption and the other (private) for decryption. The encryption algorithm and also the encryption key can be publicly revealed without compromising the security of the cryptosystem.

4.2 Conventional cryptosystems

Model of conventional cryptographic channel



Properties

- **Simple mathematical background and implementation.**
- **Protection performance depends on a safeguarding of the key.**
- **Encryption and decryption operations are reciprocal**
  $C = E_k(M), M = D_k^{-1}(C) \Rightarrow E_k = D_k^{-1}$.

4.2 Conventional cryptosystems

Substitution encryption techniques

- **Simple algorithms:**
  - **Each plaintext letter is replaced with a new letter obtained by an alphabetic shift** e.g. M1↔M4, M2↔M8, …
  - **Each plaintext letter is replaced with a new letter obtained by a combination of original letters** e.g. C1 = M1 XOR M2 XOR M6, C2=…
- **Little encryption protection**

Example 1: Caesar Cipher

- **Used by Julius Caesar during the Gallic wars**
- **Based o an alphabetic shift (3 positions)**

Plaintext:	n	o	w	i	s	t	h	e	t	i	m	e
Ciphertext:	q	r	z	l	v	w	k	h	w	l	p	h

4.2 Conventional cryptosystems

Example 2: Trithemius progressive key

- **Message character ordinary number defines the number of shifts in the alphabet. The first character is shifted by one position, the second character is shifted by two positions, …**

Plaintext:	n	o	w	i	s	t	h	e	t	i	m	e
Ciphertext:	o	q	z	m	x	z	o	m	c	s	x	q

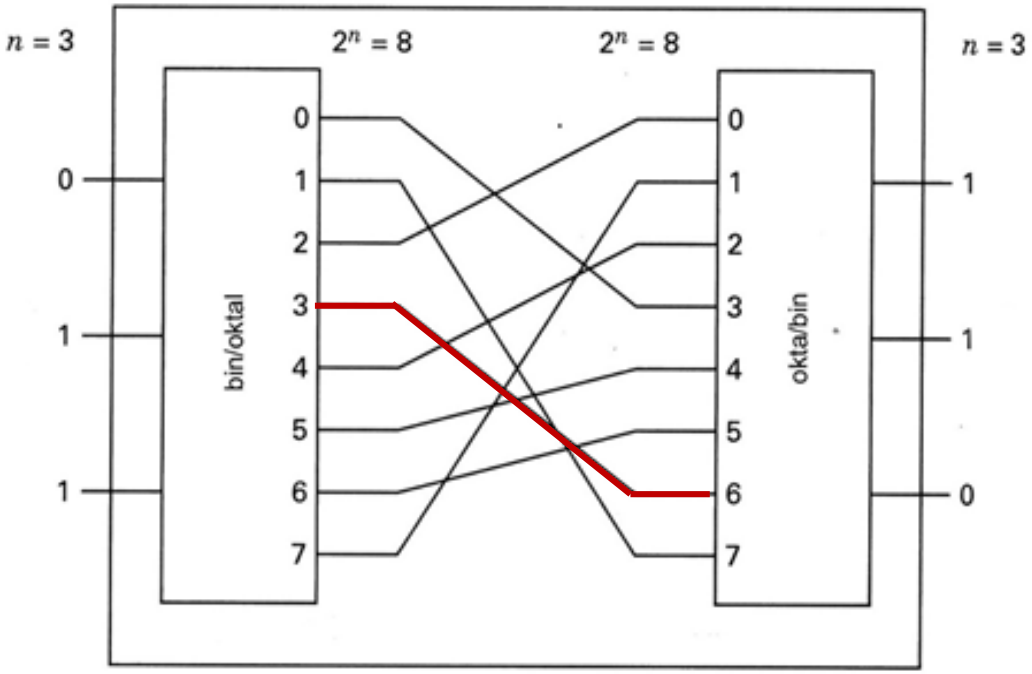
Example 3: Vigenere key method

- **Number of particular shifting defines a keyword.**
- **Position of the first character of keyword in alphabet defines the first message character shift. Position of the second character in alphabet defines the second message character shift …**

Keyword:	t	y	p	e	t	y	p	e	t	y	p	e
Shift:	19	24	15	4	19	24	15	4	19	24	15	4
Plaintext:	n	o	w	i	s	t	h	e	t	i	m	e
Ciphertext:	g	m	l	m	l	r	w	i	m	g	b	i

4.2 Conventional cryptosystems

Substitution using a nonlinear transformation



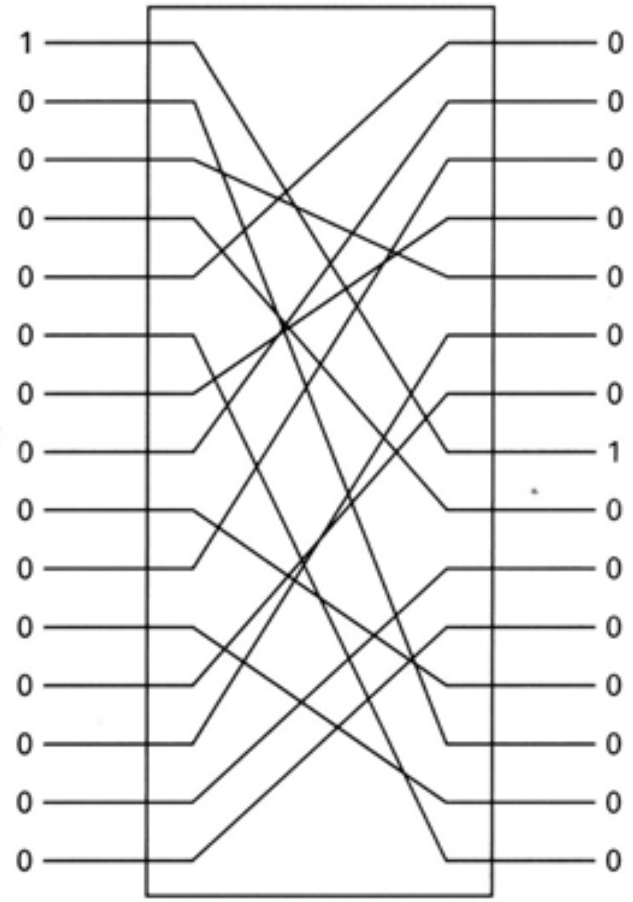
- ***n* input bits are represented as one of 2^n different characters**
- **Set of 2^n characters are permuted**
- **Character is converted back to an *n*-bit output.**

Permutation (transposition) encryption techniques

- **The positions of the plaintext letters in the message are rearranged, instead of being substituted with other letters** (THINK → HKTNI)**.**
- **This technique is vulnerable to trick messages (moving the single 1 position for each transmission can simply reveal I/O connection).**

4.2 Conventional cryptosystems

Transposition schematic diagram



Example 1: Transposition ciphering

- **Key is given by matrix size**
- **Ciphering consists in writing a plaintext into the rows and reading ciphertext from columns.**

Plain message: **this is a plain text**

t	h	i	s
i	s	a	p
l	a	i	n
t	e	x	t

Ciphertext: tilthsaeiaixspnt

4.2.1 Block and stream ciphering

Block cipher characteristics:

- Plain text is processed in *n*-bit blocks of data.
- Encrypted message is of the same length as the plain text.
- Pros: the plain text information diffuses into several ciphertext symbols (smooths out the statistical differences between characters and between character combinations).
- Cons:
  - to start the encryption it is necessary to take the entire block (large delay).
  - error affects the transformation of all the other characters of the same block (large error spreading).

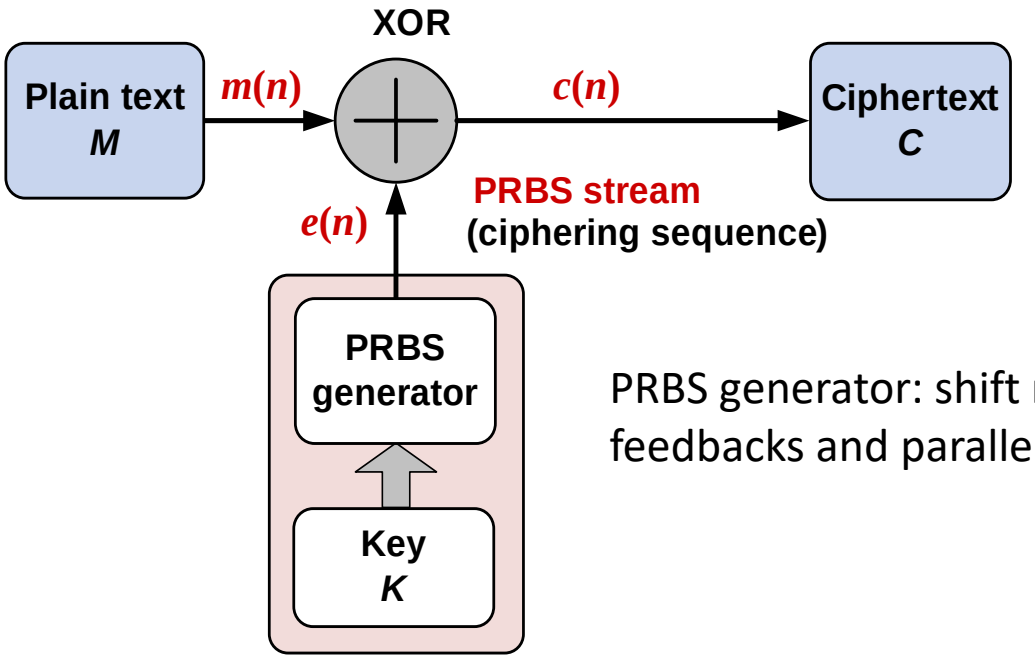
Stream cipher characteristics:

- Plain text is processed in bit-by-bit of data.
- It is based on addition of the plaintext and a „Pseudo-Random“ Binary Sequence (PRBS).

4.2.1 Block and stream ciphering

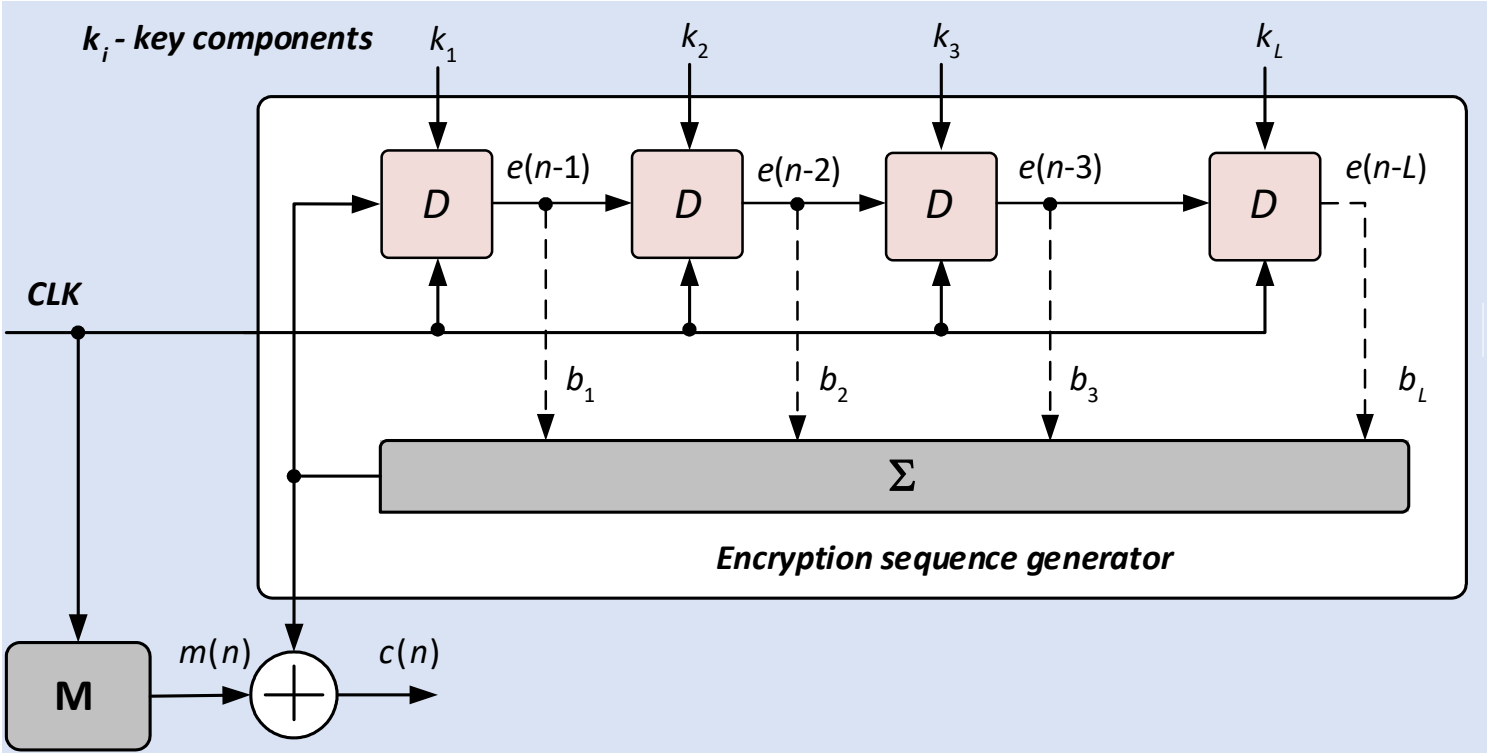
- **Pros:**
  - **each bit is ciphered separately (no delay).**
  - **error affects only one-character transformation (small error spreading).**
- **Cons: information transferred by one character of the plaintext is transformed only into one character of ciphertext.**

Stream Encryption Systems



PRBS generator: shift register with latches, linear feedbacks and parallel pre-loading of a key.

Stream cipher generator



- M: message generator.
- *D*: delay
- *CLK*: clock

4.3 Public key cryptosystem (PKC)

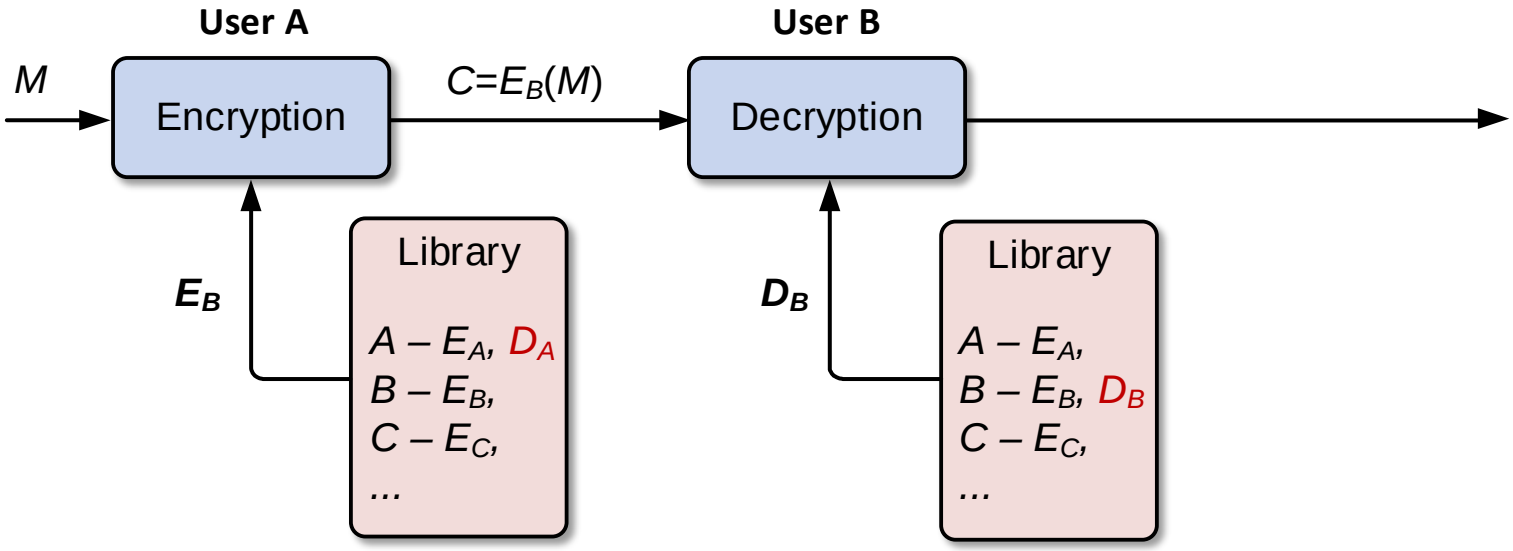
- **Introduced in 1976 by *Diffie* and *Hellman.***
- **Utilizes two different keys. One for encryption – public key E_k and the other for decryption – private key D_k.**
- **Encrypted C and decrypted M messages are given by $C = E_k(M)$, $M = D_k(C)$.**

PKC Features:

- **Encryption algorithm and public key are revealed.**
- **Private key must be kept in secrecy.**
- **Keys E_k and D_k are inverse transformations of plaintext M and ciphertext C, $C = E_k(M)$ and $M = D_k(C)$, $E_k^{-1}(X) = D_k(X)$.**
- **Derivation of D_k from E_k is difficult (practically impossible). For example trapdoor one-way functions $y = x^5 + 12x^3 + 107x + 123$, $y = f(x)$ is easy defined but the derivation $x = f(y)$ is difficult to reveal.**
- **The theoretical basis of encryption is complicated, while ciphering is relatively easy.**

4.3 Public key cryptosystem (PKC)

Authorization (more complicated but ensures greater security)



1. **User A** creates a ciphertext C from a message M : $S=D_A(M) \Rightarrow C=E_B(S)=E_B[D_A(M)]$.
2. **User B** deciphers it $D_B\{E_B[D_A(M)]\}= D_A(M)$.
3. **User B** compares known message M and $E_A[D_A(M)]=M$. In case they match, user A is authorized.

4.3 Public key cryptosystem (PKC)

El Gamal: **Security is based on the difficulty of discrete logarithms calculation (finding x in relation $y = g^x \bmod p$)**

Key calculation

1. **Selection of a prime number p, so that:** $M < p$
2. **Choice of a *private key* D and a part of a *public key* g**
3. **Calculation of a part of the public key** $y = g^D \bmod (p)$

The public key is a triplet: $E = (p, g, y)$

The ciphertext is a pair: $C = (a, b)$

Encryption, decryption

1. **Choice of a random constant k so that:** $gcd[p\text{-}1, k] = 1$
2. **Calculation of a and b:** $a = g^k \bmod (p)$, $b = y^k M \bmod (p)$
3. **The constant k has to be kept in secrecy**
4. **Decryption procedure:** $M = (b/a^D) \bmod (p)$

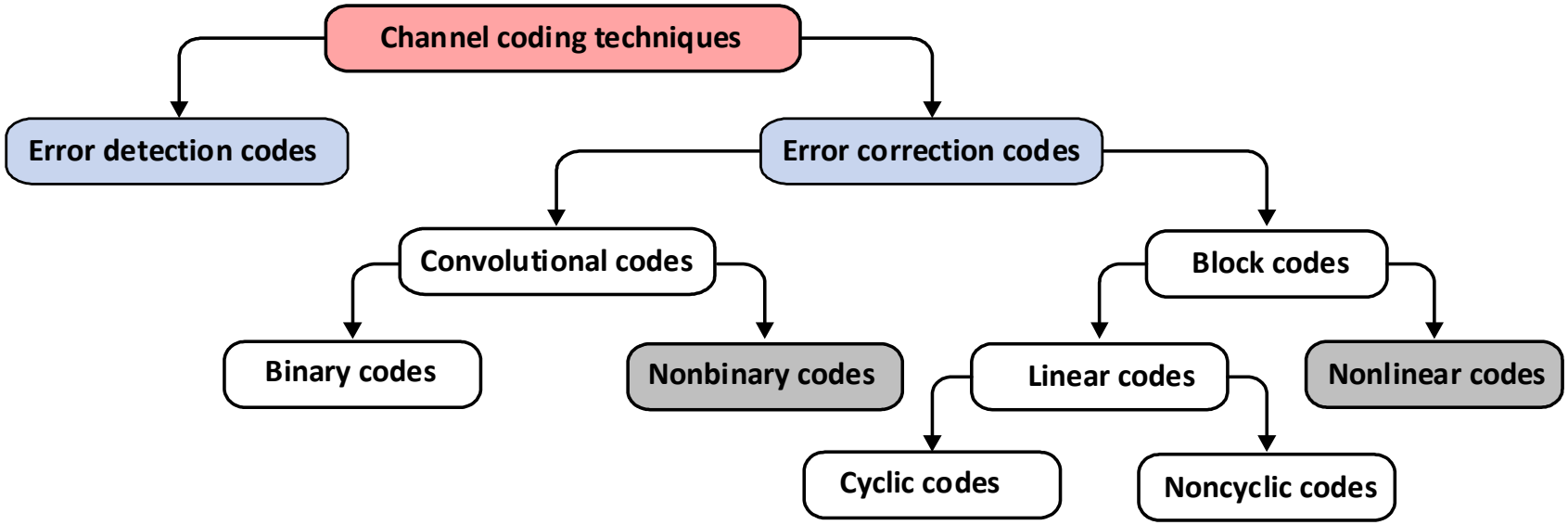
Proof:

$$\frac{b}{a^D} \bmod (p) = \frac{y^k M}{g^{Dk}} \bmod (p) = \frac{g^{Dk} M}{g^{Dk}} \bmod (p) = M \bmod (p) = M$$

5. CHANNEL CODING

Class of signal transformations designed in order to improve communications performance by enabling the transmitted signals to be better immune to the effects of various channel impairments, such as noise, interference, and fading.

5.1 Overview of channel codes



Error correction codes are designed for:

1. **Correction of single independent errors (radio channels without fading).**
2. **Correction of clustered errors (bursts) (data transfer using telephone lines).**

5.2 Channel code characteristics

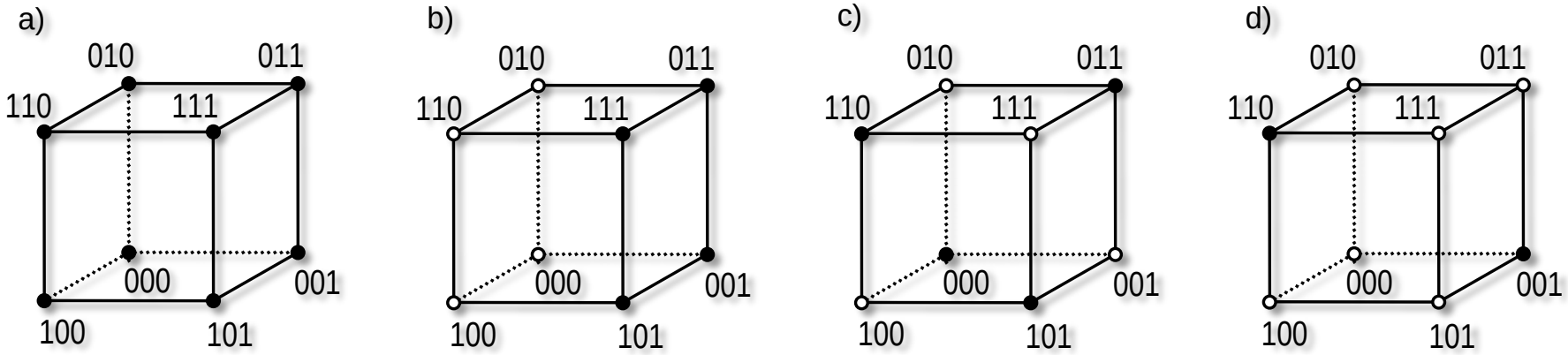
Code rate: $R = \dfrac{\text{number of message bits}}{\text{number of encoded bits}}$

Code redundancy: CR = *number of encoded bits - number of message bits.*

Hamming weight $w(u)$ of a codeword u: the number of nonzero elements in u.

Hamming distance d between two codewords u and v, denoted $d(u, v)$, is defined by the number of elements in which they differ. For example let $u = 10010$, $v = 01011$ then $d(u,v) = 3$ or $d(u,v) = w(u \oplus v) = w(11001) = 3$.

Minimum Hamming distance d_{min}: smallest d between all the codewords.



$d_{min} = 1$ $d_{min} = 1$ $d_{min} = 2$ $d_{min} = 3$

5.3 Code error detecting and correcting capability

Maximum number of guaranteed observable errors per codeword for given d_{min}:

$$k_z = d_{\min} - 1$$

Maximum number of guaranteed correctable errors per codeword:

For d_{min} odd

$$k_o = \frac{d_{\min} - 1}{2}$$

For d_{min} even

$$k_o = \frac{d_{\min} - 2}{2}$$

5.4 Basic codes

Codes *k* from *n*: each code-word contains just *k* ones.

Simple parity codes: parity character is chosen so that the number of ones in code-word is either even or odd (odd is better for synchronization).

Decoding – sum of the bits modulo 2 (XOR).

Iterative codes: double application of simple parity code.

$d_{\min} = 2$

0	0	0	1	1
0	0	1	0	1
0	1	0	0	1
1	0	0	0	1
0	0	1	1	0
0	1	0	1	0
1	0	0	1	0
0	1	1	0	0
1	0	1	0	0
1	1	0	0	0

$d_{\min} = 4$

1	1	0	0
0	0	1	1
1	0	0	1
0	1	0	1
0	0	1	1

5.5 Linear block codes (LBC)

General coding procedure: a block of k message digits (a message vector) is transformed into a longer block of n codeword digits (a code vector) constructed from a given alphabet of elements (usually 0 and 1) using $p = n - k$ parity (guard) digits.

Linear block code definition: subset of vectors assigned to a code-words forming a vector subspace. A subset S of the vector space is called a subspace if the two following conditions are met:

1. The all-zeros vector is in S.
2. The sum of any two vectors in S is also in S (known as the *closure* property).

Basis of the subspace: the smallest linearly independent set of vectors which spans the subspace.

Dimension of the subspace: number of vectors in the basis set

Minimum Hamming distance d_{min}: Hamming weight of the vector (except all zeros vector) with minimum number of ones.

5.5.1 Generator and parity-check matrix

Generator matrix G: $(k \times n)$ **matrix whose rows are equal to the subspace basis vectors.**

$$\mathbf{G} = \begin{bmatrix} \mathbf{v_1} \\ \mathbf{v_2} \\ \vdots \\ \mathbf{v_k} \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}$$

Example:

$$\mathbf{G} = \begin{Vmatrix} \mathbf{v_1} \\ \mathbf{v_2} \\ \mathbf{v_3} \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{Vmatrix}$$

The codewords are formed by linear combinations of the G matrix rows.

$\mathbf{u} = m_1\mathbf{v_1} + m_2\mathbf{v_2} + \cdots + m_k\mathbf{v_k}$, $\quad \mathbf{m} = m_1, m_2, \ldots, m_k$: **message bits (data word)**

For each $(k \times n)$ **generator matrix G, there exists an** $(n - k) \times n$ **parity-check matrix H, such that the rows of G are orthogonal to the rows of H is,** $\mathbf{GH^T = 0}$.

If $\mathbf{vH^T = 0}$, **vector v is a codeword of the subspace S.**

In our example H is:

$$\mathbf{H} = \begin{Vmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{Vmatrix}$$

5.5.1 Generator and parity-check matrix

Systematic block code: code where the message and parity bits are separated.

Any matrix $\mathbf{G}$ can be converted to the form: $\mathbf{G} = [\mathbf{I}_k|\mathbf{P}]$ (see below) by

- interchanging the rows (the code will not change)
- adding any row to another row (the code will not change)
- interchanging the columns (a different code with the same properties will be created)

$$\mathbf{G} = [\mathbf{I}_k|\mathbf{P}] = \left[\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & p_{11} & \cdots & p_{1,(n-k)} \\ 0 & 1 & \cdots & 0 & p_{21} & \cdots & p_{2,(n-k)} \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & p_{k1} & \cdots & p_{k,(n-k)} \end{array}\right]$$

$\mathbf{I}_k$ is a unit matrix of the $k \times k$ size

Codeword vectors:

$$\mathbf{u} = \mathbf{mG} \qquad \mathbf{u} = \underbrace{m_1, m_2, \cdots, m_k}_{\text{Message bits}}, \underbrace{p_1, p_2, \cdots, p_{n-k}}_{\text{Parity bits}}$$

For a systematic code, the orthogonality condition is satisfied if the matrix $\mathbf{H}$ components are in the form $\mathbf{H} = [-\mathbf{P}^T|\mathbf{I}_{n-k}]$.

5.5.1 Generator and parity-check matrix

Example:

$$\mathbf{G} = \left\|\begin{array}{ccc:cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right\| \qquad \mathbf{H} = \left\|\begin{array}{ccc:cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right\|$$

The codeword **u** for a message vector (dataword) **m** is **u = mG**

Example:

$$\underbrace{\begin{Vmatrix} 1 & 0 & 1 \end{Vmatrix}}_{\mathbf{m}} \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{Vmatrix} = \begin{Vmatrix} 1+0+0 & 0+0+0 & 0+0+1 & 0+0+1 & 1+0+1 \end{Vmatrix} =$$

$$= \underbrace{\begin{Vmatrix} 1 & 0 & 1 \end{Vmatrix}}_{\mathbf{m}} \begin{Vmatrix} 1 & 1 \end{Vmatrix}$$

The dataword appears unaltered in the codeword!

Nonsystematic block code: **code where the message and parity bits are not separated but mixed. Other encoding methods are used.**

5.5.1 Generator and parity-check matrix

Syndrome of a linear code

If a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ has been sent and the vector $\mathbf{r} = \mathbf{u} + \mathbf{e}$, where $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ is an **error vector**, has been received, then, the occurrence of an error can be identified by the code syndrome $\mathbf{S}$ (only if $\mathbf{S} \neq \mathbf{0}$) given by

$$\mathbf{S} = \mathbf{r}\mathbf{H}^{\mathbf{T}} = (\mathbf{u} + \mathbf{e})\mathbf{H}^{\mathbf{T}} = \underbrace{\mathbf{u}\mathbf{H}^{\mathbf{T}}}_{=0} + \mathbf{e}\mathbf{H}^{\mathbf{T}} = \mathbf{e}\mathbf{H}^{\mathbf{T}}$$

Because each possible error corresponds to a different error vector $\mathbf{e}$, the error position in the corrupted codeword can be determined by the product $\mathbf{e}\mathbf{H}^{\mathbf{T}}$, but the parity-check matrix must meet the following conditions:

- Any column of the matrix H must not be zero, otherwise an error at the position corresponding to the position of this zero vector would not be detectable.
- Any column of the matrix H must be unique, otherwise the position of the error would not be unambiguous for two identical vectors **e.**

5.5.2 Hamming codes (HC)

- **Class of block codes characterized by the structure** $(n, k) = (2^p - 1, 2^p - 1 - p)$.
- **Typical examples: HC (7,4), HC (15,11) and HC (31,26).**
- **Capable of correcting all single errors** $(d_{min} = 3)$.
- **Encoding/decoding techniques are based on the equation** $\mathbf{vH^T = 0}$.

Hamming code (7,4)

Code rate: $R = k/n = 4/7$, **Parity-check matrix:**

$$\mathbf{H} = \begin{Vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{Vmatrix}$$

Encoding message

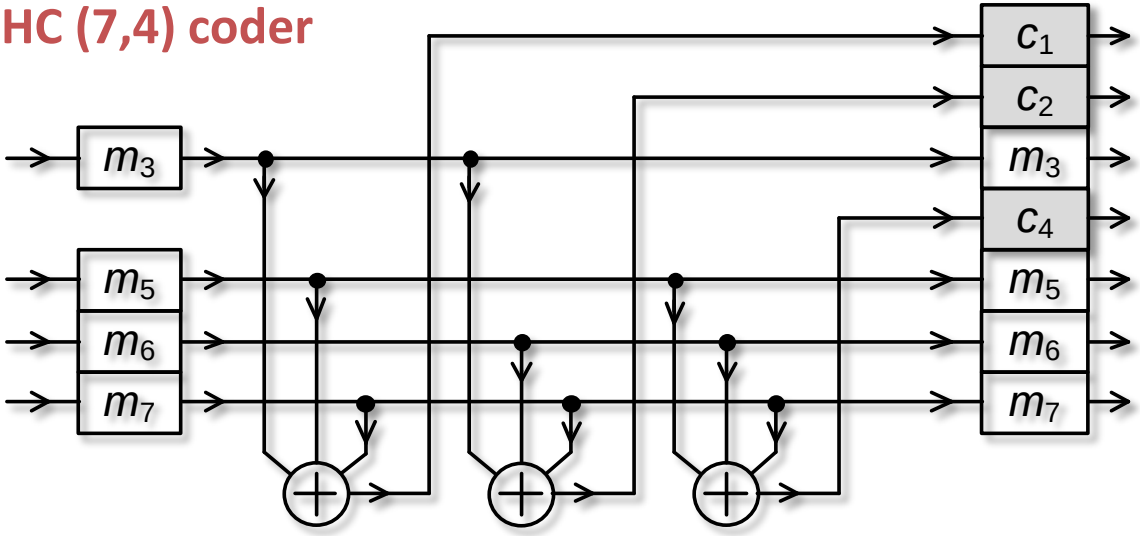
m = $[m_3, m_5, m_6, m_7]$:

$$[c_1 \quad c_2 \quad m_3 \quad c_4 \quad m_5 \quad m_6 \quad m_7] \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [0 \quad 0 \quad 0]$$

5.5.2 Hamming codes (HC)

$$c_4 + m_5 + m_6 + m_7 = 0 \Rightarrow c_4 = m_5 + m_6 + m_7$$
$$c_2 + m_3 + m_6 + m_7 = 0 \Rightarrow c_2 = m_3 + m_6 + m_7$$
$$c_1 + m_3 + m_5 + m_7 = 0 \Rightarrow c_1 = m_3 + m_5 + m_7.$$

HC (7,4) coder



Example: $\mathbf{m}$ = [0 0 0 1] $\Rightarrow$ $c_1 = c_3 = c_4 = 1$ $\Rightarrow$ $\mathbf{c}$ = [1 1 0 1 0 0 1]

Codeword decoding

Previous example: $\mathbf{m}$ = [0 0 0 1] $\Rightarrow$ $c_1 = c_3 = c_4 = 1$ $\Rightarrow$ $\mathbf{c}$ = [1 1 0 1 0 0 1]
Let us have error at the third position: $\mathbf{c}$ = [1 1 1 1 0 0 1]

5.5.2 Hamming codes (HC)

Syndrome calculation:

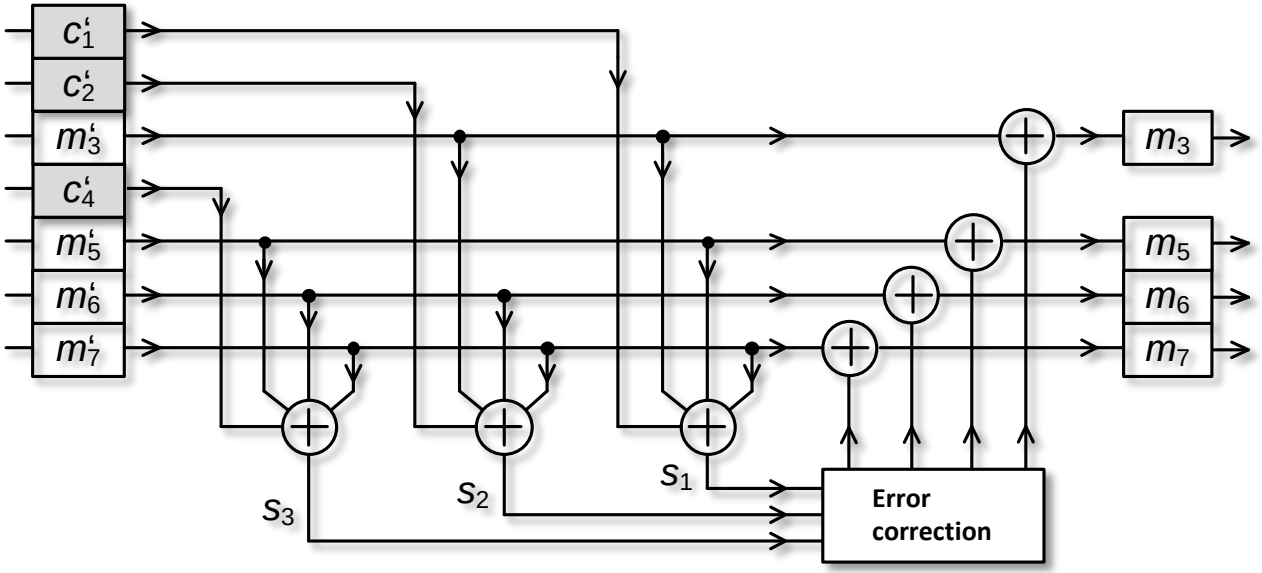
$$\begin{bmatrix}1 & 1 & 1 & 1 & 0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 0\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\end{bmatrix} = \begin{bmatrix}0 & 1 & 1\end{bmatrix}$$

Syndrome = 3

$\Rightarrow$ **error at third position.**

After correction we have: $\mathbf{c} = \begin{bmatrix}1 & 1 & 0 & 1 & 0 & 0 & 1\end{bmatrix}$

HC (7,4) decoder



5.5.3 Cyclic codes (CC)

- **Subclass of linear block codes.**
- **Easily implemented with feedback shift registers.**
- **If the codeword $\mathbf{u} = [u_{n-1}, u_{n-2}, \ldots, u_0]$ is a codeword in subspace S, then $\mathbf{u}^{(1)} = [u_{n-2}, u_{n-3}, \ldots, u_0, u_{n-1}]$ obtained by an end-around shift is also a codeword in S.**
- **Components of a codeword are treated as the coefficients of a polynomial $u(x)$**
- **Cyclic code is most frequently generated using a generator polynomial $g(x)$.**

Encoding message:

1. **We express message vector $\mathbf{m}$ in polynomial form, as follows**

$$\mathbf{m} = [m_{k-1}, m_{k-2}, \ldots, m_0] \Rightarrow m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + m_1x^1 + m_0x^0 = \sum_{i=0}^{k-1} m_i x^i$$

2. **We multiply $m(x)$ by x^{n-k}. We get the left-shifted message polynomial.**

$$z(x) = x^{n-k}m(x) = m_{n-1}x^{n-1} + m_{n-2}x^{n-2} + \cdots + m_{n-k}x^{n-k}.$$

3. **We next divide $z(x)$ by $g(x)$. The result containing quotient $q(x)$ and remainder $r(x)$ of degree $n - k - 1$ or lower can bed expressed as**

$$\frac{z(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

4. **Finally we generate codewords $u(x)$ by adding $u(x) = r(x) + z(x)$**

Note: **the generator polynomial $g(x)$ degree is of the order n-1 or lower and the polynomial $x^n - 1$ has to be divisible by $g(x)$.**

Codeword decoding

1. **We divide received codeword $u'(x)$ by generator polynomial**

$$\frac{u'(x)}{g(x)} = \frac{u(x) + e(x)}{g(x)} = q(x) + \frac{s(x)}{g(x)}$$

2. **Remainder $s(x)$ of degree $n - k - 1$ or lower is codeword syndrome**
3. **If the vector s corresponding to the $s(x)$ coefficients fulfils condition**
   - $w(s) = 0$ **(all-zero syndrome) codeword is error-free** ($s(x)$ is *aliquot*).
   - $w(s) \geq 1$ **codeword is affected by error. We will use some of error correcting methods (see examples in seminary).**

5.5.3 Cyclic codes (CC)

Coding example:

Encode message $m = [1\ 1\ 1\ 0]$ using the CC(7, 4). The generator polynomial is: $g(x) = x^3 + x + 1$.

1. $m(x) = x^3 + x^2 + x$

2. $z(x) = x^{n-k} m(x)$

$= x^3(x^3 + x^2 + x) = x^6 + x^5 + x^4$

3.

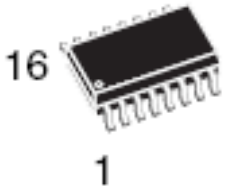
$$\begin{array}{rl} x^6 + x^5 + x^4 & : x^3 + x + 1 = x^3 + x^2 \\ \underline{x^6 + x^4 + x^3} & = g(x) \quad = q(x) \\ x^5 + x^3 & \\ \underline{x^5 + x^3 + x^2} & \\ x^2 & = r(x) \end{array}$$

4. $u(x) = z(x) + r(x) = x^6 + x^5 + x^4 + x^2$

Most often CC application: *Cyclic redundancy check* (CRC) - error-detecting code commonly used in digital, telecom and broadcast networks (TCP/IP, CAN, DAB,…) and storage devices to detect accidental changes to raw data.

Most often $g(x)$ lengths $l = n - k + 1$ are: 9 bits (CRC-8) 17 bits (CRC-16) 33 bits (CRC-32), 65 bits (CRC-64)

ISO14443 type-B contactless coupler chip with anti-collision and CRC management



5.5.4 BCH Codes

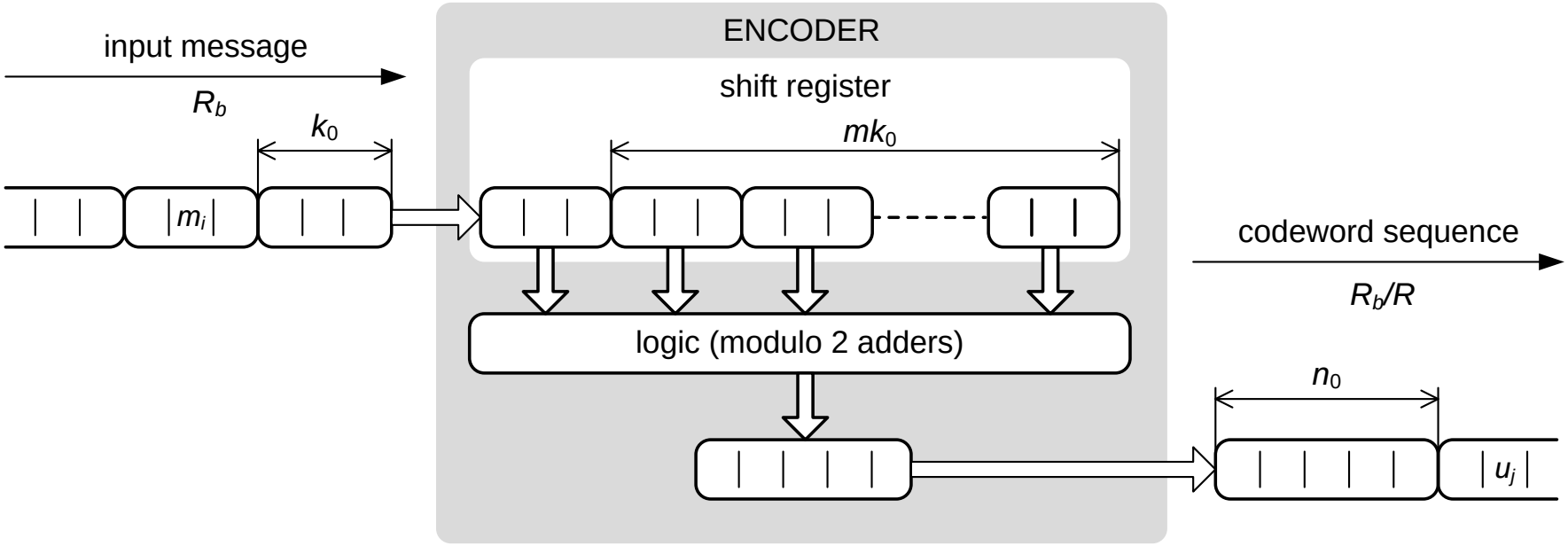
- **Bose-Chadhuti-Hocquenghem (BCH) codes are powerful class of cyclic codes that provide a large selection of block lengths, code rates, alphabet sizes, and error correcting capability.**
- **At block lengths of a few hundreds symbols, the BCH codes outperform all other block codes with the same block length and code rate.**
- **The most commonly used BCH codes employ a binary alphabet and a codeword block length of $n = 2^{p-1}$. where $p = 3, 4, \ldots$.**

5.5.5 Reed-Solomon codes

- **Special subclass of the nonbinary BCH codes (the discovery of which preceded the BCH codes) with symbols made up of t-bit sequences, where $m > 2$.**
- **Capable of correcting $p/2$ Bytes (symbols) or $pt = n - k$ bits, where p is a number of parity bits, $n = 2^t - 1$, k is a number of message bits, and *t* is a number of bits per symbol).**
- **Suitable for interleaving and concatenated codes.**
- **Application: NASA/ESA standard for space, record/reading CD, DMB.**

5.5.6 Convolutional codes

Type of error-correcting code in which each k_0 - bit information symbol is transformed into an n_0 - bit symbol. Input data stream is encoded continuously.



A convolutional code is described by following integers:

- **Constraint length: number of m-bit shifts over which a single information bit can influence the encoder output.**
- **Code rate (information per coded bit): $R = k_0/n_0$.**
- **Message block length: $k = (m+1)\,k_0$.**
- **Codeword block length: $n = (m+1)\,n_0$.**

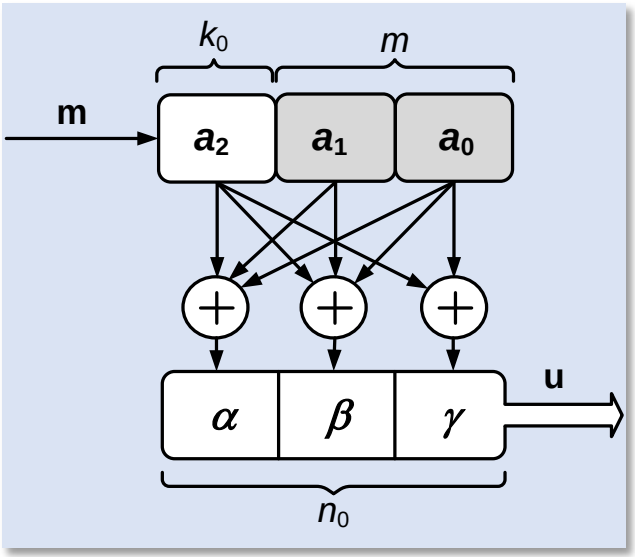
5.5.6 Convolutional codes

Convolutional encoding

Example: $k_0 = 1, m = 2, n_0 = 3$

Input message $\leftarrow$ **1011**

Convolutional encoder - example

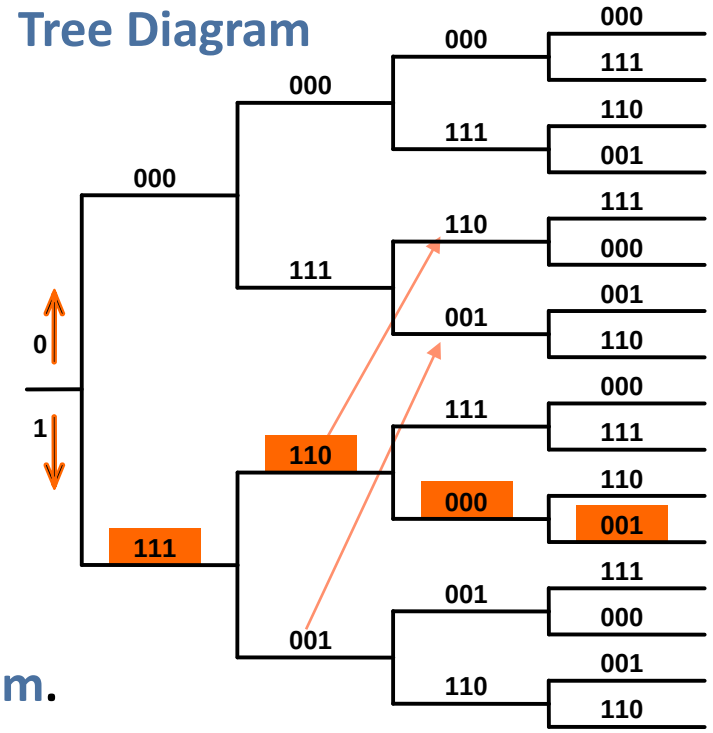


- **If the input bit is a zero/one, we go to the next rightmost branch in the up/downward direction.**
- **For L input symbols we have at L-th step 2^L branches and 2^m different states - trellis diagram.**

Encoding table

	a_2	a_1	a_0	α	β	γ
0	0	0	0	-	-	-
1	1	0	0	1	1	1
2	0	1	0	1	1	0
3	1	0	1	0	0	0
4	1	1	0	0	0	1

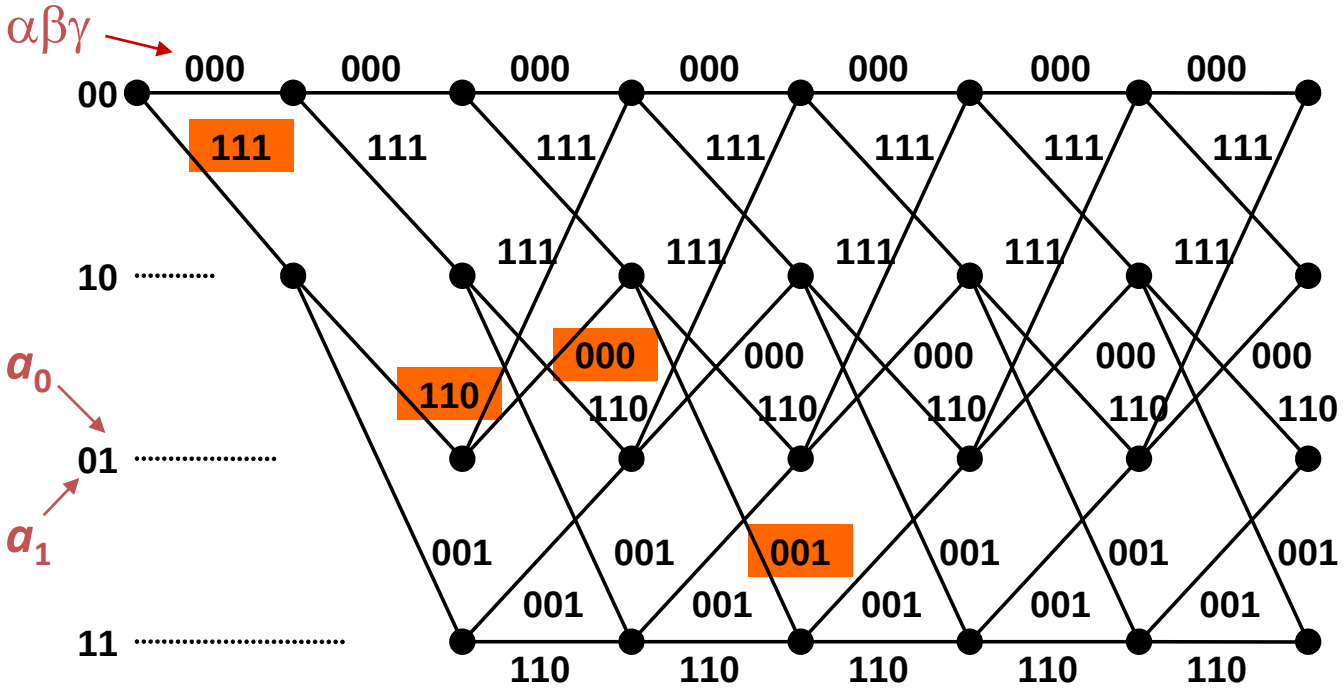
Tree Diagram



Viterbi optimal decoding

- **Comparing the received sequence of bits possibly disturbed by errors with all of sequences that can be sent.**
- **The comparison is based on a calculating the likelihood ratio and its maximization (*maximum likelihood decoding*).**

Trellis diagram



5.5.6 Convolutional codes

Viterbi decoder calculates the Hamming distance of each received block of the length n_0 with all possible branch sequences. In the framework of a specific finite length segment (window) only the most likely paths are preserved.

An example of Viterbi decoding:

Encoder input: **1 0 1 1 0 0 0**

Encoder output: **111 110 000 001 001 111 000**

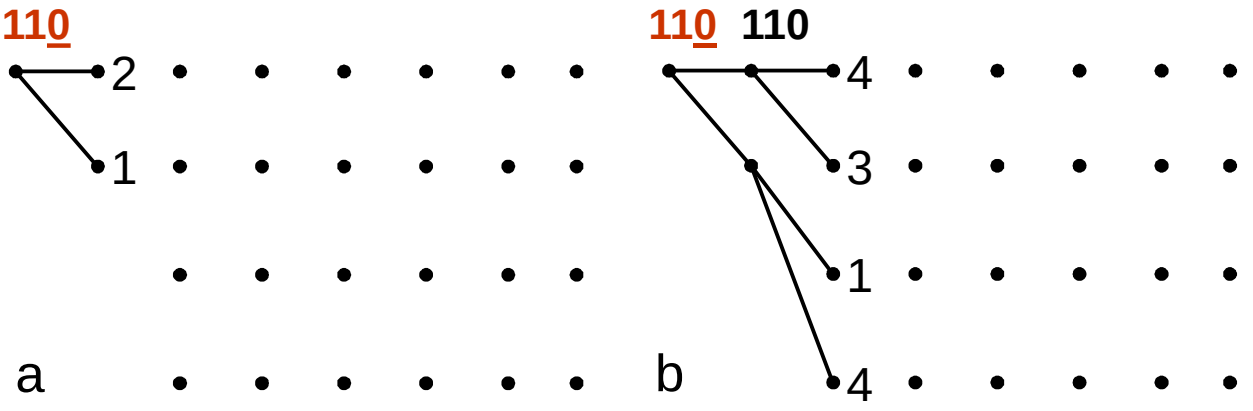
Decoder input: **110 110 001 101 001 110 000**

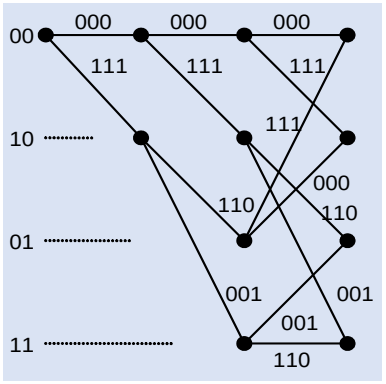
This sequence does not match any possible path in the trellis diagram.

First received block: 110

Possible branches: 000, 111

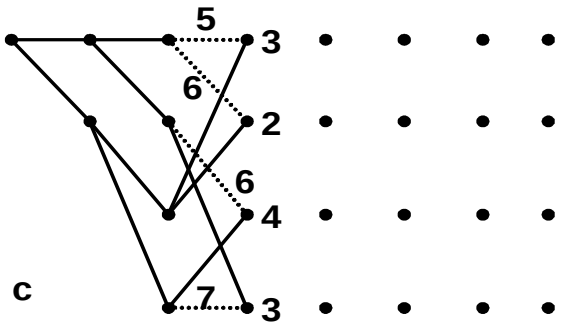
Corresponding distances: $d = 2$ (for 000) and $d = 1$ (for 111) etc. Distances are accumulated, the path with the least total d prevails.



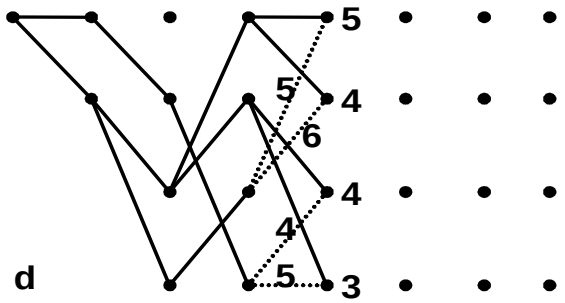


5.5.6 Convolutional codes

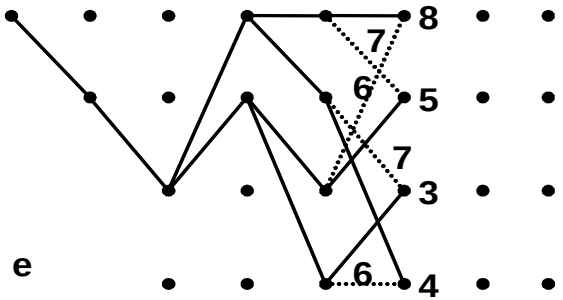
110 110 001



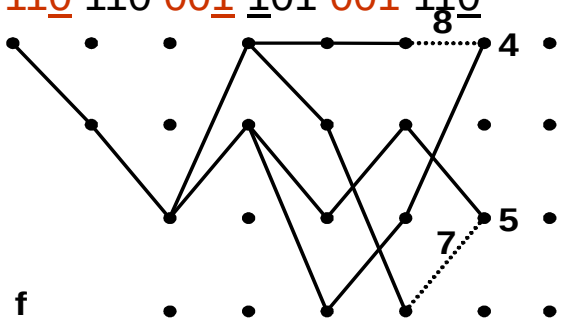
110 110 001 101



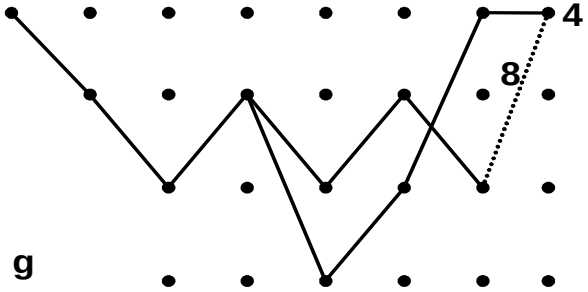
110 110 001 101 001

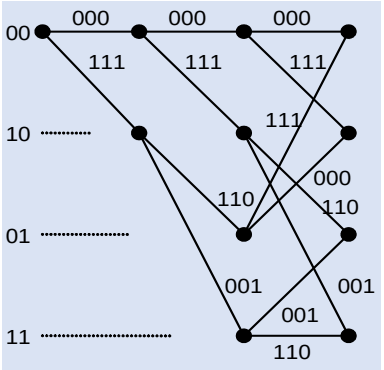


110 110 001 101 001 110



110 110 001 101 001 110 000





5.5.7 LDPC (*Low Density Parity-check*) codes

- **Introduced by Gallager in his PhD thesis in 1960**
- **Class of linear block codes**
- **Parity-check matrix contains only a few 1's**
- **Suited for implementations that make heavy use of parallelism**

Representations for LDPC codes

1. **Matrix representation**
2. **Graphical representation**

As for 1: **Parity check matrix** with dimension $n \times m$. Example for a (8, 4) code:

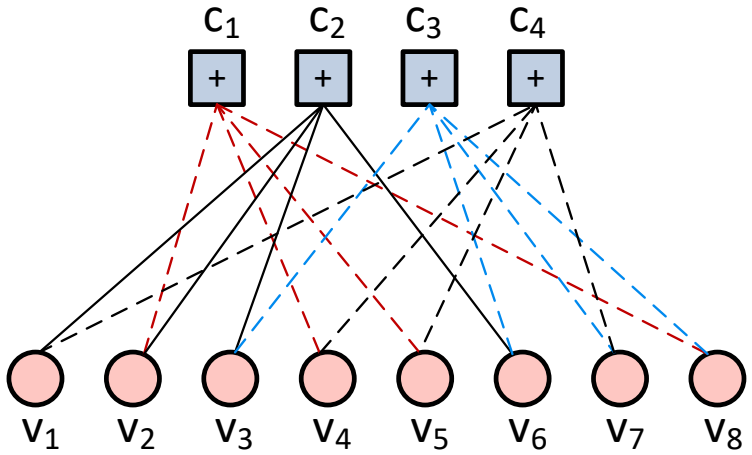
$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

As for 2: Effective graphical representation is known as ***Tanner graph*****.** It

- provides a complete representation of the code,
- helps to describe the decoding algorithm, and
- contains the two types of nodes called variable nodes (*v*-nodes) and check nodes (*c*-nodes).

5.5.7 LDPC (*Low Density Parity-check*) codes

- The number of *c-nodes* corresponds to the number of rows k. The number of *v-nodes* corresponds to the number of columns n.
- The one in the matrix corresponds to the connection of the corresponding *c-node* with the *v-node*.
- ***v-nodes:*** correspond to the transmitted bit sequences.
- ***c-nodes:*** are control nodes. The number of ones entering the node must be even (even parity check is performed).

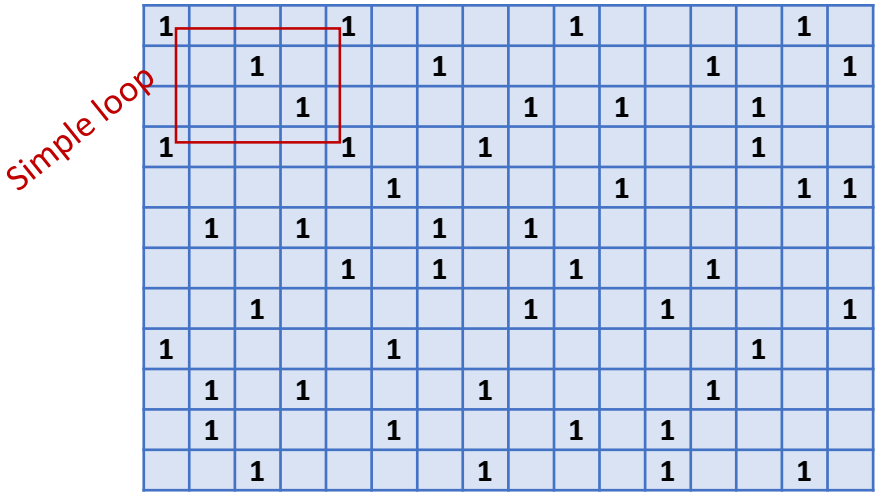


$$H = \begin{array}{c|cccccccc} & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ c_1 & & 1 & & 1 & 1 & & & 1 \\ c_2 & 1 & 1 & 1 & & & 1 & & \\ c_3 & & & 1 & & & 1 & 1 & 1 \\ c_4 & 1 & & & 1 & 1 & & 1 & \end{array}$$

5.5.7 LDPC (*Low Density Parity-check*) codes

Parity check matrix random construction

- **Each row of the matrix $\mathbf{H}$ must contain a constant number w_r of 1's,**
- **Each column of the matrix must contain a constant number w_c of 1's**
- **The matrix must be sparse,**
- **Any two rows in the matrix must be linearly independent,**
- **There must be no cycles in the matrix (see simple loop).**



5.5.7 LDPC (Low Density Parity-check) codes

LDPC encoding

It is performed in blocks of size $\mathbf{m} = [m_1, m_2, \ldots, m_k]$: $\mathbf{y} = \mathbf{mG}$. The matrix $\mathbf{G}$ is obtained from the matrix $\mathbf{H}$ as $\mathbf{G} = [\mathbf{I_k}|\mathbf{P}] = [\mathbf{m}|\mathbf{mP}]$. The matrix $\mathbf{H}$ is created by a random construction, a geometric construction (similar to the creation of a cyclic code - cyclic shift of lines), or by means of a Gallager parity matrix, etc.

LDPC hard decoding

Based on the exchange of messages between *c-nodes* with *v-nodes* of the Tanner graph.

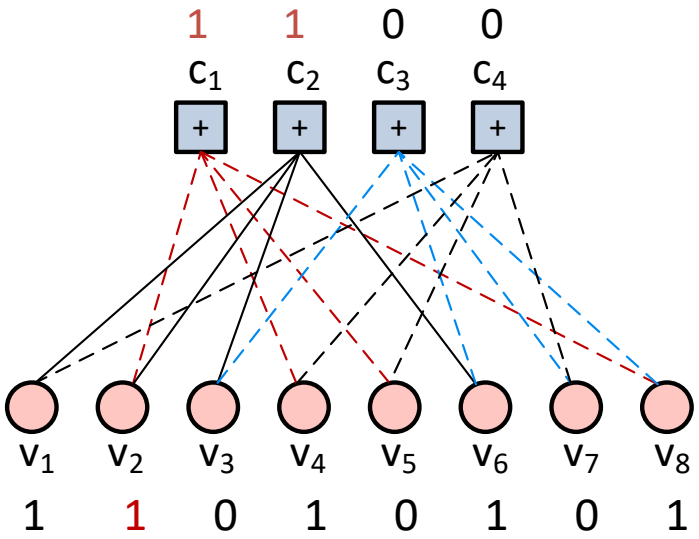
Decoding procedure:

1. *v-nodes* send their values to the corresponding *c-nodes*.
2. *c-nodes* perform parity check.
   - Check OK $\Rightarrow$ *c-nodes* return to the *v-nodes* the same value.
   - Wrong parity $\Rightarrow$ *c-nodes* return to the *v-nodes* an opposite value.
3. *v-nodes* update their values according to messages from the *c-nodes.*
4. Steps 1 to 3 are repeated.

5.5.7 LDPC (Low Density Parity-check) codes

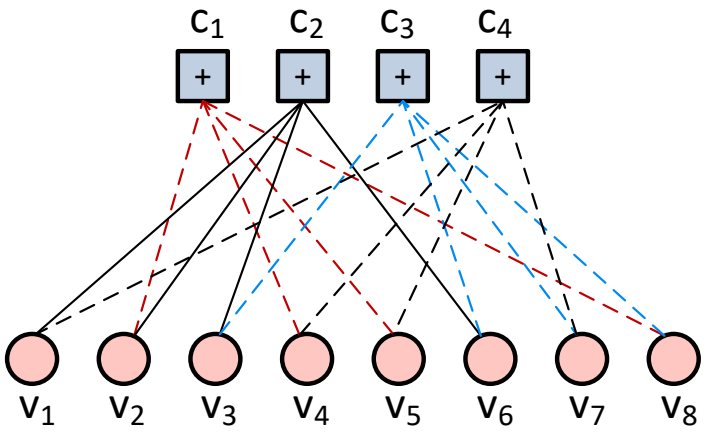
***Example*:** Let the sequence **y** = [1 0 0 1 0 1 0 1] be sent and **y'**= [1 1 0 1 0 1 0 1] be received. Correct the sequence.

$$H = \begin{array}{c|cccccccc} & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\ c_1 & & 1 & & 1 & 1 & & & 1 \\ c_2 & 1 & 1 & 1 & & & 1 & & \\ c_3 & & & 1 & & & 1 & 1 & 1 \\ c_4 & 1 & & & 1 & 1 & & 1 & \end{array}$$



c_1	*received*	$v_2 \to 1$	$v_4 \to 1$	$v_5 \to 0$	$v_8 \to 1$
	sent	$0 \to v_2$	$0 \to v_4$	$1 \to v_5$	$0 \to v_8$
c_2	*received*	$v_1 \to 1$	$v_2 \to 1$	$v_3 \to 0$	$v_6 \to 1$
	sent	$0 \to v_1$	$0 \to v_2$	$1 \to v_3$	$0 \to v_6$
c_3	*received*	$v_3 \to 0$	$v_6 \to 1$	$v_7 \to 0$	$v_8 \to 1$
	sent	$0 \to v_3$	$1 \to v_6$	$0 \to v_7$	$1 \to v_8$
c_4	*received*	$v_1 \to 1$	$v_4 \to 1$	$v_5 \to 0$	$v_7 \to 0$
	sent	$1 \to v_1$	$1 \to v_4$	$0 \to v_5$	$0 \to v_7$

5.5.7 LDPC (Low Density Parity-check) codes



v-nodes	**y**	Messages from ***v-nodes***		New **y**
v_1	**1**	$c_2 \to 1$	$c_4 \to 1$	**1**
v_2	**1**	$c_1 \to 0$	$c_2 \to 0$	**0**
v_3	**0**	$c_2 \to 1$	$c_3 \to 0$	**0**
v_4	**1**	$c_1 \to 0$	$c_4 \to 1$	**1**
v_5	**0**	$c_1 \to 1$	$c_4 \to 0$	**0**
v_6	**1**	$c_2 \to 0$	$c_3 \to 1$	**1**
v_7	**0**	$c_3 \to 0$	$c_4 \to 0$	**0**
v_8	**1**	$c_1 \to 1$	$c_3 \to 1$	**1**

Node v_2 sends symbol 1 to c_1 a c_2 and both the nodes return symbol 0, while e.g. v_4 gets the opposite answer only from one node $\Rightarrow$ correction of v_2.

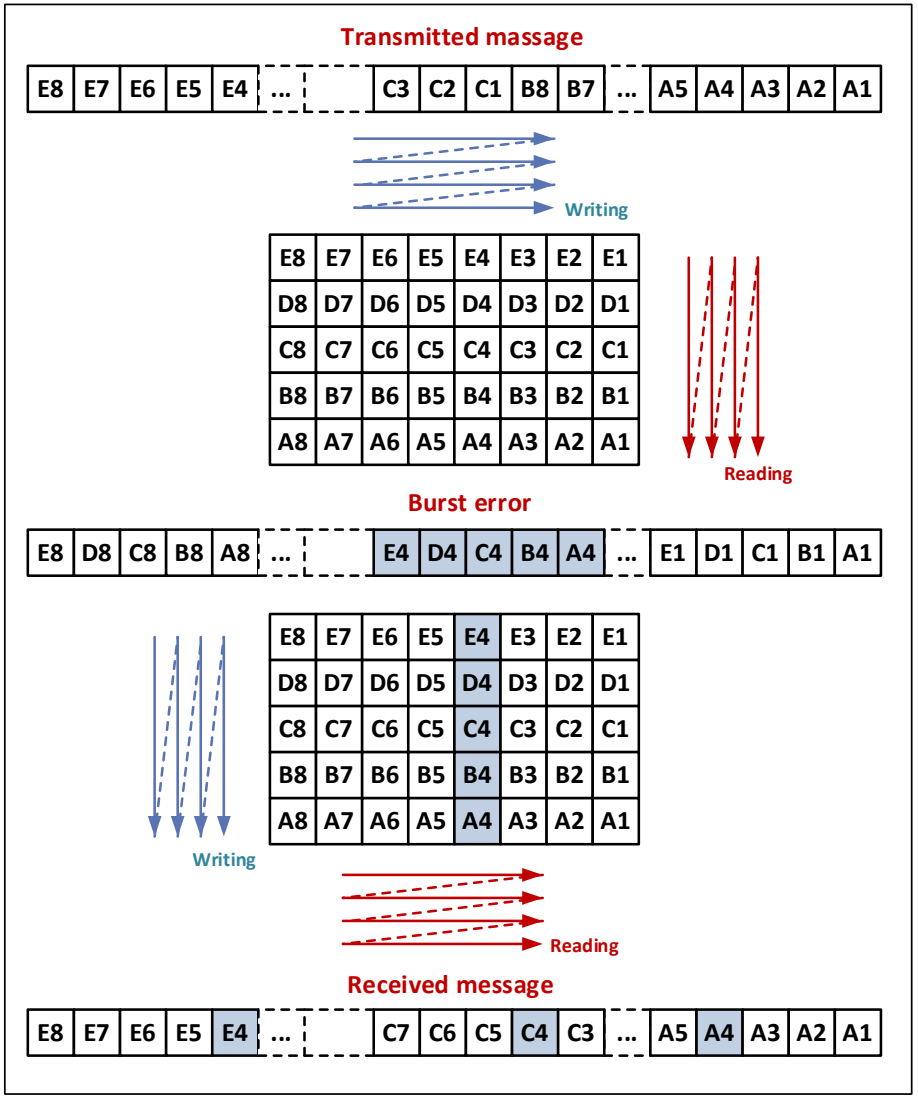
5.5.7 LDPC (Low Density Parity-check) codes

The **low internal complexity** of the LDPC decoder allows it to be used for high-speed applications. For example, 10 Gbit Ethernet (10GBASE-T), optional in Wi-Fi 802.11 standards (specifically 802.11n and 802.11ac), DVB-S2 and DVB-T2 standard.

Signal protection against burst errors (Interleaving)

Encoding and decoding principle

- Encoding a message using a single independent error encoder.
- Filling the rows of an *M*-row-by *N*-column (*M* x *N*) matrix with the encoded sequence.
- Transmission of the column by column read data through the channel.
- Filling the columns of the same matrix with the received data and reading the array row by row.
- Correction of the possible errors using single independent error decoder.
- The largest depth of the interleaving, the longest allowable burst error.



Problems

1. *Consider the **Vigenere key algorithm** and encrypt the message **The moon landing was successful** using the keyword **Apollo.***

2. *Encrypt the same message (as in Example 1) using the **transposition cipher** given by the array dimension of **4×4** cells. Missing characters replace (if necessary) by x.*

3. *For the **El Gamal** encryption algorithm the private key **D = 17**, and part of the public key **g = 5** and **p = 13** are given. Let the symbols of a plain message are encoded by their serial number in the alphabet (A = 1, B = 2, C = 3, ...). What is the ciphertext for the **character H** (chose **k ≥ 10**)? Verify the correctness of the ciphered message by decryption.*

4. *Encode the message **m = [1 0 1 1]** using the **Hamming code (7,4)** defined by the parity check matrix*

$$\mathbf{H} = \begin{Vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{Vmatrix}$$

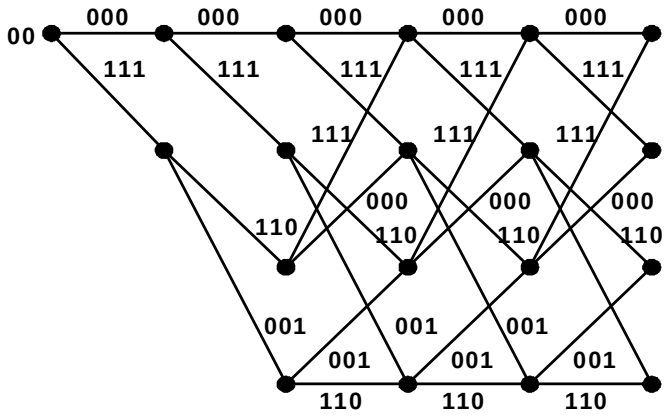
Problems

5. *Consider the **Hamming code (7,4).** Let the codeword **c = [1 1 0 1 0 1 1]** was received at the output of a noisy channel. Check whether the codeword is corrupted. If so, correct it.*

6. *Encode the message **m = [1 1 0 1]** using the **cyclic code (7,4)** defined by the polynomial generator **g(x) = $x^3 + x + 1$**.*

7. *Consider now the same **cyclic code** as in Example 6. Let the codeword represented by the polynomial **c = $x^6 + x^5 + x^4 + x^3 + 1$** was received at the output of a noisy channel. In the case the codeword is corrupted, correct it.*

8. *Let the **convolutional code** is given by the trellis diagram below. Encode the message **m = [1 1 0 1 0 0 1].***



9. *Decode the received bit sequence **c = 111 010 001 000 111 111** using above **convolutional decoder**.*

Problems

As for 1

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Key:	a	p	o	l	l	o	a	p	o	l	l	o	a	p	o	l	l	o	...
Shift:	0	15	14	11	11	14	0	15	14	11	11	14	0	15	14	11	11	14	...
Plain text:	t	h	e	m	o	o	n	l	a	n	d	i	n	g	w	a	s	s	...
Cipher text:	**t**	**w**	**s**	**x**	**z**	**c**	**n**	**a**	**o**	**y**	**o**	**w**	**n**	**v**	**k**	**l**	**d**	**g**	...

As for 2

t	h	e	m
o	o	n	l
a	n	d	i
n	g	w	a

s	s	u	c
c	e	s	s
f	u	l	x
x	x	x	x

Cipher text: **toan hong endw mlia scfx seux uslx csxx**

Problems

As for 3 *H = 8*

$p := 13 \quad g := 5 \quad D := 17 \quad H := 8$

$x := g^{D}$ $\quad x = 762939453125$

$y := \mathrm{mod}(x, p)$ $\quad y = 5$

Zvolim $\quad k := 11$

$\gcd(p - 1, k) = 1$

$a := \mathrm{mod}\left(g^{k}, p\right)$ $\quad a = 8$

$b := \mathrm{mod}\left(y^{k} \cdot H, p\right)$ $\quad b = 12$

Deciphering

$$\frac{b}{a^{D}} \bmod(p) = \frac{12 \bmod(13)}{8^{17} \bmod(13)} = \frac{12}{8} = \frac{12 + 4 \times 13}{8} = \frac{64}{8} = 8$$

Problems

As for 4

$$[c_1 \quad c_2 \quad 1 \quad c_4 \quad 0 \quad 1 \quad 1] \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [0 \quad 0 \quad 0]$$

$$\begin{aligned} c_4 + 0 + 1 + 1 = 0 &\Rightarrow c_4 = 0 \\ c_2 + 1 + 1 + 1 = 0 &\Rightarrow c_2 = 1 \\ c_1 + 1 + 0 + 1 = 0 &\Rightarrow c_1 = 0 \end{aligned}$$

c = [0 1 1 0 0 1 1]

As for 5 ***c*** = [1 1 0 1 0 1 1]

$$[1 \quad 1 \quad 0 \quad 1 \quad 0 \quad \cancel{1} \quad 1] \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [1+1+1 \quad 1+1+1 \quad 1+1] = [1 \quad 1 \quad 0]_2 = (6)_{10}$$

0

Problems

As for 6 $m = [1\ 1\ 0\ 1]$

$g(x) = x^3 + x + 1 \Rightarrow g = [1\ 0\ 1\ 1]$

$$z(x) = x^{n-k} m(x) = x^3\left(x^3 + x^2 + 1\right) = x^6 + x^5 + x^3$$

$z = 1\ 1\ 0\ 1\ 0\ 0\ 0$

$g = \underline{1\ 0\ 1\ 1}$

$0\ 1\ 1\ 0\ 0$

$\underline{1\ 0\ 1\ 1}$

$0\ 1\ 1\ 1\ 0$

$\underline{1\ 0\ 1\ 1}$

$1\ 0\ 1\ 0$

$\underline{1\ 0\ 1\ 1}$

$s = 0\ 0\ 0\ 1$

c = z + s = [1 1 0 1 0 0 1]

As for 7

c' = $x^6 + x^5 + x^4 + x^3 + 1$.

c' = 1 1 1 1 0 0 1

$g = \underline{1\ 0\ 1\ 1}$

$0\ 1\ 0\ 0\ 0$

$\underline{1\ 0\ 1\ 1}$

$0\ 0\ 1\ 1\ 0\ 1$

$\underline{1\ 0\ 1\ 1}$

$s = 0\ 1\ 1\ 0$

$w(s) > 1$

$c'' = 1\ 1\ 1\ 1\ 1\ 0\ 0$

$g = \underline{1\ 0\ 1\ 1}$

$0\ 1\ 0\ 0\ 1$

$\underline{1\ 0\ 1\ 1}$

$0\ 0\ 1\ 0\ 0\ 0$

$\underline{1\ 0\ 1\ 1}$

$s = 0\ 0\ 1\ 1$

$w(s) > 1$

$c''' = 0\ 1\ 1\ 1\ 1\ 1\ 0$

$g = \underline{1\ 0\ 1\ 1}$

$0\ 1\ 0\ 0\ 1$

$\underline{1\ 0\ 1\ 1}$

$s = 0\ 0\ 1\ 0\ 0$

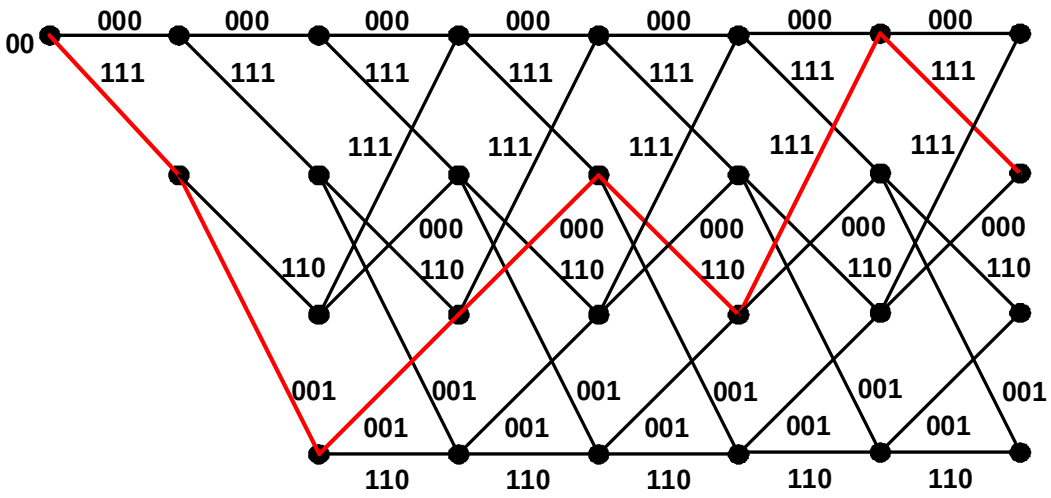
$w(s) = 1$

$c''' + s = 0\ 1\ 1\ 1\ 0\ 1\ 0$

c = [1 1 0 1 0 0 1]

Problems

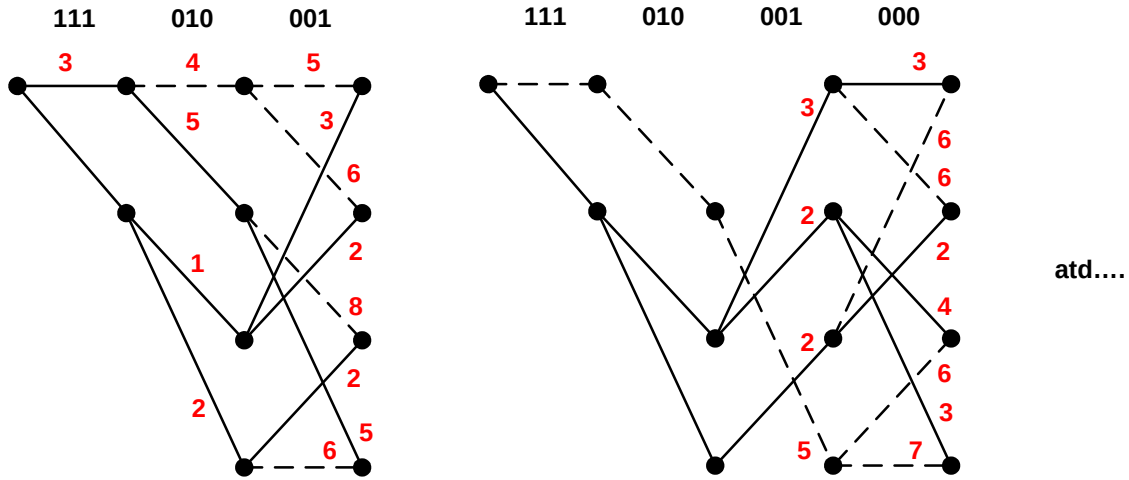
As for 8 *m = [1 1 0 1 0 0 1].*

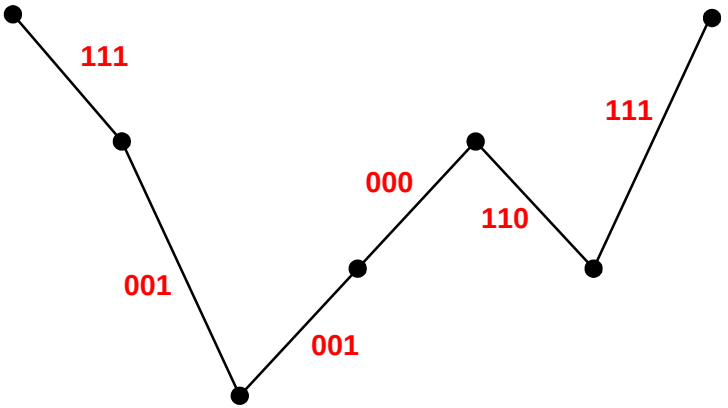


c = [111 001 001 000 110 111 111].

Problems

As for 9 *c' = [111 010 001 000 111 111]*





c = [111 001 001 000 110 111]

6 PULSE (BASEBAND) MODULATION

6.1 Introduction

The goals of a digital communication system (DCS) design

- to maximize transmission bit rate R;
- to minimize probability of bit error P_b;
- to minimize required power (required bit energy to noise power spectral density E_b/N_0);
- to minimize required system bandwidth B_W;
- to maximize system utilization, (to provide reliable service for a maximum number of users with minimum delay and with maximum resistance to interference);
- to minimize system complexity, computational load, and system cost.

The constraints and theoretical limitations of DCS

1. The *Nyquist* theoretical minimum bandwidth requirement.
2. The *Shannon-Hartley* capacity theorem (and the *Shannon* limit).
3. Government regulations (e.g., frequency allocations).
4. Technological limitations (e.g., state-of-the-art components).
5. Other system limitations (e.g., propagation delay, multipath propagation).
6. Other system requirements (e.g., satellite orbits).

6.1 Introduction

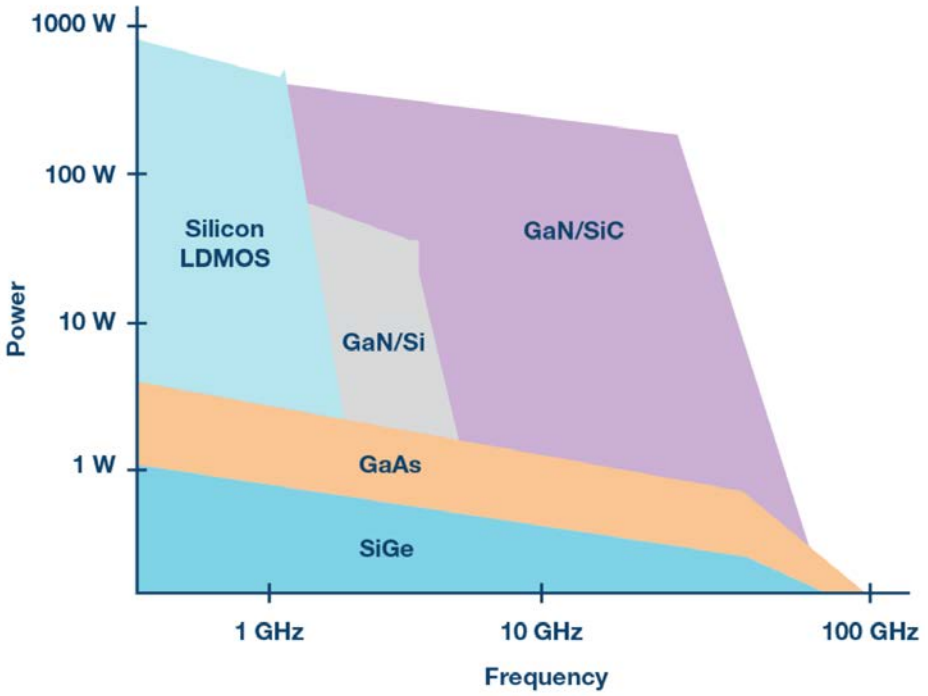
As for 1: The *Nyquist* theoretical minimum bandwidth for the baseband transmission of R_s symbols per second without *inter-symbol interference* (ISI) is $R_s/2$ hertz, $R_s = R/k$, where R is bitrate and k is a number of bits per symbol. In practice, the *Nyquist* minimum bandwidth is expanded by about 10% to 40%, due to the constraints of real filters.

As for 2: The Shannon-Hartley capacity of channel C depends on *signal to noise ratio* (SNR) and bandwidth B:

$$C = B \times \log_2(1 + \mathrm{SNR}).$$

As for 3: See the *National Table of Frequency Allocations*

As for 5: State-of-the-art of semiconductor components



6.1 Introduction

As for 5: ***Propagation delay*** τ **is caused by finite speed of light. Channel frequency response is then**

$$H(f) = K \times e^{j2\pi ft},$$

where K **includes propagation loss and attenuation of the channel.**

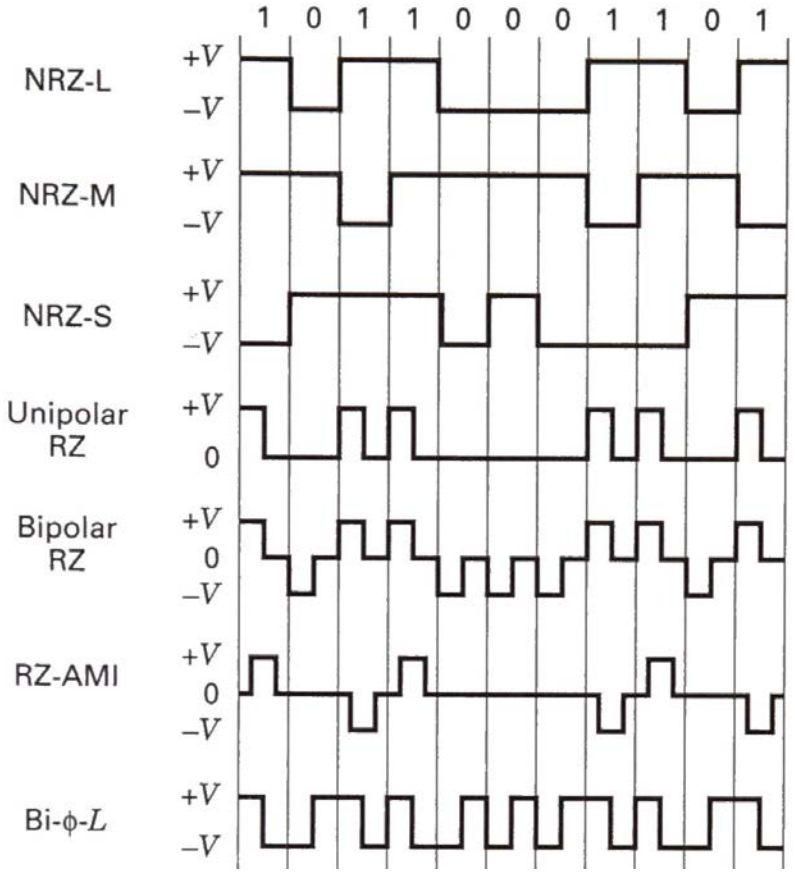
Multipath propagation **results in non-flat frequency response** $H(f)$ **of the channel. It can be compensated using an** ***equalizer*** **with the transfer function**

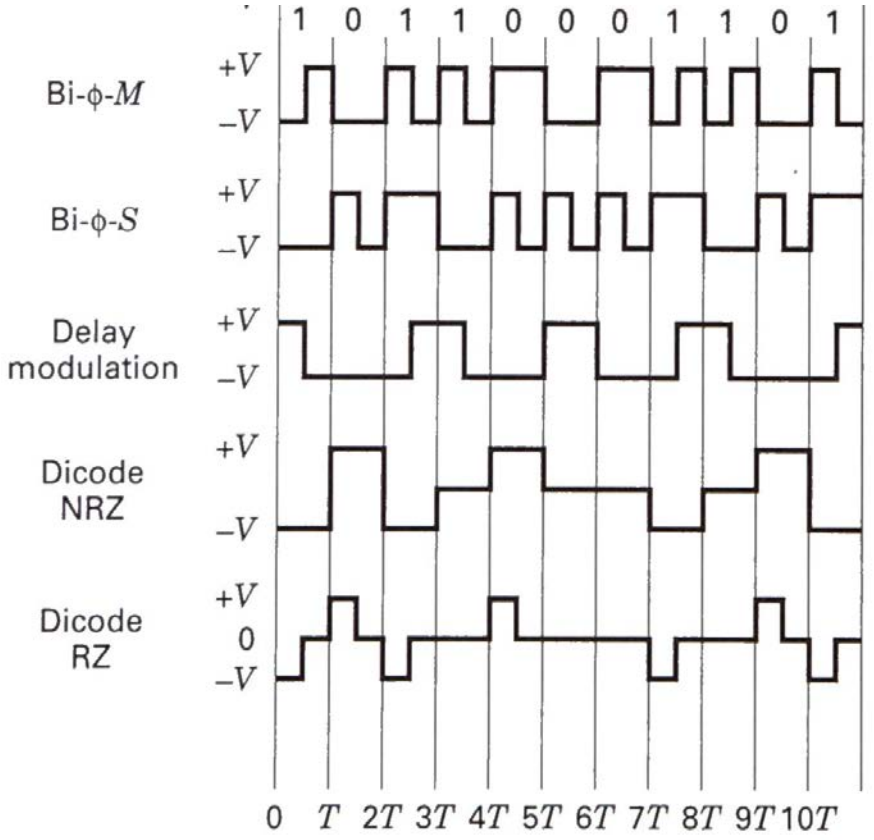
$$E(f) = H(f)^{-1}.$$

6.2 Line codes

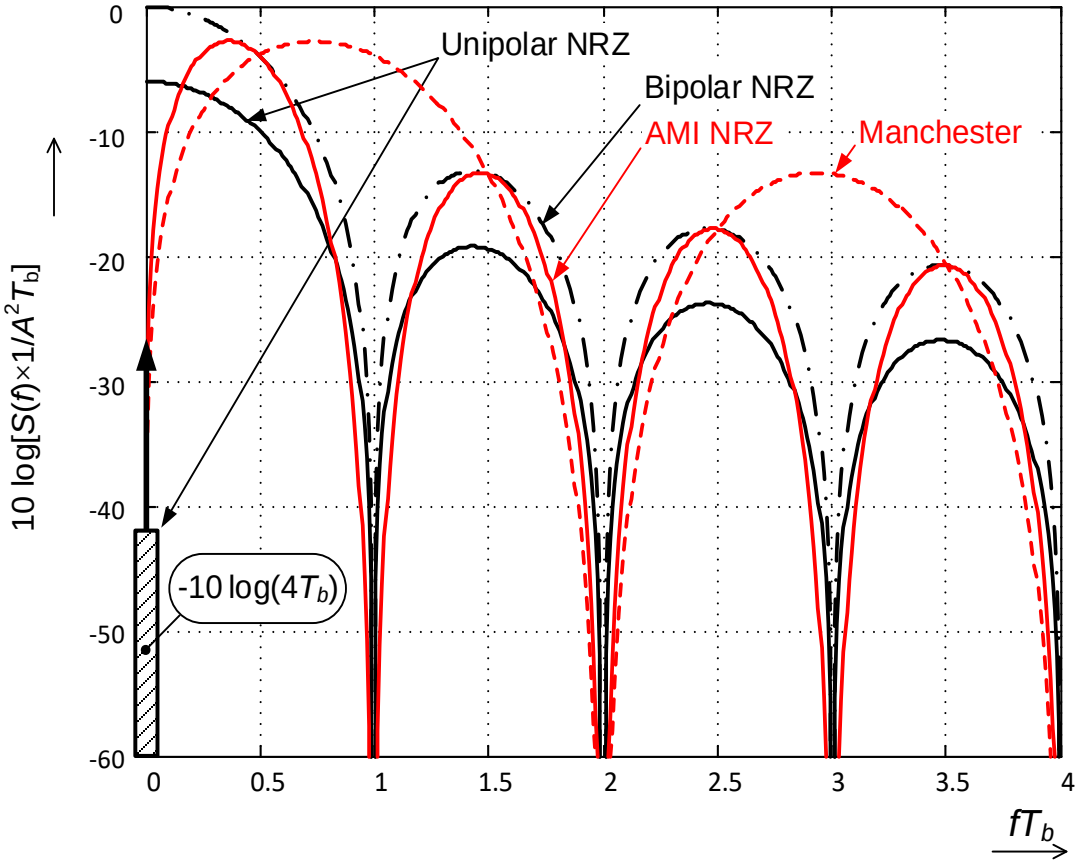
Family of codes for baseband signal encoding in order to achieve the desired properties (transmission of synchronization, removal of DC component …)

- **Basic categories: NRZ (*Non Return to Zero*), RZ (*Return to Zero*), *phase encoded, binary two-level/multilevel*. *L* = Level, *M* = Mark, *S* = Space.**





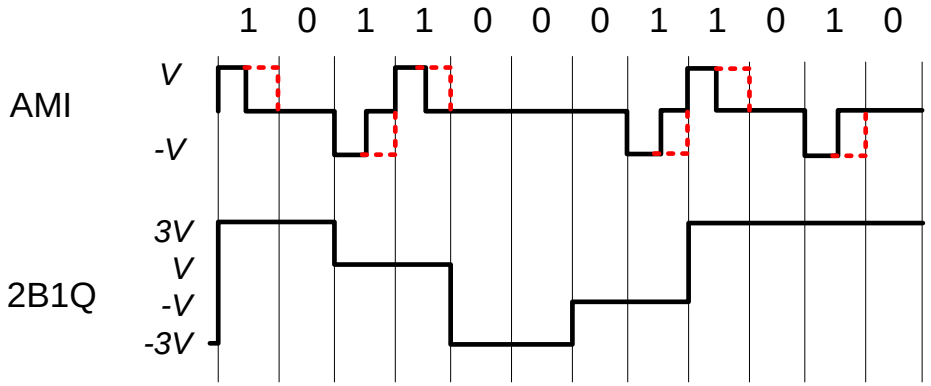
Power spectral density of selected line codes (some of them do not contain DC component: AMI NRZ, Manchester)



6.2 Line codes

Line code 2B1Q two-binary, one-quaternary (used in DSL)

Incoming dibit	Output level
11	*V*
10	+3*V*
01	-*V*
00	-3*V*



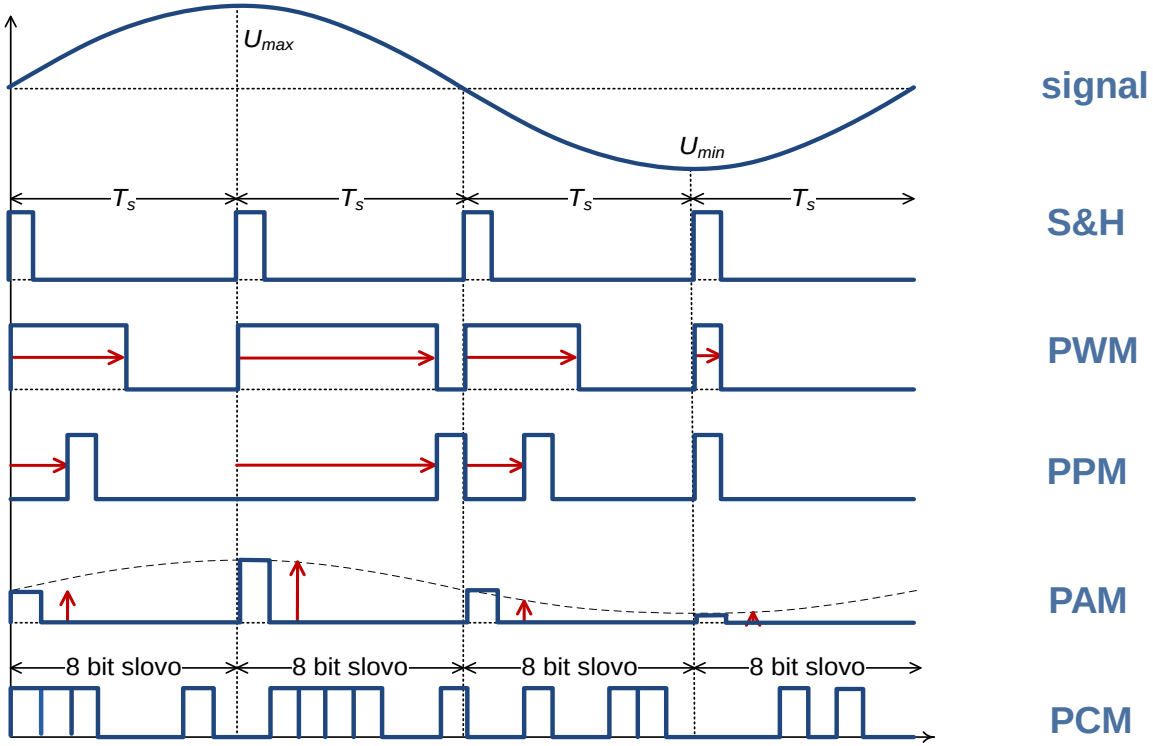
Why so many codes? Different codes have different specific properties:

1. **Removal of the DC component: easier implementation of circuits (AC coupling).**
2. **Level change in each bit: easier synchronization (example: Bi-ϕ-*L*, i.e. Manchester).**
3. **A specific encoding:**
   - **more information can be transferred in a given bandwidth.**
   - **greater noise immunity can be obtained for a given SNR.**
4. **Differential encoding: avoids erroneous decoding in the case of code level inversion being used.**

6.3 M-ary pulse modulation

Information may be generally encoded into

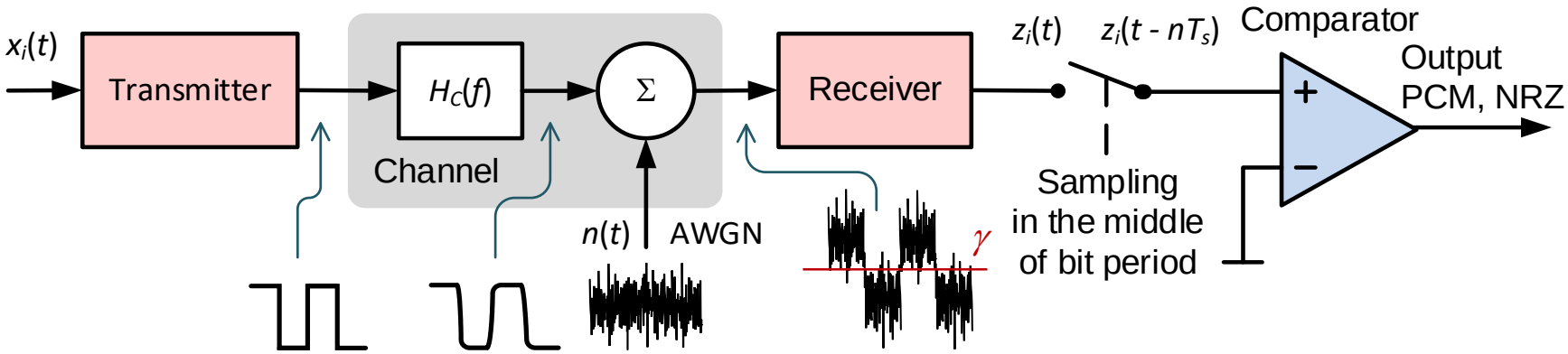
- **pulse amplitude: PAM (*Pulse Amplitude Modulation*) - natural sampling,**
- **pulse width: PWM (*Pulse Width Modulation*),**
- **pulse position: PPM (*Pulse Position Modulation*).**



Symbol vs. bit: continuous/discrete signal (symbol PAM) is expressed in binary scale using bits (PCM word).

6.4 Baseband signal detection in AWGN channel

6.4.1 Data transmission over AWGN channel



Probability of incorrect detection of

$z_1(t)$ - miss :

$$P\left[z_1(T_s) \le \gamma\right] = F_{z_1}(\gamma) = \int_{-\infty}^{\gamma} p(x \mid s_1)dx = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-\frac{1}{2}\left(\frac{x-a_1}{\sigma}\right)^2} dx = \Phi\left(\frac{\gamma - a_1}{\sigma}\right)$$

$z_0(t)$ - false alarm :

$$P\left[z_0(T_s) > \gamma\right] = 1 - P\left[z_0(T_s) \le \gamma\right] = 1 - F_{z_0}(\gamma) = \ldots = Q\left(\frac{\gamma - a_0}{\sigma}\right)$$

a_i: pulse amplitude (average value of a random variable),

σ: standard deviation of a noise,

$p(x)$: probability density function (PDF),

$F(x)$: cumulative probability density function (CDF),

$\Phi(z) = 1\text{-}Q(z)$: normalized CDF,

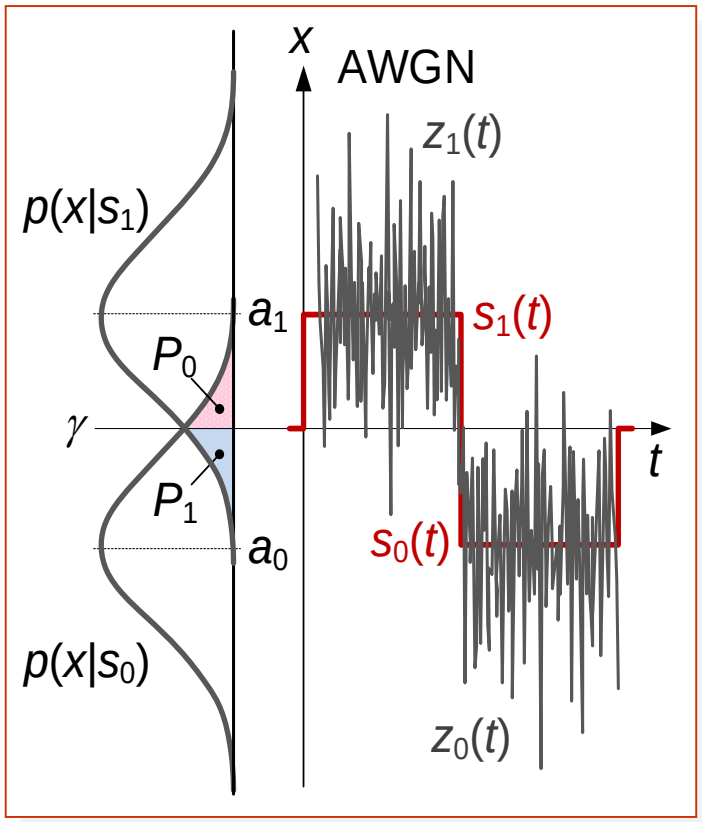
$Q(z) = 1\text{-}\Phi(z)$: inverse normalized CDF.

6.4.1 Data transmission over AWGN channel

Probability of incorrect detection
graphical interpretation

P_1 **(area): probability of** $z_1(t)$ **being detected as** $z_0(t)$ ***(miss).***

P_0 **(area): probability of** $z_0(t)$ **being detected as** $z_1(t)$ ***(false alarm).***



If $P(s_1)$ is the probability of s_1 occurrence and $P(s_0)$ is the probability of s_0 occurrence then

the probability of error P_e is:

$$P_e = P(s_1)\Phi\left(\frac{\gamma - a_1}{\sigma}\right) + P(s_0)Q\left(\frac{\gamma - a_0}{\sigma}\right)$$

6.4.1 Data transmission over AWGN channel

Optimal threshold γ for minimizing P_e is given by the local extremum of P_e

$$\frac{\partial P_{ch}}{\partial \gamma} = \frac{\partial}{\partial \gamma}\left[P(s_1)Q\left(\frac{a_1-\gamma}{\sigma}\right) + P(s_0)Q\left(\frac{\gamma-a_0}{\sigma}\right)\right] = 0 \quad \Rightarrow \textbf{Solution for } \gamma$$

$$\gamma = \frac{a_1+a_0}{2} + \frac{\sigma^2}{a_0-a_1}\ln\frac{P(s_1)}{P(s_0)}$$

Then $P_{ch} = Q\left(\frac{a_0-a_1}{2\sigma}\right)$

For $P(s_1) = P(s_0)$ $\quad \gamma = \frac{a_1+a_0}{2}$

The bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a given time interval. It is obtained by a measurement.

The probability of error P_e is usually derived at theoretical basis for a specific case.

6.4.2 Matched filter (MF)

MF: linear filter designed to provide the maximum *Signal-to-Noise power Ratio* (SNR) at its output for a given transmitted symbol waveform.

Let *s*(*t*) is a known waveform. Then SNR will be maximized if the MF impulse response is

$$h(t)=\begin{cases} ks(T_s-t) & 0\le t\le T_s, \quad k \text{ is an arbitrary constant} \\ 0 & \text{otherwise} \end{cases}$$

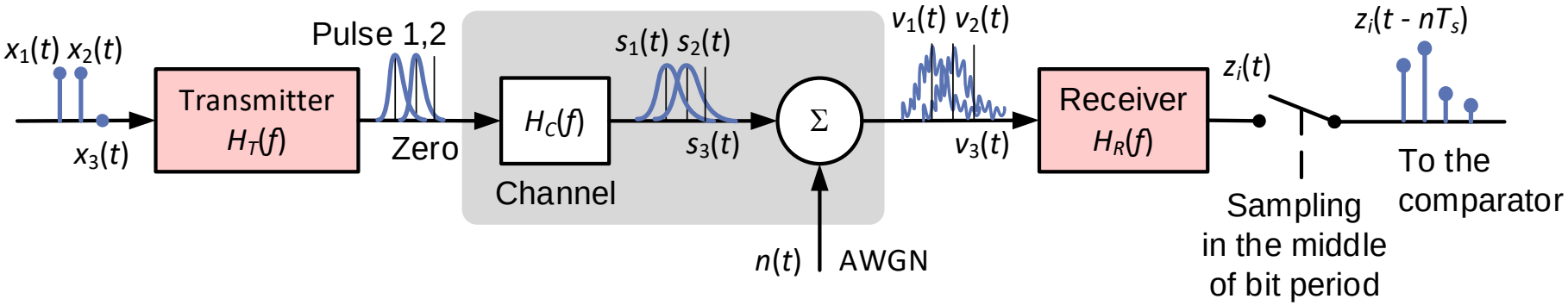
Typical application: detection of reflected radio-impulses corrupted by noise - radar

6.5 Inter-Symbol Interference (ISI)

There are various frequency restrictions (filters) throughout the channel:

- **Transmitter has to comply with some bandwidth constraint due to regulations.**
- **Baseband channel (a wire cable) has distributed reactance that distort the pulses.**
- **Band-pass channel (wireless system) is characterized by fading channels (it acts as a low-pas filter).**
- **Receiver eliminates the input noise by a band-pass filter.**

Inter-symbol interference in the transmission process



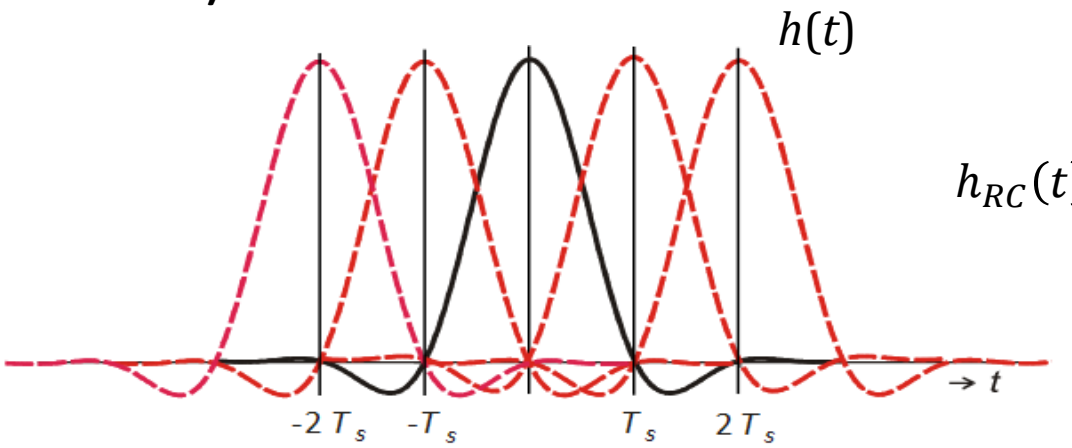
System total response: $H(f)=H_T(f)H_C(f)H_R(f)$

6.5 Inter-Symbol Interference (ISI)

How the transfer function $H(f)$ can provide zero ISI?

It can be performed by

1. **Nyquist filter: ideal lowpass filter (LPF) with the cut-off frequency $R_s/2$ (unrealizable),**
2. **Raised-cosine (RC) filter: LPF with the modified cosine spectrum $H_{RC}(f)$ (digitally realizable).**



$$h_{RC}(t) = \text{sinc}(\pi R_s t)\frac{\cos\beta\,\pi R_s t}{1-(2\beta R_s t)^2}$$

***Roll off-factor β*: relative increase of the bandwidth related to the Nyquist one ($0.5R_s$).**

6.6 Equalization

Reduction of an influence of fading in non-stationary channels.

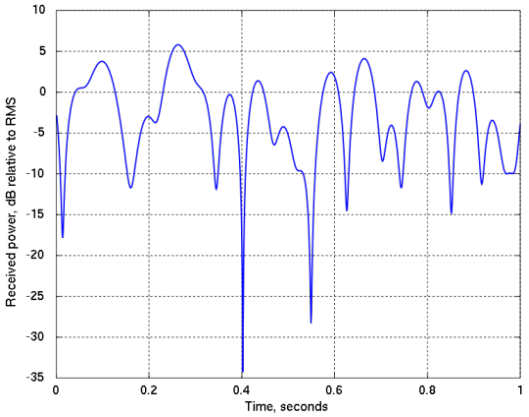
Frequency selective fading: **combination of several phase-shifted (delayed) signals complying the condition** $T_m = (1/\Delta f) << (1/B)$ **(**T_m**: delay dispersion** Δf**: coherence bandwidth,** B**: RF bandwidth)** $\Rightarrow$ **ISI occurrence and BER degradation.**

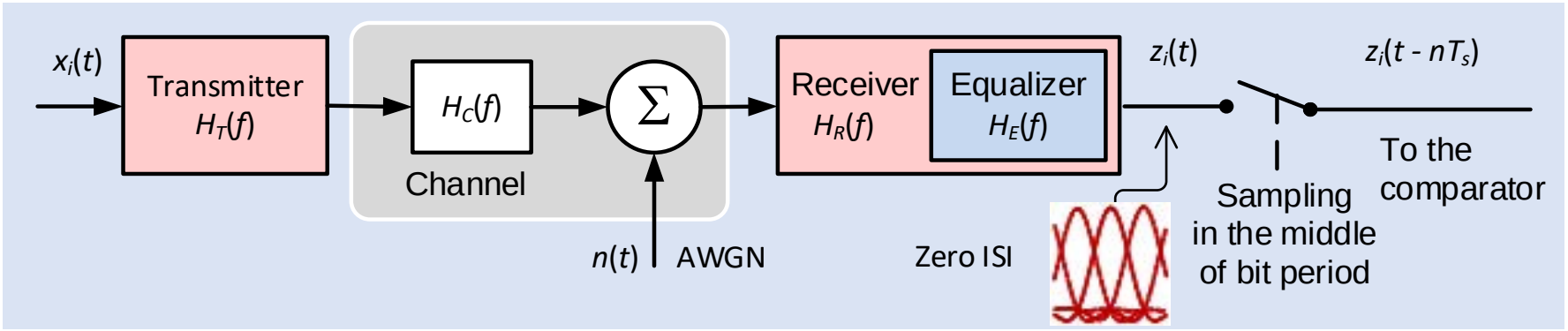
Frequency flat fading: **caused by atmospheric attenuation (rain,..)** $(1/\Delta f) >> 1/B.$

Fast fading $(T_m << T_s)$ ***vs*** **slow fading** $(T_m >> T_s)$.

In practice the transmitter and receiver filters have transfer function $H_{RC}(f)$**. Then:**

$$H(f) = H_{RC}(f) = \underbrace{H_T(f)H_R(f)}_{H_{RC}(f)}\underbrace{H_C(f)H_E(f)}_{1}$$





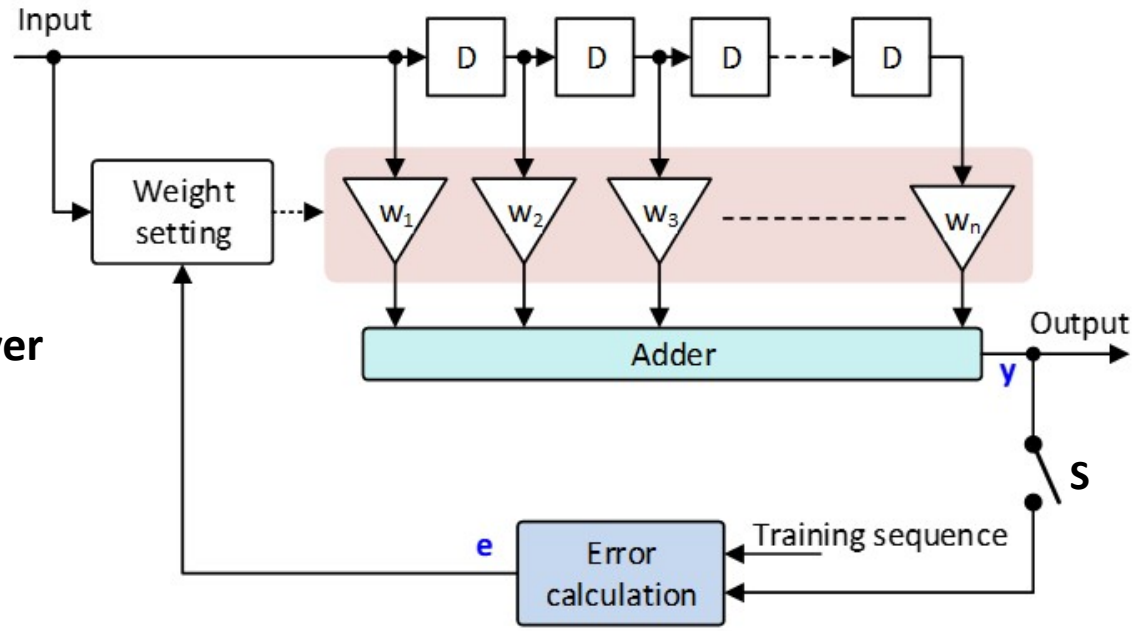
6.6 Equalization

Because $H_C(f)H_E(f) = 1$ the equalizer have to meet condition $H_E(f) = H_C(f)^{-1}$

Equalizer in training mode

- **Transmitter inserts periodically a training sequence into the transmitted data stream.**
- **Switch S is ON.**
- **After filtering the received training sequence (y) is compared with the same sequence generated by receiver (stored in memory) and the error signal (e) is calculated.**
- **In case of nonzero error the filter weights are changed in order to minimize it.**

Equalizer (adaptive FIR filter)



Equalizer in data mode: switch S is OFF and the equalized signal is fetched from output.

7. BAND-PASS MODULATION
7.1 Modulation techniques overview

Why modulate?

- Baseband signal modulates a sinusoidal waveform called a *carrier wave*, or simply a *carrier* that are compatible with the characteristics of the channel.
- Carrier is converted to an electromagnetic (EM) field for propagation to the desired destination.
- The transmission of EM fields through space is accomplished with the use of antennas.

Classification

- Analog (transmission of analog signals) AM, FM, PM, QAM
- Digital (transmission of digital signals) ASK, FSK, PSK, QAM
- Linear (with variable modulation envelope) AM, QAM, ASK
- Nonlinear (with constant modulation envelope) FM, PM, FSK, PSK
- Coherent (demodulation with recovered carrier) ASK, FSK, PSK
- Noncoherent (demodulation without recovered carrier) DPSK, FSK, ASK

7.1 Modulation techniques overview

Harmonic signal: $s_0(t) = S_0 \cos(2\pi f_0 t + \varphi_0) = S_0 \cos\Phi(t)$.

S_0: **Amplitude (positive constant).**
Its variation = **amplitude modulation/keying (AM, ASK).**

f_0: **Frequency (positive constant).**
Its variation = **frequency modulation/keying (FM).**

φ_0: **Phase.** Its variation = **phase modulation/keying (PM).**

$\Phi(t)$: **Phase angle.** Its variation = **class of angle modulations.**

7.2 Analogue modulations

- **Modulations used in real communication systems: AM, FM, PM, QAM.**
- **Require large SNR.**

7.2.1 Amplitude modulation

Typical application: broadcasting at long wave (LW), medium wave (MW) and short wave (SW) bands (at frequencies from hundreds of kHz to couple of MHz) and powers of hundreds of kW.

7.2.1 Amplitude modulation

$$s(t) = S(t)\cos 2\pi f_0 t = S_0\left[1 + \frac{\Delta S}{S_0} n(t)\right]\cos 2\pi f_0 t$$

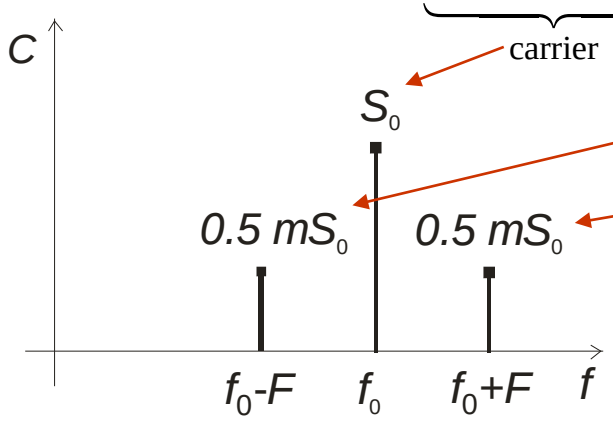
$$S(t) = S_0 + \Delta S n(t)$$

ΔS: amplitude deviation,
$n(t)$: normalized baseband function, $n \in \langle -1, 1 \rangle$,
m: modulation depth $m \in (0, 1\rangle$.

AM spectrum for harmonic baseband signal $n(t) = \cos 2\pi Ft$, **(*F* – harmonic signal frequency):**

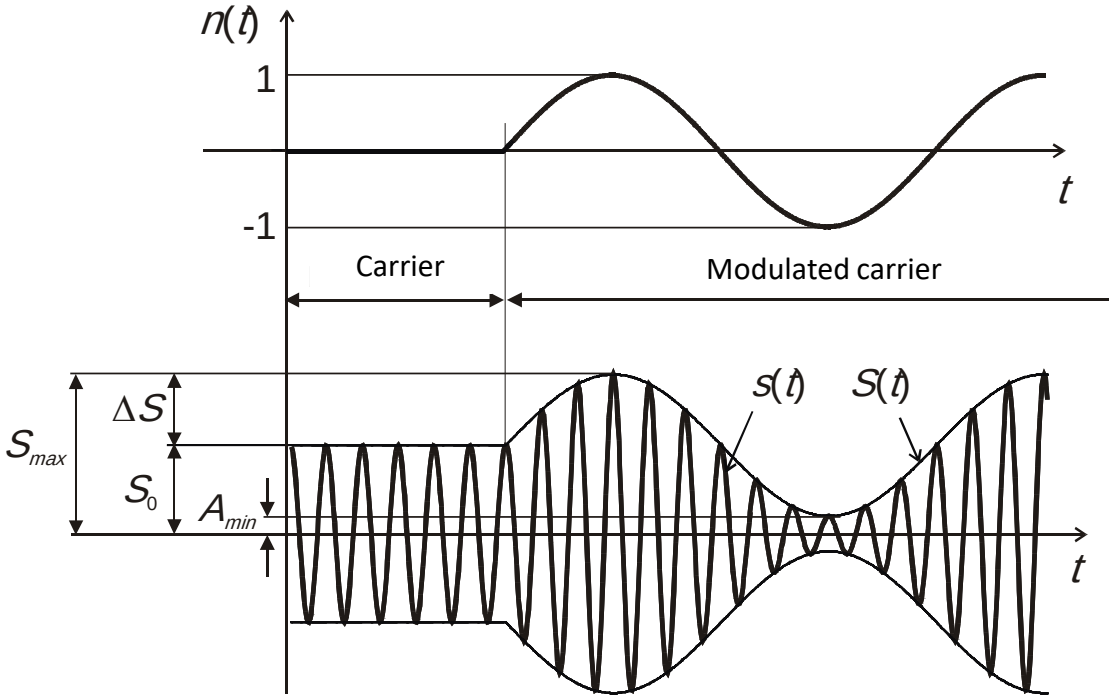
$$s(t) = \underbrace{S_0\left[1 + m\cos 2\pi Ft\right]}_{\text{envelope}}\cos 2\pi f_0 t$$

$$= \underbrace{S_0 \cos 2\pi f_0 t}_{\text{carrier}} + \underbrace{S_0 \frac{m}{2}\cos 2\pi\left(f_0 - F\right)t}_{\text{lower pass-band}} + \underbrace{S_0 \frac{m}{2}\cos 2\pi\left(f_0 + F\right)t}_{\text{upper pass-band}}.$$



7.2.1 Amplitude modulation

AM in time domain



Normalized AM average power

$$P_S = \underbrace{\left(\frac{S_0}{\sqrt{2}}\right)^2}_{\text{carrier power}} + \underbrace{2\left(\frac{1}{2}m\frac{S_0}{\sqrt{2}}\right)^2}_{\text{pass-bands power}} = P_0\left(1+\frac{m^2}{2}\right)$$

Normalized peak envelope power (*PEP*)

$$P_{PEP} = \left(\frac{S_0 + mS_0}{\sqrt{2}}\right)^2 = P_0(1+m)^2$$

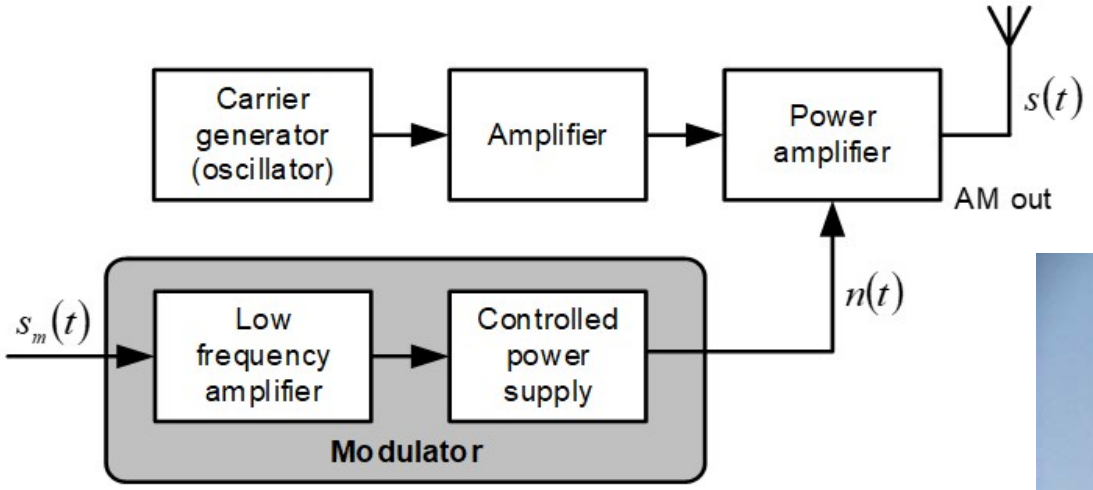
7.2.1 Amplitude modulation

Example: let we have a) $m = 0.35$ then $P_S = 1.061P_0$

b) $m = 1$ then $P_{PEP} = 4\ P_0$

⇒ **Main AM disadvantage: Transmitter have to be designed for** $PEP = 4\ P_0$**.**

Transmitter for AM

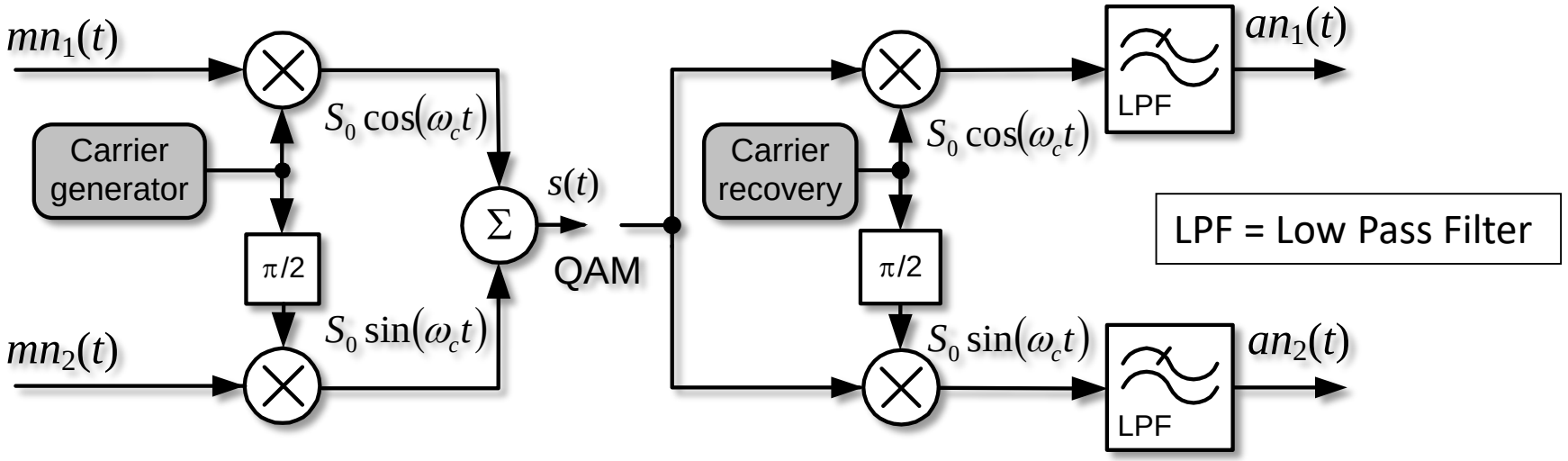


7.2.2 Quadrature Amplitude Modulation (QAM)

- **Most often used QAM modification is QAM_{SC} (with *suppressed carriers*).**
- **QAM can transfer two baseband independent signals n_1 and n_2 through the same channel as in the case of AM (better utilization of RF channel).**
- **Basis of digital variant of QAM.**

$$s(t) = S_0[m_1 n_1(t)]\cos 2\pi f_0 t + S_0[m_2 n_2(t)]\sin 2\pi f_0 t$$

QAM modulator and demodulator



QAM application: Modulation of chrominance signals in PAL TV color system.

7.2.3 Frequency modulation

Case of angle modulation signaling. Let $S(t) = S_0$ and $\varphi(t) = \varphi_0 = 0$ then

$$s(t) = S_0 \cos \Phi_{FM}(t)$$

$$f(t) = f_0 + \Delta f n(t)$$

$$\Phi_{FM}(t) = \int_0^t \omega(\alpha) d\alpha = \int_0^t 2\pi f(\alpha) d\alpha = 2\pi f_0 t + 2\pi \Delta f \int_0^t n(\alpha) d\alpha$$

Δf: frequency deviation, $n(t)$: normalized baseband function , $n \in \langle -1, 1 \rangle$.

For harmonic baseband signal $n(t) = \cos 2\pi F t$ we get

$$s(t) = S_0 \cos \Phi(t) = S_0 \cos\left[2\pi f_0 t + 2\pi \Delta f \int_0^t \cos 2\pi F \alpha d\alpha \right] =$$

$$= S_0 \cos\left[2\pi f_0 t + \frac{\Delta f}{F} \sin 2\pi F t \right] = S_0 \cos\left[2\pi f_0 t + \beta \sin 2\pi F t \right].$$

$\beta = \Delta f / F$: **FM index**

FM application:

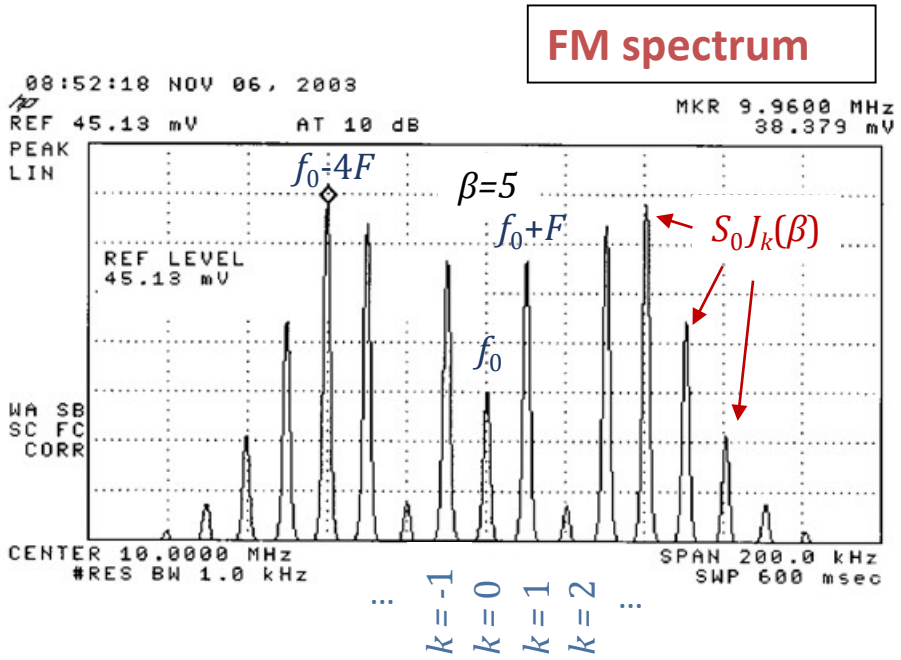
$\beta >> 1$: **wideband FM (VHF broadcasting CCIR 87.5-108 MHz),**

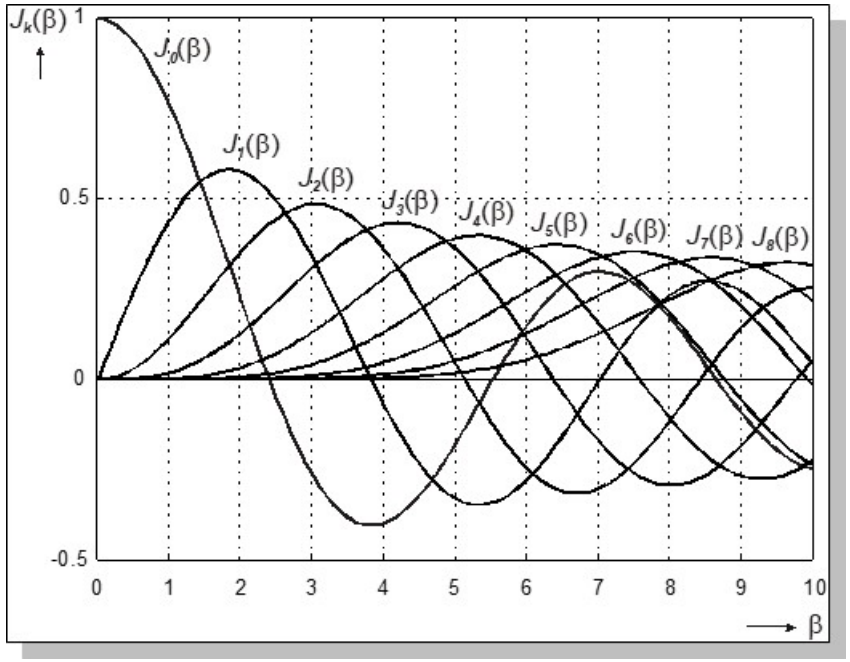
$\beta << 1$: **narrowband FM (land services – ambulance, army, emergency rescue).**

7.2.3 Frequency modulation

$$s(t) = S_0 \cos(2\pi f_0 t + \beta \sin 2\pi F t) = S_0 \sum_{k=-\infty}^{\infty} J_k(\beta) \cos 2\pi (f_0 + kF)t$$

$J_k(\beta)$: **Bessel function of the first kind, k-th order, argument β.**
$J_{-k}(\beta) = (-1)^k J_k(\beta)$.

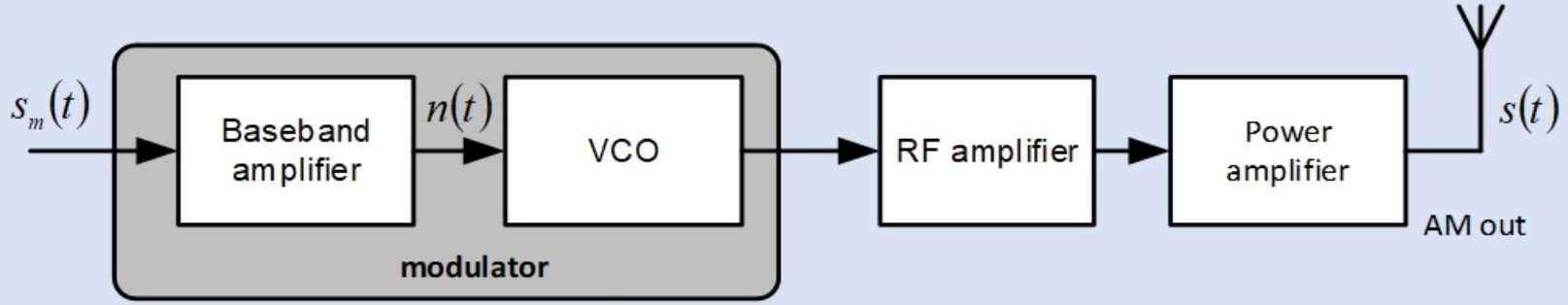




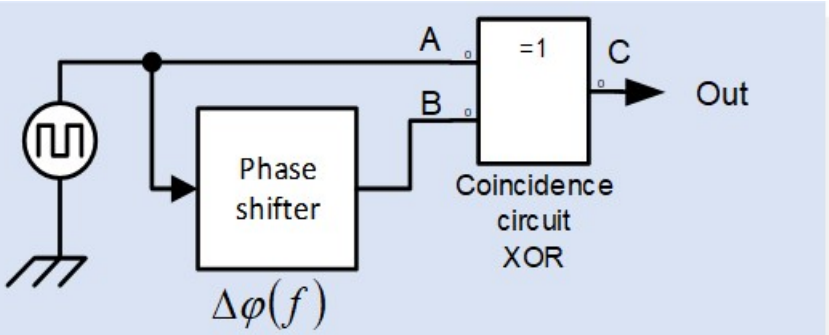
FM bandwidth (Carson's rule): $B_{FM} = 2(F + \Delta f) = 2F(\beta + 1)$ contains 98% of the total power.

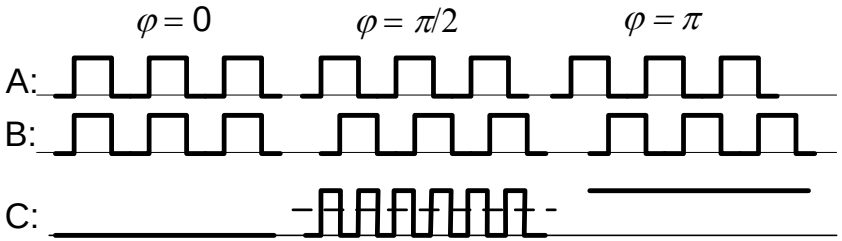
7.2.3 Frequency modulation

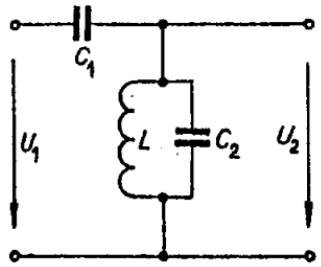
Typical architecture of FM transmitter (with direct modulation)

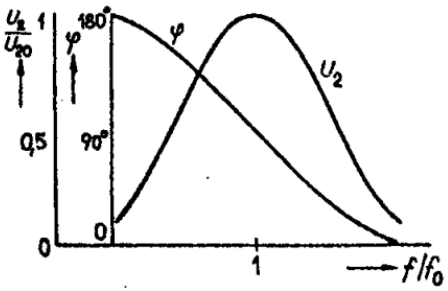


Coincidence demodulator FM









Typical FM demodulators

- FM to AM conversion and AM demodulation
- FM to PM conversion and PM demodulation

7.2.4 Phase modulation

Member of angle modulation family. Let $S(t) = S_0$ and $f(t) = f_0$ then

$$s(t) = S_0 \cos \Phi_{PM}(t)$$

$$\varphi(t) = \varphi_0 + \Delta\varphi n(t)$$

$$\Phi_{PM}(t) = \int_0^t 2\pi f(\alpha) d\alpha + \varphi(t) = 2\pi f_0 t + \Delta\varphi n(t) + \varphi_0$$

$\Delta\varphi$: phase deviation, $n(t)$: normalized baseband function.

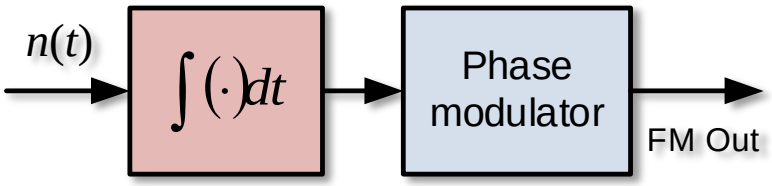
For harmonic baseband signal $n(t) = \cos 2\pi Ft$ we get

$$s(t) = S_0 \cos \Phi(t) = S_0 \cos[2\pi f_0 t + \beta \cos 2\pi Ft]$$

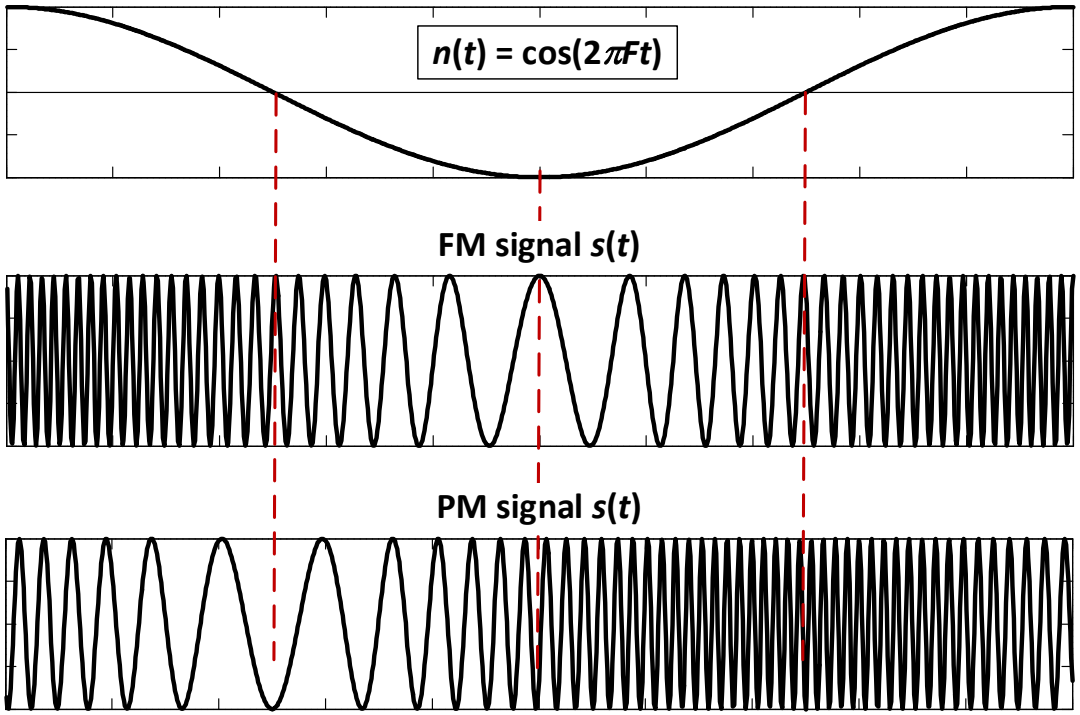
$\beta = \Delta\varphi$: index of PM

Indirect modulation techniques

Putting $\Phi_{FM}(t) = \Phi_{PM}(t)$ we can find out that FM can be obtained using PM modulator and by integration of the baseband signal.



7.2.5 Phase and frequency modulation comparison



Hády

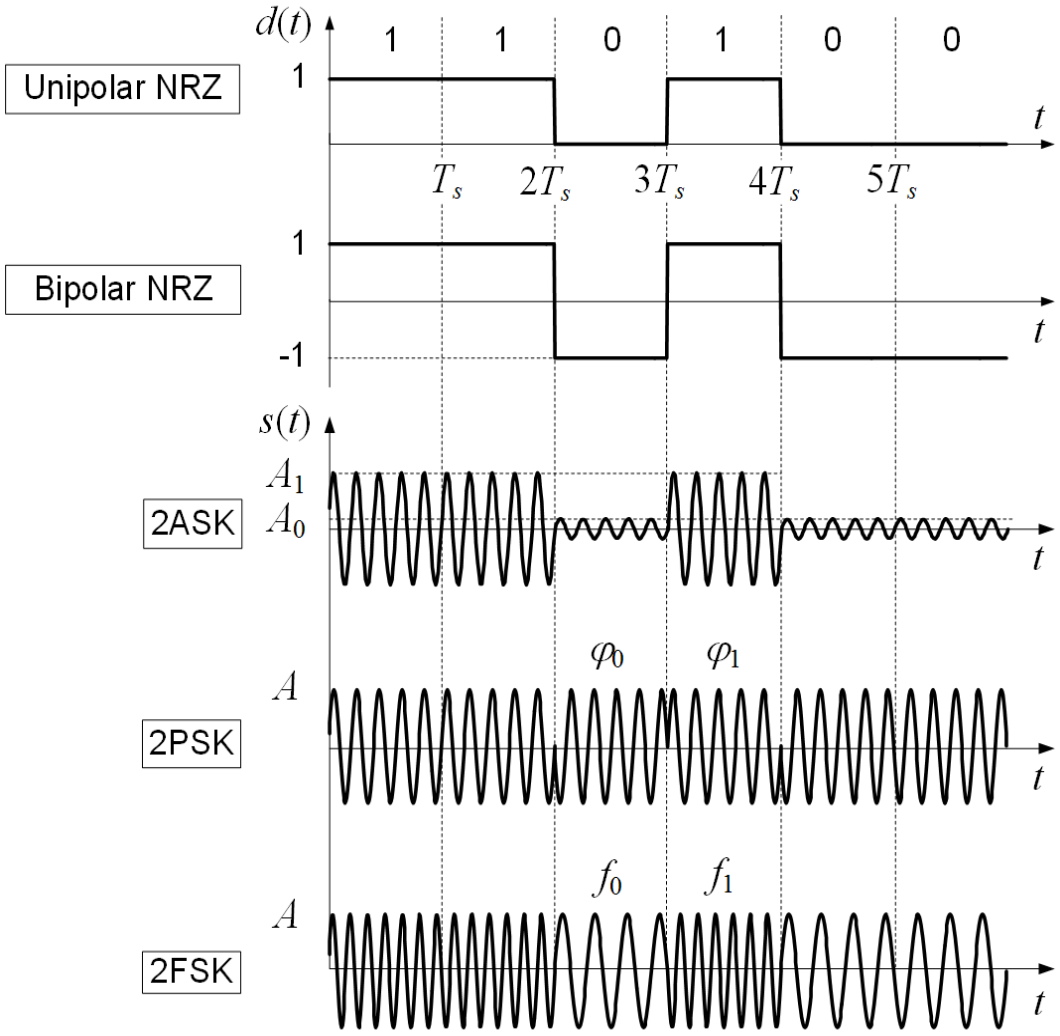
- **Maximum/minimum frequency of FM signal corresponds to a maximum/minimum voltage of $n(t)$.**
- **Maximum/minimum frequency of PM signal corresponds to a maximum rise/fall rate of voltage $n(t)$.**

7.3 Digital modulations

7.3.1 General characteristics

Generally they produce M different waveforms: M-ary signaling. An example below shows basic types for $M = 2$.

- **Amplitude Shift Keying (ASK)**
  Keying of carrier amplitude between values $A_0, A_1, \ldots$. If $M=2$ and $A_0 = 0$, ASK changes to On-Of-Keying (OOK).
- **Phase Shift Keying (PSK).**
  Keying of carrier phase between values $\varphi_0, \varphi_1, \ldots$ where $\varphi_i - \varphi_{i-1} = 2\pi/M$.
- **Frequency Shift Keying (FSK).**
  Keying of carrier frequency between values $f_0, f_1, \ldots$



7.3.1 General characteristics

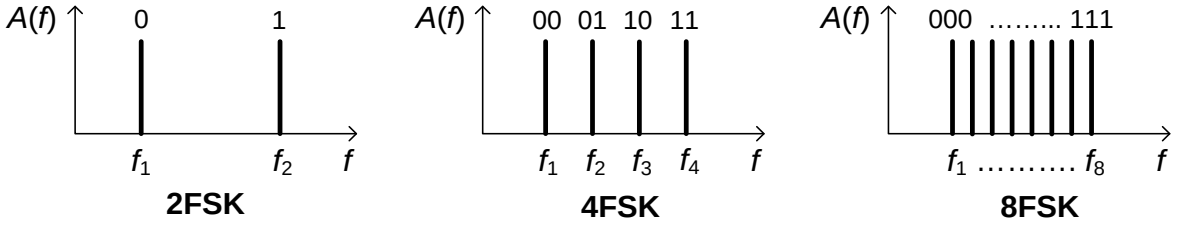
***M*-ary digital modulations:** number of waveforms $M = 2^n$, number of bits: n.

Methods of modulated signal representation:

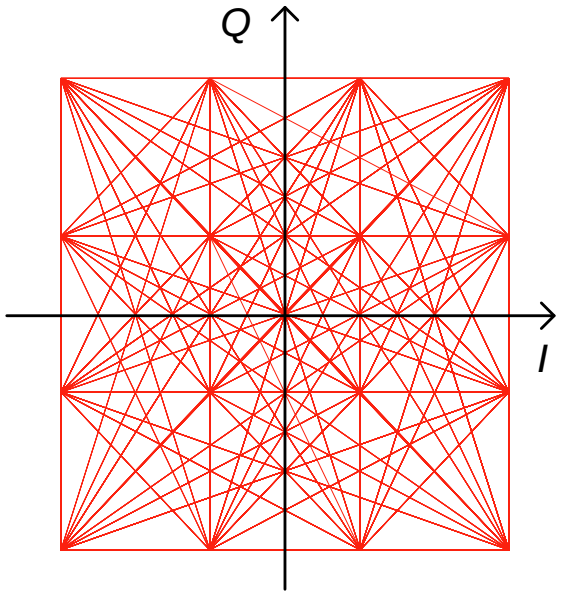
- In time domain: time waveforms - see previous page
- In frequency domain: spectrum of modulated signal (dominantly FSK)
- In IQ plane (*In-phase* and *Quadrature* axis (components)), vector diagram, constellation (state) diagram.

Examples:

2FSK to 8FSK in frequency domain

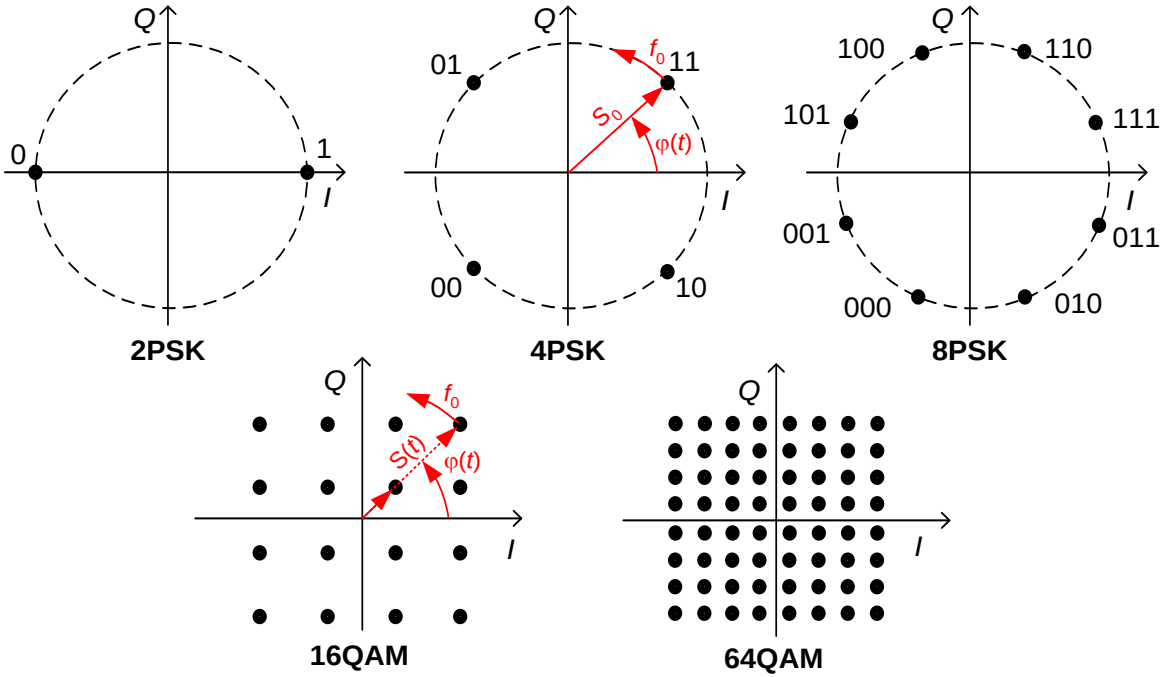


16QAM representation in IQ plane – vector diagram →



7.3.1 General characteristics

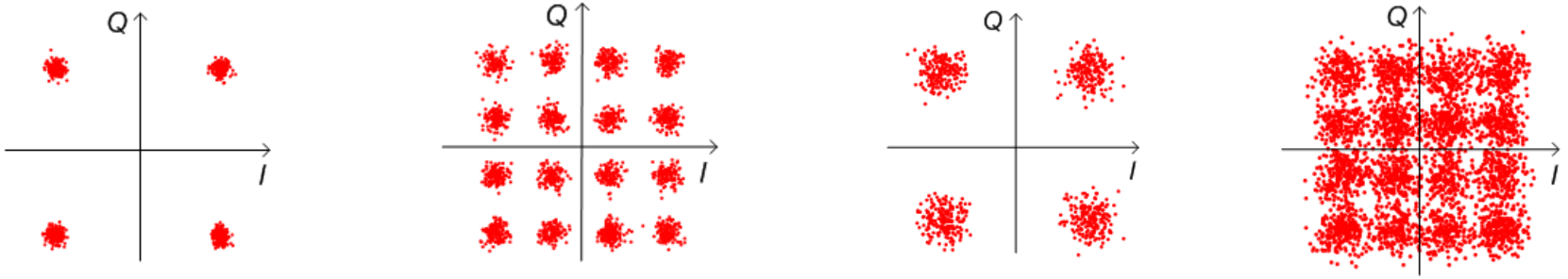
PSK and QAM representation in IQ plane – constellation diagram



Effect of noise on spread of QPSK and 16 QAM constellation points

Acceptable noise

unacceptable noise (for 16 QAM)



7.3.2 Common parameters of digital modulations

Let we have bit period T_b, symbol period T_s, bit rate R_b, symbol rate R_s and number of bits n per symbol of M – ary signaling then we can introduce:

$$M = 2^n, \quad n = \log_2 M, \quad T_s = nT_b \quad \text{and} \quad R_s = \frac{1}{T_s} = \frac{1}{nT_b} = \frac{R_b}{n} = \frac{R_b}{\log_2 M}.$$

- **Bit Error Rate (BER): the number of bit errors divided by the total number of transferred bits during a given time interval. It is obtained by a measurement.**
- **Symbol Error Rate (SER): the number of symbol errors divided by the total number of transferred symbols in a given time interval.**
- **Energetic Efficiency η_e:** $\eta_e = \frac{E_b}{N_0}$ [–] or $\eta_{e\text{dB}} = 10\log\left(\frac{E_b}{N_0}\right)$ [dB]

  E_b: average energy of modulated signal related to 1 bit,
  N_0: power spectral density of the noise.

- **Spectral Efficiency η_s:** $\eta_s = \frac{R_b}{B_c}$ [bit/s/Hz],

  B_c: RF bandwidth.

7.3.3 Binary Amplitude Shift Keying

M = 2, **BASK, 2ASK.** **The BASK is generated by multiplication of the carrier** $S_0 \cos 2\pi f_c t$ **by a unipolar NRZ signal of the two amplitudes** a_1 **and** a_0 **(optionally filtered by the RC filter). It forms two waveforms:**

$$s_1(t) = a_1 S_0 \cos(2\pi f_c t) \quad \text{for} \quad 0 \geq t \geq T_b \quad \log 1$$
$$s_0(t) = a_0 \underbrace{S_0 \cos(2\pi f_c t)}_{\text{carrier}} \quad \text{for} \quad 0 \geq t \geq T_b \quad \log 0 \qquad 1 \geq a_1 >> a_0 > 0$$

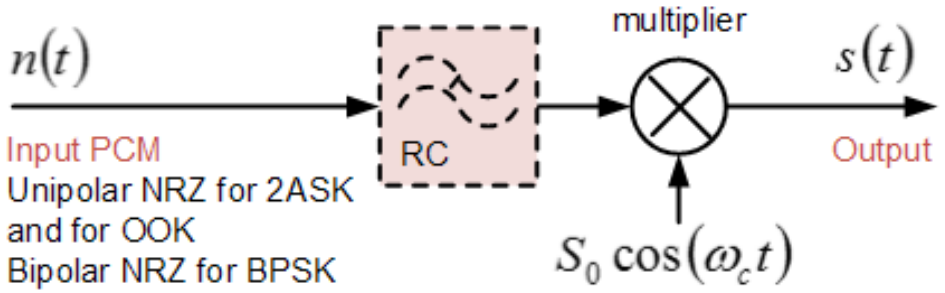
7.3.4 Binary Phase Shift Keying

M = 2, **BPSK, 2PSK.** **The BPSK is generated by multiplication of the carrier by a bipolar NRZ signal of the two amplitudes** a_1 **and** $-a_1$**. It forms the two waveforms:**

$$s_1(t) = a_1 S_0 \cos(2\pi f_c t) \quad \text{for} \quad 0 \geq t \geq T_b \quad \log 1$$
$$s_0(t) = -a_1 S_0 \cos(2\pi f_c t) = a_1 S_0 \cos(2\pi f_c t \pm \pi) \quad \text{for} \quad 0 \geq t \geq T_b \quad \log 0$$

7.3.4 Binary Phase Shift Keying

2ASK and BPSK modulator:



7.3.5 Binary Frequency Shift Keying

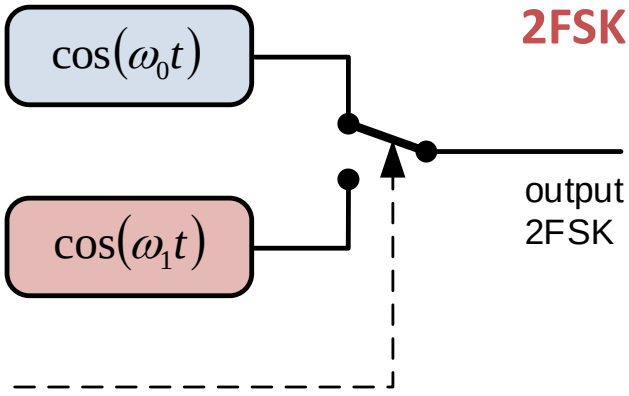
M = 2, **BFSK, 2FSK.** **The BPSK is generated by switching of the two carriers with different frequencies f_1 and f_0. It forms the two waveforms:**

$$s_1(t) = S_0 \cos(2\pi f_1 t) \quad \text{for} \quad \log 1$$
$$s_0(t) = S_0 \cos(2\pi f_0 t) \quad \text{for} \quad \log 0$$

Application of BFSK:

Remote control, data transmission in industrial applications.

2FSK modulator



7.3.6 Quadrature Phase Shift Keying

M = 4, **4PSK, QPSK:** **Carrier takes four possible phase states – usually** ±45° **and** ± 135°. **Obtained QPSK waveform sets then is:**

$$s_i(t) = S_0 \cos\left[2\pi f_c t + (2i-1)\frac{\pi}{4}\right] \qquad i = 0,1,2,3$$

By application the goniometrical rule $\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$

we get:

$$s_i(t) = \underbrace{S_0 \cos\left[(2i-1)\frac{\pi}{4}\right]}_{I(t)} \cos 2\pi f_c t - \underbrace{S_0 \sin\left[(2i-1)\frac{\pi}{4}\right]}_{Q(t)} \sin 2\pi f_c t$$

QAM

$$s_i(t) = I(t)\cos 2\pi f_c t - Q(t)\sin 2\pi f_c t$$

AM AM

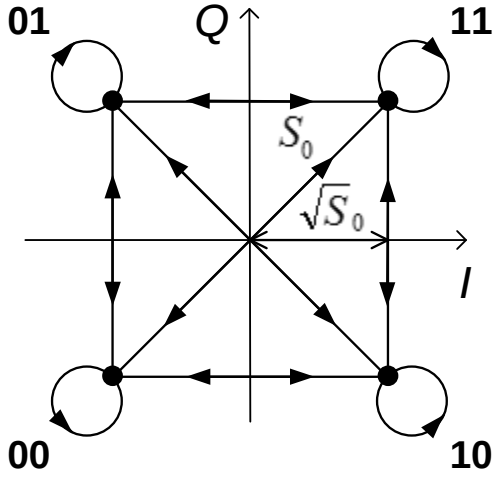
7.3.6 Quadrature Phase Shift Keying

⇒ **QPSK is actually four-ary QAM with suppressed carrier.** It is generated by multiplication of the two orthogonal carriers $S_0 \cos 2\pi f_c t$ and $S_0 \sin 2\pi f_c t$ by two bipolar NRZ signals (double application of BPSK).

⇒ QPSK represented in **polar coordinates** by shifted phase $(2i\text{-}1)\pi/4$ is transformed into **cartesian coordinates** and represented by the two variable voltages $I(t) = S_0 \cos(2i\text{-}1)\pi/4 = \pm S_0/\sqrt{2}$ and $Q(t) = S_0 \cos(2i\text{-}1)\pi/4 = \pm S_0/\sqrt{2}$. Particular values of $I(t)$ and $Q(t)$ are given by two input bits – **dibit.**

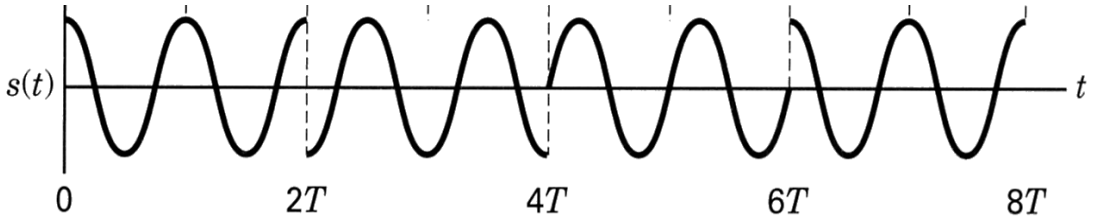
Table of QPSK I and Q states and vector diagram

i	I,Q dibit	φ	I,Q amplitudes (S_0=1)
0	1, 0	-45	0.707, -0.707
1	1, 1	45	0.707, 0.707
2	0, 1	135	- 0.707, 0.707
3	0, 0	-135	- 0.707, - 0.707



7.3.6 Quadrature Phase Shift Keying

Example of QPSK vaweform:

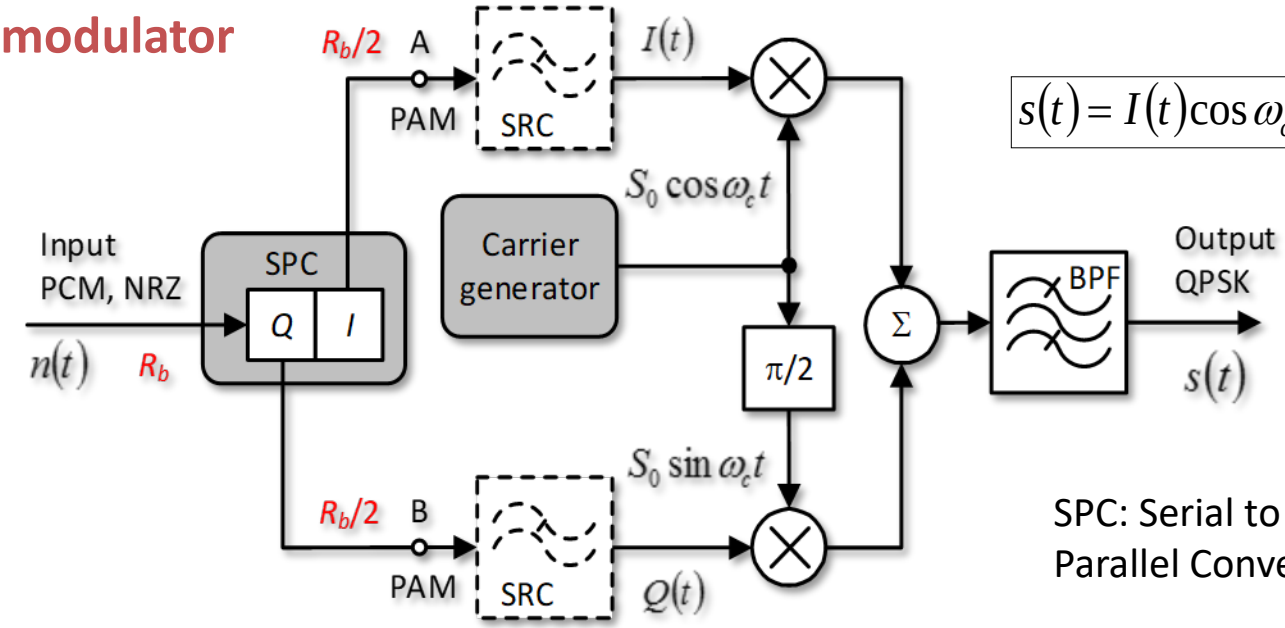


QPSK characteristics:

- **Optimal compromise between a good spectral efficiency (theoretically 2 bit/s/Hz) and energy efficiency.**
- **The problem with carrier recovery (phase uncertainty $\pm\pi/4$).**
- **Large parasitic AM.**

7.3.6 Quadrature Phase Shift Keying

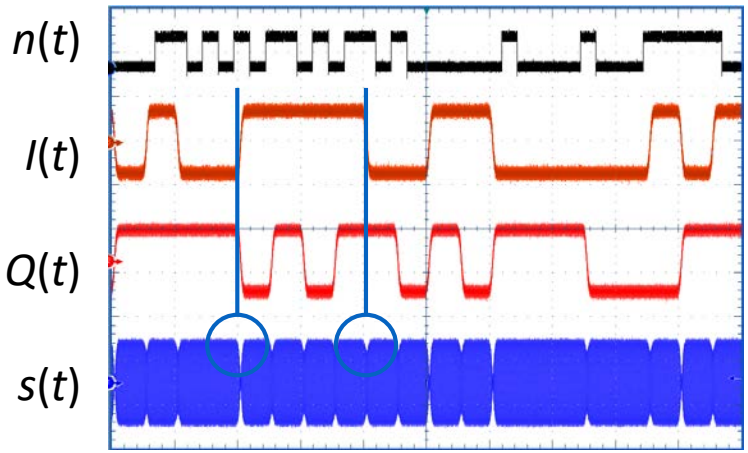
QPSK modulator



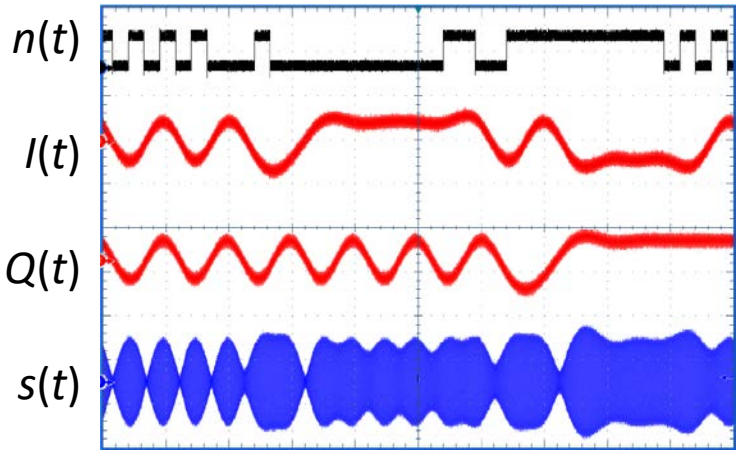
$$s(t) = I(t)\cos \omega_c t - Q(t)\sin \omega_c t$$

SPC: Serial to Parallel Converter

Symbol filtering: Rectangle



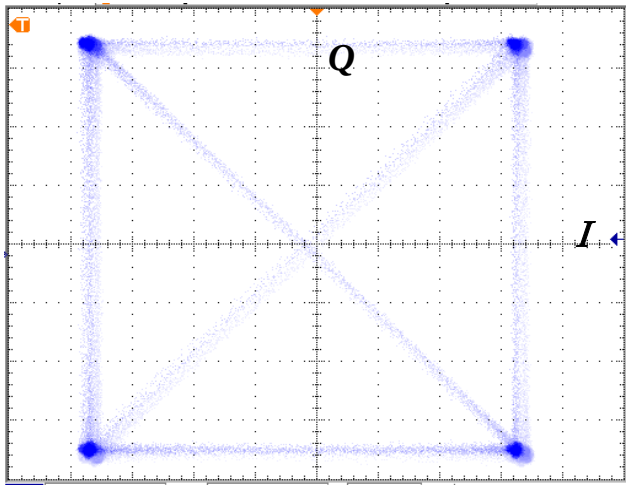
Symbol filtering: Raised-Cosine (RC)



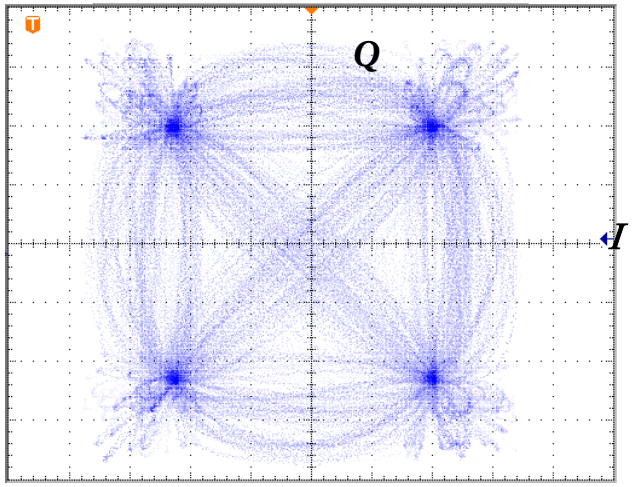
7.3.6 Quadrature Phase Shift Keying

Effect of symbol filtering

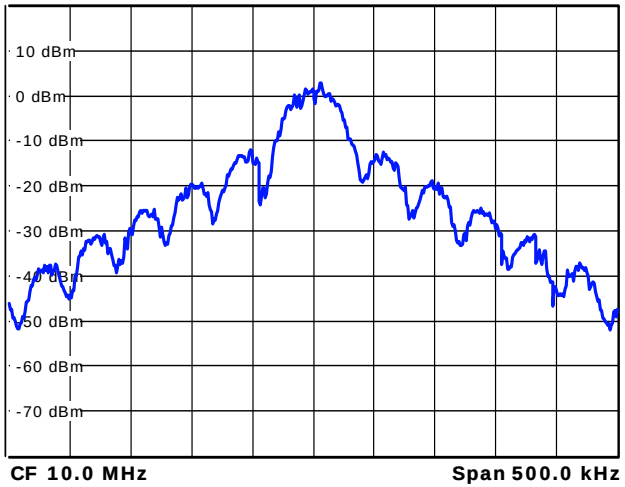
Vector diagram (rectangle)



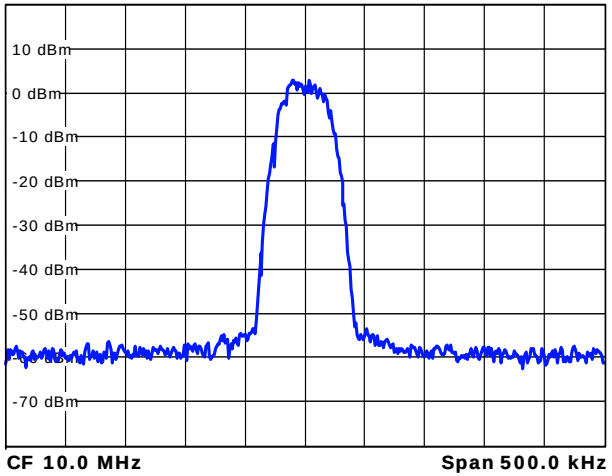
Vector diagram (Raised-Cosine)



Spectrum (rectangle)



Spectrum (Raised-Cosine)



7.3.7 Modified Quadrature Phase Shift Keying

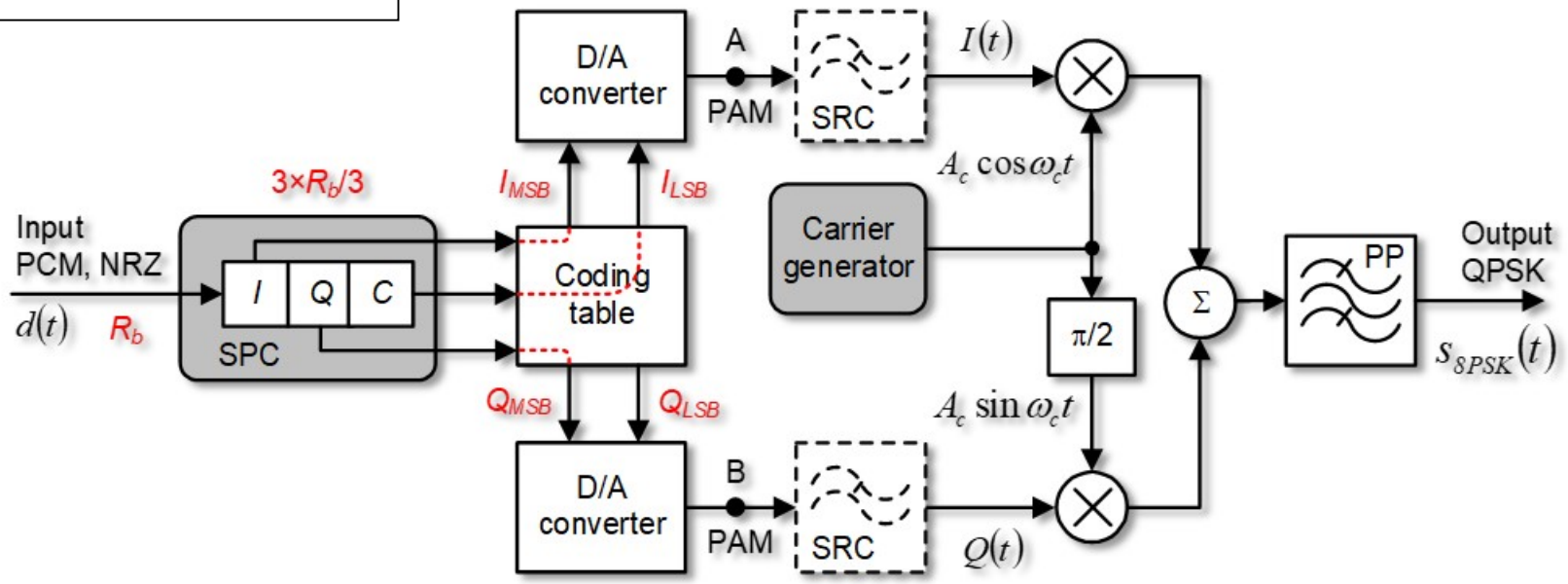
- **Offset-Quadrature Phase Shift Keying (O-QPSK):** also known as staggered QPSK. The mutual timing of the symbol stream $I(t)$ and $Q(t)$ is shifted such that the alignment of the two streams is offset by T_b. There are no zero crossings in the vector diagram $\Rightarrow$ **lower parasitic AM** related to QPSK.
- **π/4-Quadrature Phase Shift Keying (π/4-QPSK):** Between two consecutive incoming dibits the **carrier is shifted by 45°.** The maximum phase shift is then 135° $\Rightarrow$ **lower parasitic AM** related to QPSK, more complex demodulation.
- **π/4-Differential Quadrature Phase Shift Keying (π/4-DQPSK):** each dibit defines specific carrier phase shift related to previous value. The maximum phase shift is also 135° $\Rightarrow$ **lower parasitic AM** related to QPSK. It is used in radiotelephone systems D-AMPS (USA) and JDC (Japan).

7.3.8 8 Phase Shift Keying

M = 8, **8PSK: Carrier takes eight possible phase states – usually** $\pm 22.5°, \pm 67.5°, \pm 112.5°, \pm 157.5°$**. Obtained QPSK waveform sets then is:**

$$s(t) = S_0 \sin\left[2\pi f_0 t + (2i-1)\frac{\pi}{8}\right]$$

8PSK modulator

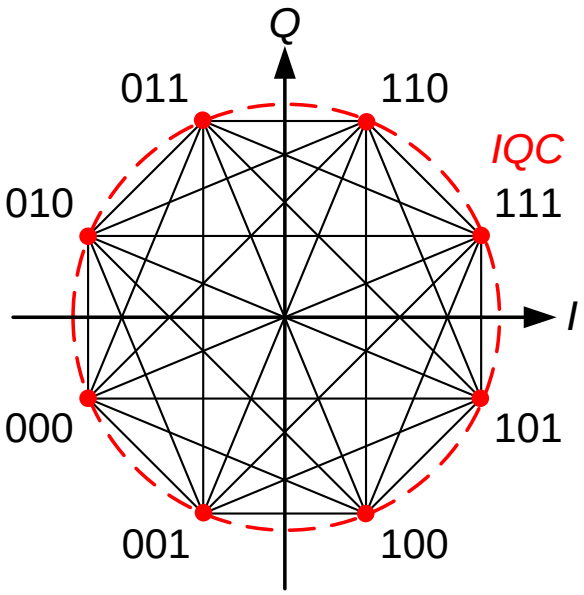


7.3.8 8 Phase Shift Keying

Example of a coding table

I	Q	C	I_{MSB}	I_{LSB}	Q_{MSB}	Q_{LSB}	PAM (A) $I(t)$	PAM (B) $Q(t)$
0	0	0	0	0	0	1	-0,92	-0,38
0	0	1	0	1	0	0	-0,38	-0,92
0	1	0	0	0	1	0	-0,92	0,38
0	1	1	0	1	1	1	-0,38	0,92
1	0	0	1	0	0	0	0,38	-0,92
1	0	1	1	1	0	1	0,92	-0,38
1	1	0	1	0	1	1	0,38	0,92
1	1	1	1	1	1	0	0,92	0,38

Vector diagram



Properties:

- **Good spectrum efficiency (theoreticaly** 3 bit/s/Hz**).**
- **Difficult carrier recovery (phase uncertainty** $\pm\pi/8$**).**
- **Large parasitic AM.**
- **Applied in GSM EDGE.**

7.3.9 Minimum Shift Keying

M = 2, **MSK. The MSK can be viewed as either a special case of Continuous Phase Frequency Shift Keying (CPFSK), or a special case of O-QPSK with sinusoidal symbol weighting.** CPFSK family is characterized by a continuous change of the carrier phase when changing its frequency. CPFSK can generally be realized e.g. by a voltage-controlled oscillator (VCO).

- **During the symbol period the carrier frequency is constant ⇒ phase grows linearly**
- **It uses the two signaling frequencies:** $f_1 = f_0 - \Delta f = 1/T_1$, $f_2 = f_0 + \Delta f = 1/T_2$.
- **Condition for achiewing of a continuous phase is:**

$$T_b = k\frac{T_1}{2} \Rightarrow f_1 = k\frac{R_b}{2}, \qquad T_b = (k+1)\frac{T_2}{2} \Rightarrow f_2 = (k+1)\frac{R_b}{2}$$

$$\Rightarrow \quad \Delta f = \frac{f_2 - f_1}{2} = \frac{R_b}{4}, \qquad \beta = \frac{\Delta f}{R_b/2} = 0.5$$

- **Instant frequency depends on incoming bit:** $n_i = \pm 1$, **then** $f_i = f_0 + \Delta f n_i$, $i = 0,1$.
- **Phase variation during** *i*-ith **symbol duration:** $\Delta\Phi_i(t) = 2\pi\Delta f n_i T_b = \pm\pi/2$

7.3.9 Minimum Shift Keying

- **MSK signal is then:** $s(t) = S_0 \cos\left[2\pi\left(f_0 + n_i \frac{R_b}{4}\right)t\right] =$

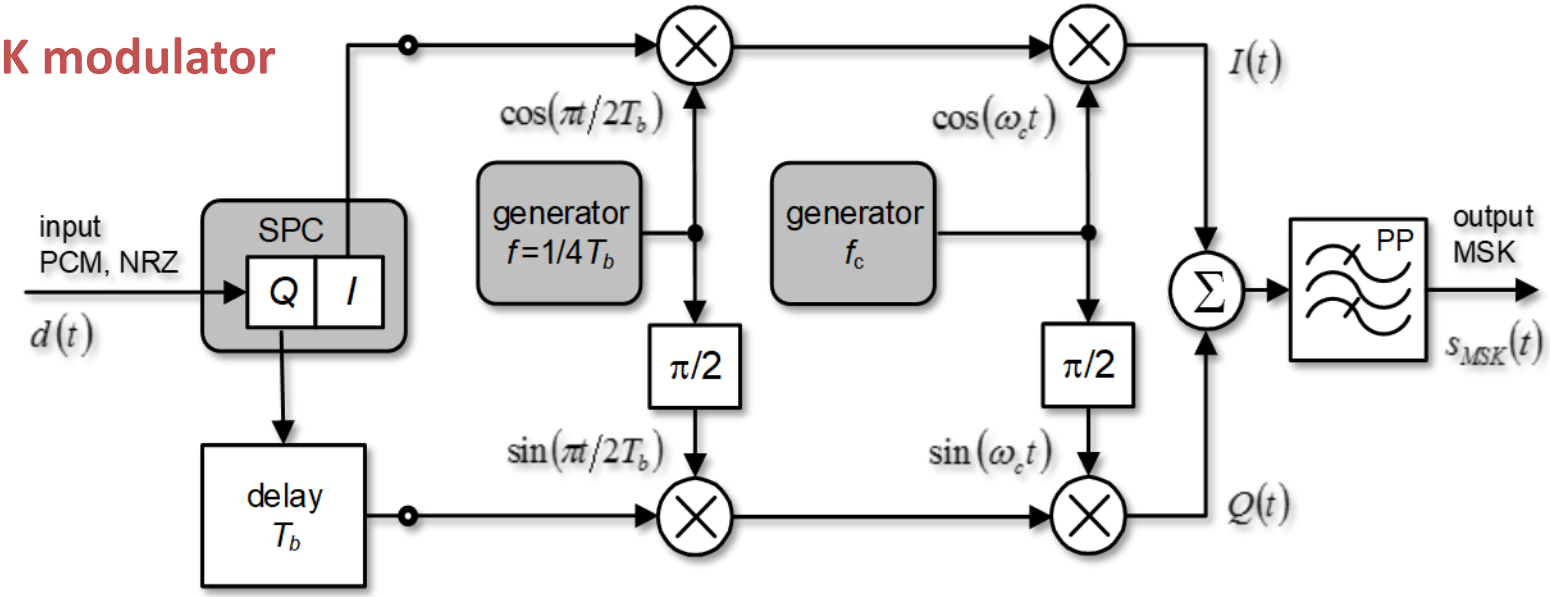
QAM

$$= \underbrace{S_0 \cos\left(2\pi n_i \frac{R_b}{4} t\right)}_{I(t)} \cos 2\pi f_0 t - \underbrace{S_0 \sin\left(2\pi n_i \frac{R_b}{4} t\right)}_{Q(t)} \sin 2\pi f_0 t$$

AM AM

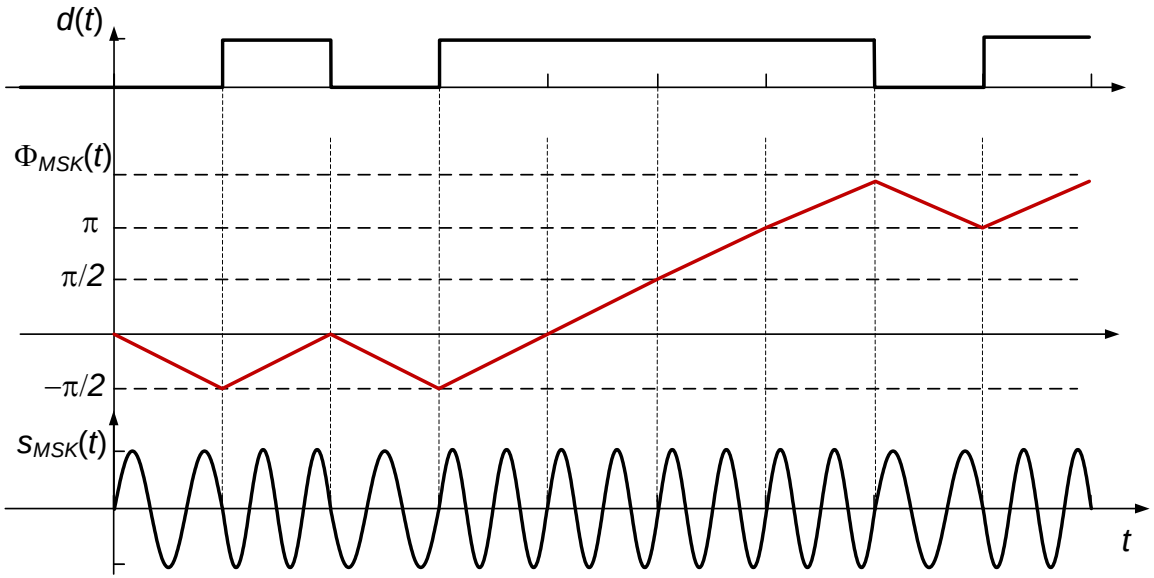
- **MSK can also be generated by a quadrature modulator. (O-QPSK with sinusoidal symbol weighting, because** $\cos x = \sin(x - \pi/2)$**).**

MSK modulator

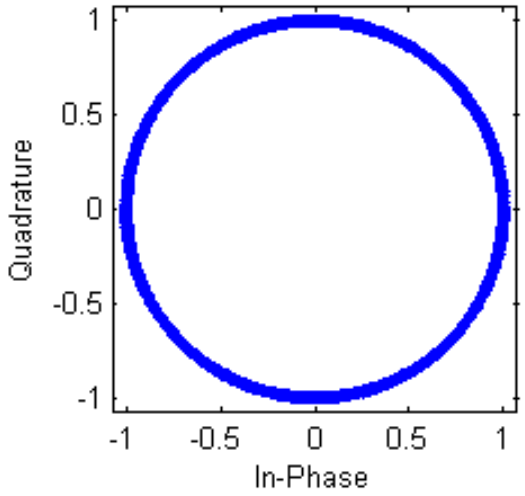


7.3.9 Minimum Shift Keying

Example of MSK modulation:



MSK vector diagram

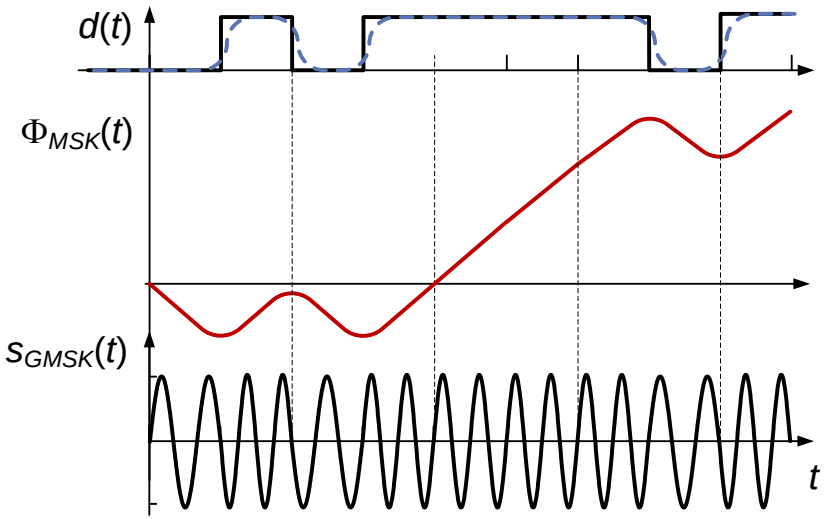


Properties:

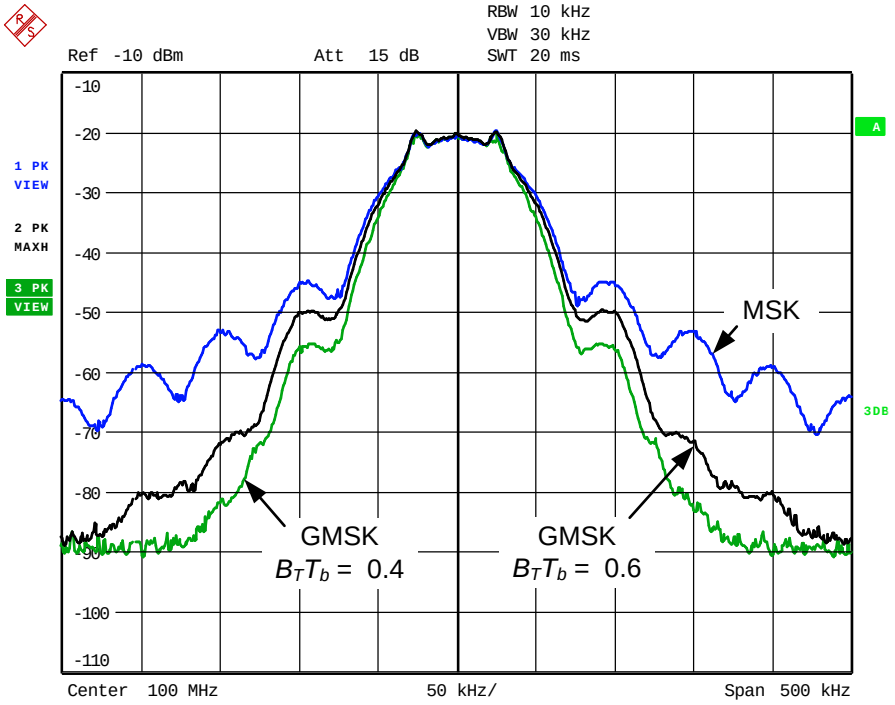
- **Possibility of incoherent demodulation,**
- **Good spectral and energetic efficiency .**

7.3.10 Gaussian minimum Shift Keying

Symbols are fed into the MSK modulator through *Gaussian Low Pass Filter* (GLPF) (its behavior is defined by the BT_b parameter) ⇒ frequency limitation of the input data ⇒ modulated GMSK signal has substantially suppressed side-lobes in the spectrum. Output signal does not require any additional filtering.



Spectrum GMSK for two parameters BT_b



Application:

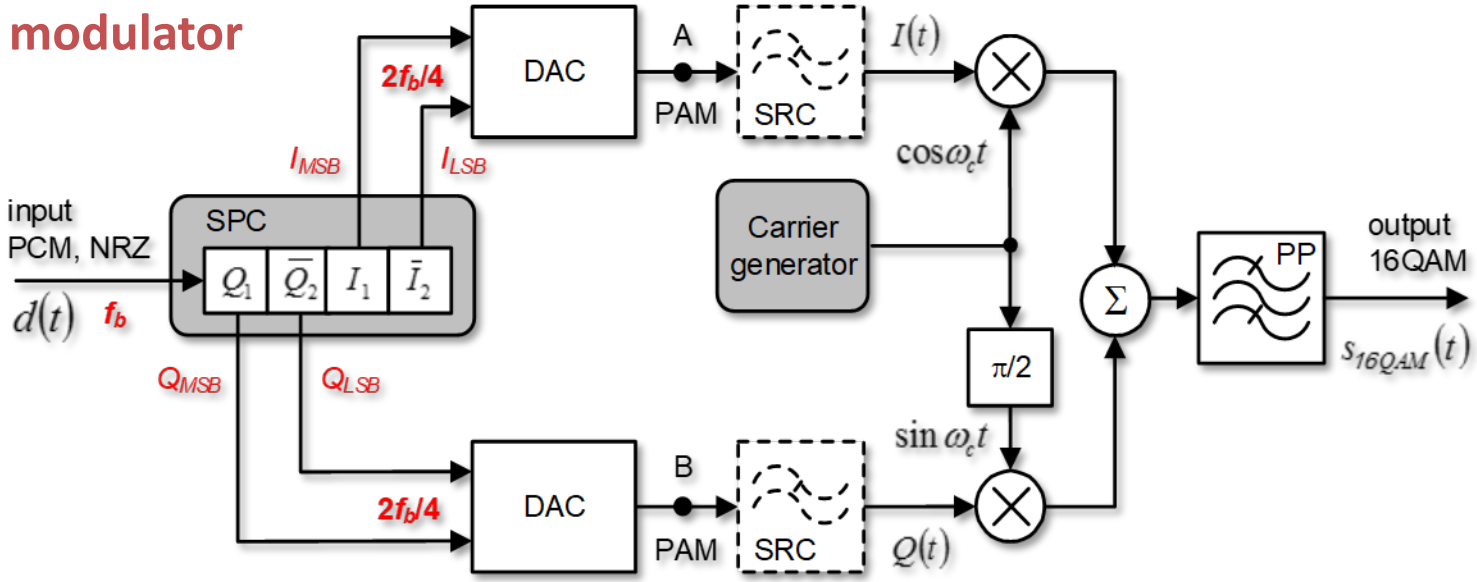
- **Modulation of the voice in radiotelephone network GSM.**

7.3.11 16 QAM (Quadrature Amplitude Shift Keying)

M = 16, **16QAM.** **The QAM signaling can be viewed as a combination of amplitude shift keying and phase shift keying, giving rise to the alternative name, amplitude phase keying (APK).**

$$s(t) = S_0(t)\sin[2\pi f_0 t + \varphi_0(t)]$$
$$= \underbrace{S_0(t)\cos\varphi_0(t)}_{I(t)}\sin 2\pi f_0 t + \underbrace{S_0(t)\sin\varphi_0(t)}_{Q(t)}\cos 2\pi f_0 t$$

16 QAM modulator



7.3.11 16 QAM (Quadrature Amplitude Shift Keying)

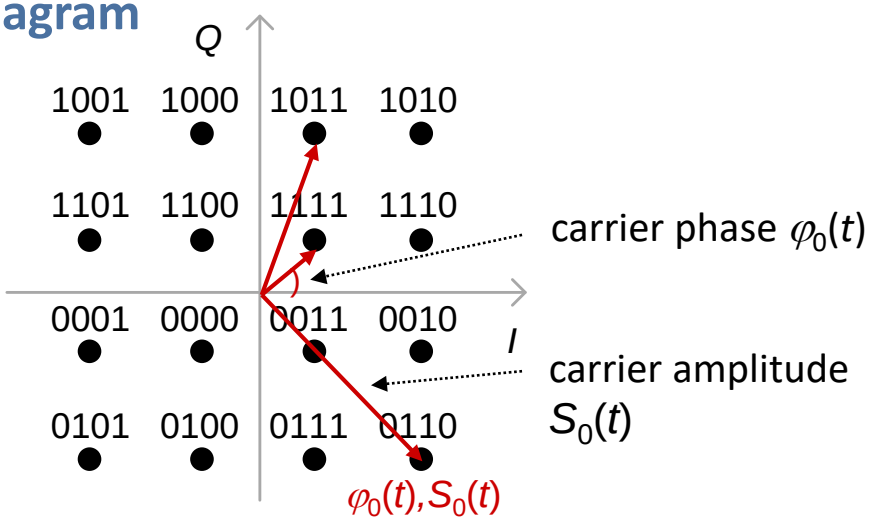
Properties:

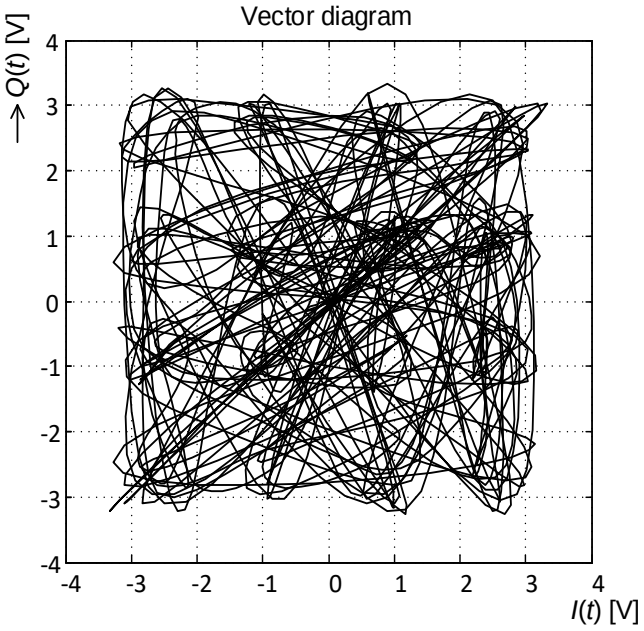
- **Very good spectral efficiency.**
- **Non-constant envelope (linear modulation).**

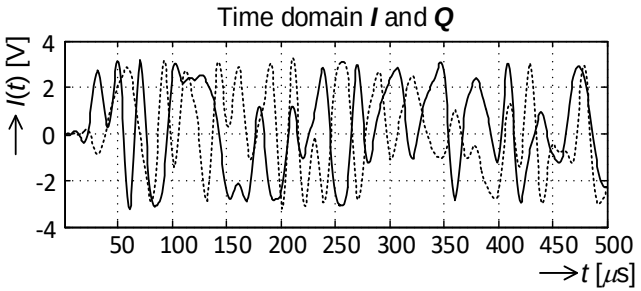
Application:

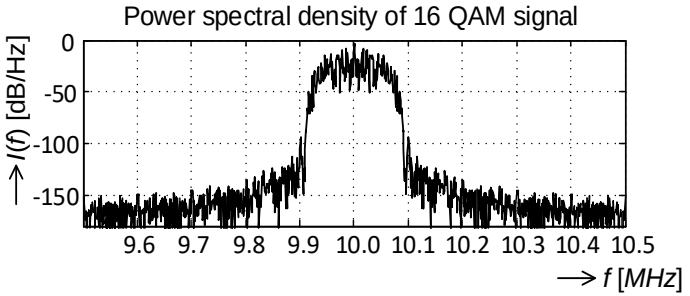
- **DVB, member of QAM adaptive. modulation formats in ADSL, WiFi.**

Constellation diagram



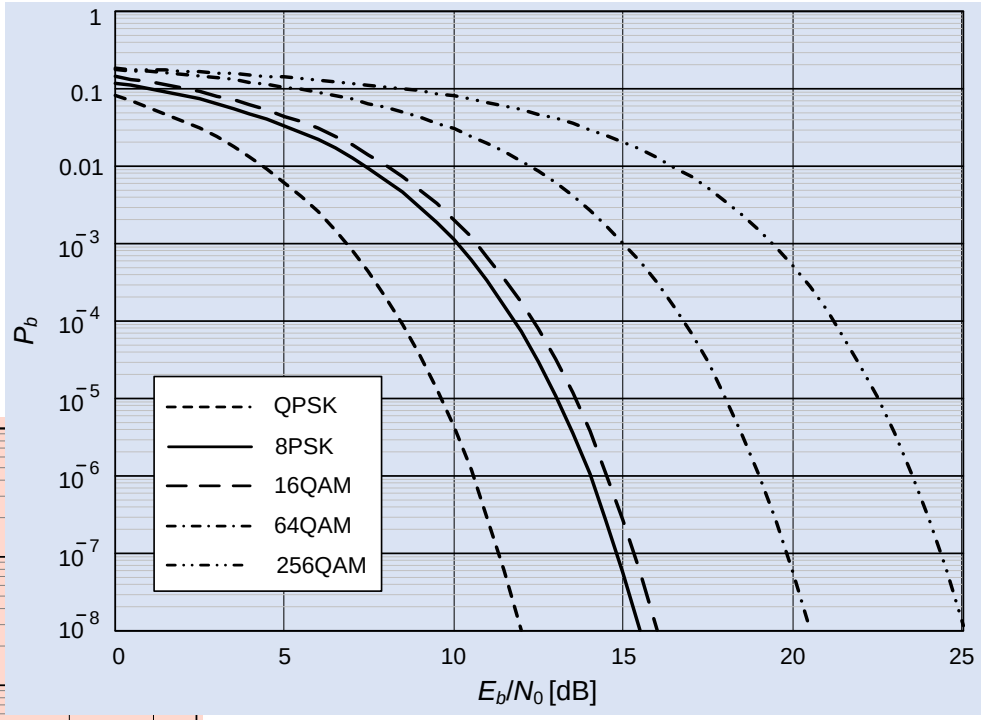


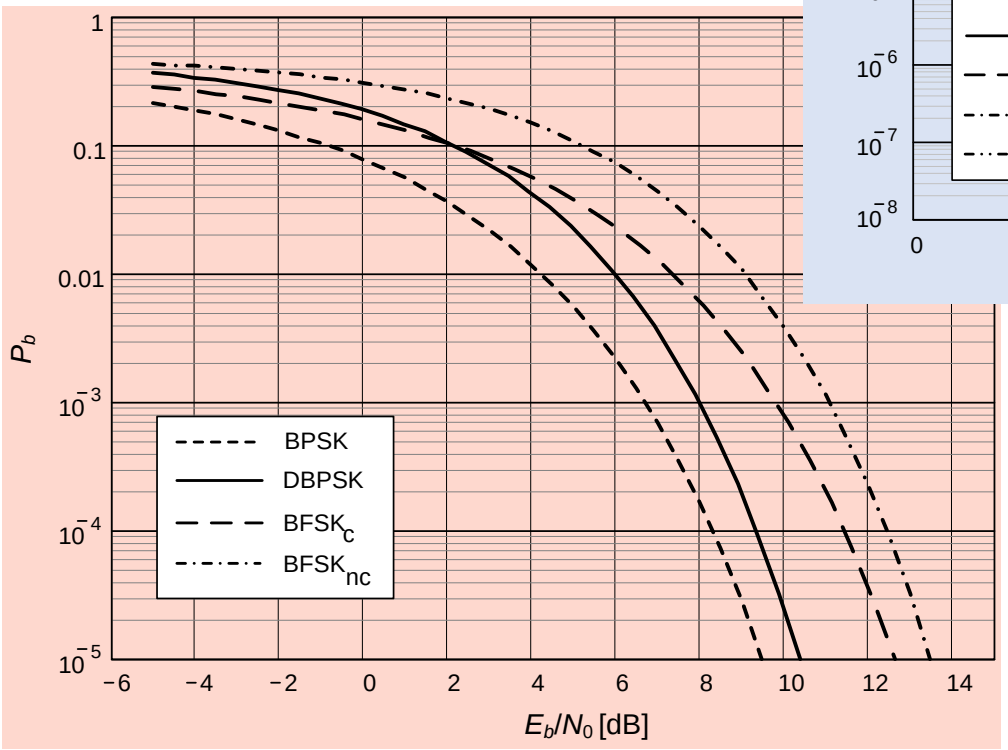




7.3.12 Characteristics of digital modulations

Bit error probability of digital modulations for AWGN channel →



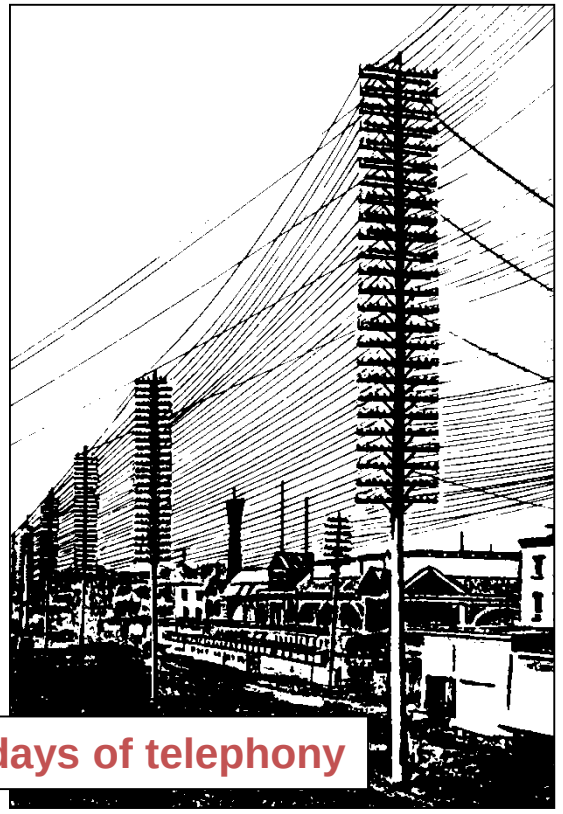


← **Bit error probability of binary digital modulations for AWGN channel (nc – non-coherent, c – coherent demodulation)**

8. MULTIPLE ACCESS
8.1 Deterministic Multiple access techniques overview

A communications resource (CR) represents the time and bandwidth that is available for communication associated with a given system.
The terms "multiplexing" and "multiple access" refers to the sharing of a CR. The basic ways of communications resources are the following:

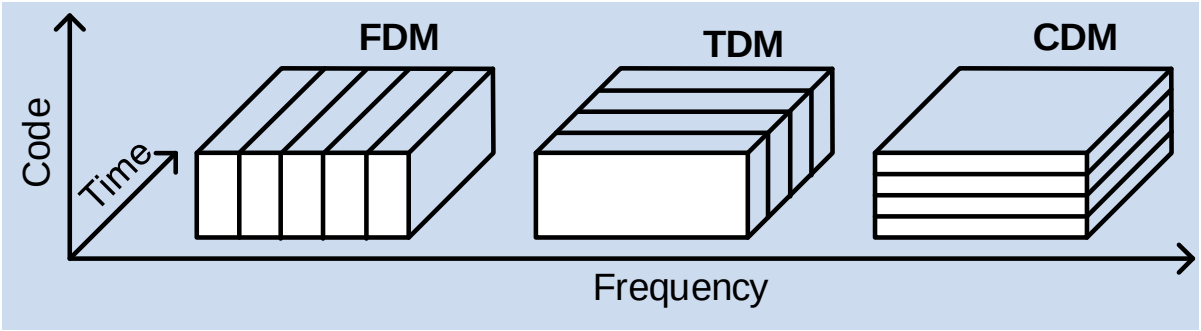
- **Frequency Division Multiple Access (FDMA)**
  Specified sub-bands of frequency are allocated to a particular user.
- **Time Division Multiple Access (TDMA)**
  Periodically recurring time slots are identified. In dependence on TDMA technique used, users may access the resource at fixed or randomly generated time intervals.
- **Code Division Multiple Access (CDMA)**
  Specified members of a set of orthogonal spread spectrum codes (each using the full channel bandwidth) are allocated.



Early days of telephony

8.1 Deterministic Multiple access techniques overview

Above basic multiple access techniques are based on multiplexing methods FDM (*Frequency Division Multiplex*), TDM (*Time Division Multiplex*) and CDM (*Code Division Multiplex*), which can be graphically interpreted as follows:

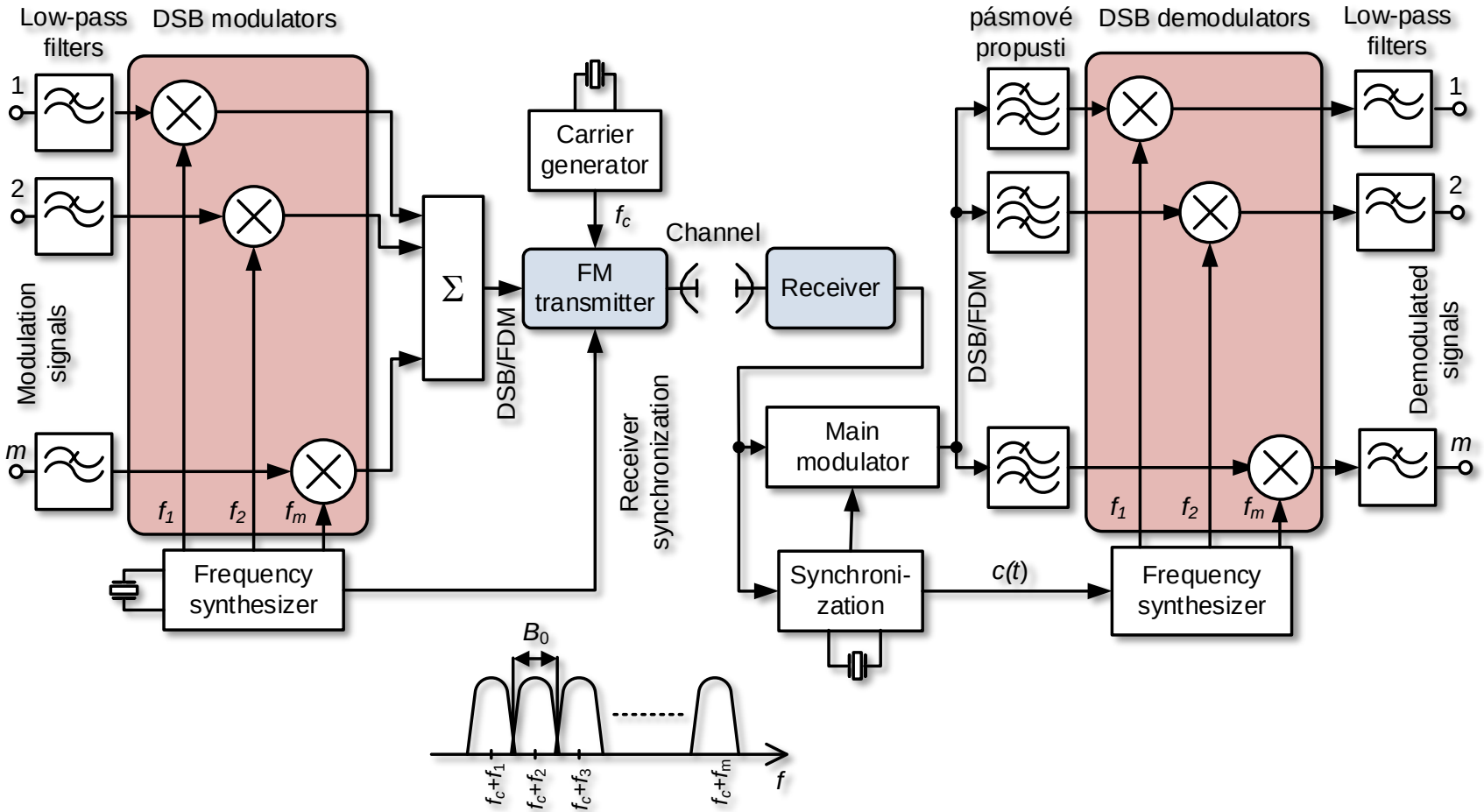


Sometimes also following techniques are included into the access techniques

- **Space Division Multiple Access (SDMA)** or multiple beam frequency reuse. Spot beam antennas (antennas with narrow radiating pattern) are used to separate RF signals by pointing in different directions. It allows for reuse of the same frequency band.
- **Polarization Division Multiple Access (PDMA)** or dual polarization frequency reuse. Orthogonal polarizations (most often vertical and horizontal) are applied to separate signals allowing to reuse of the same frequency band.

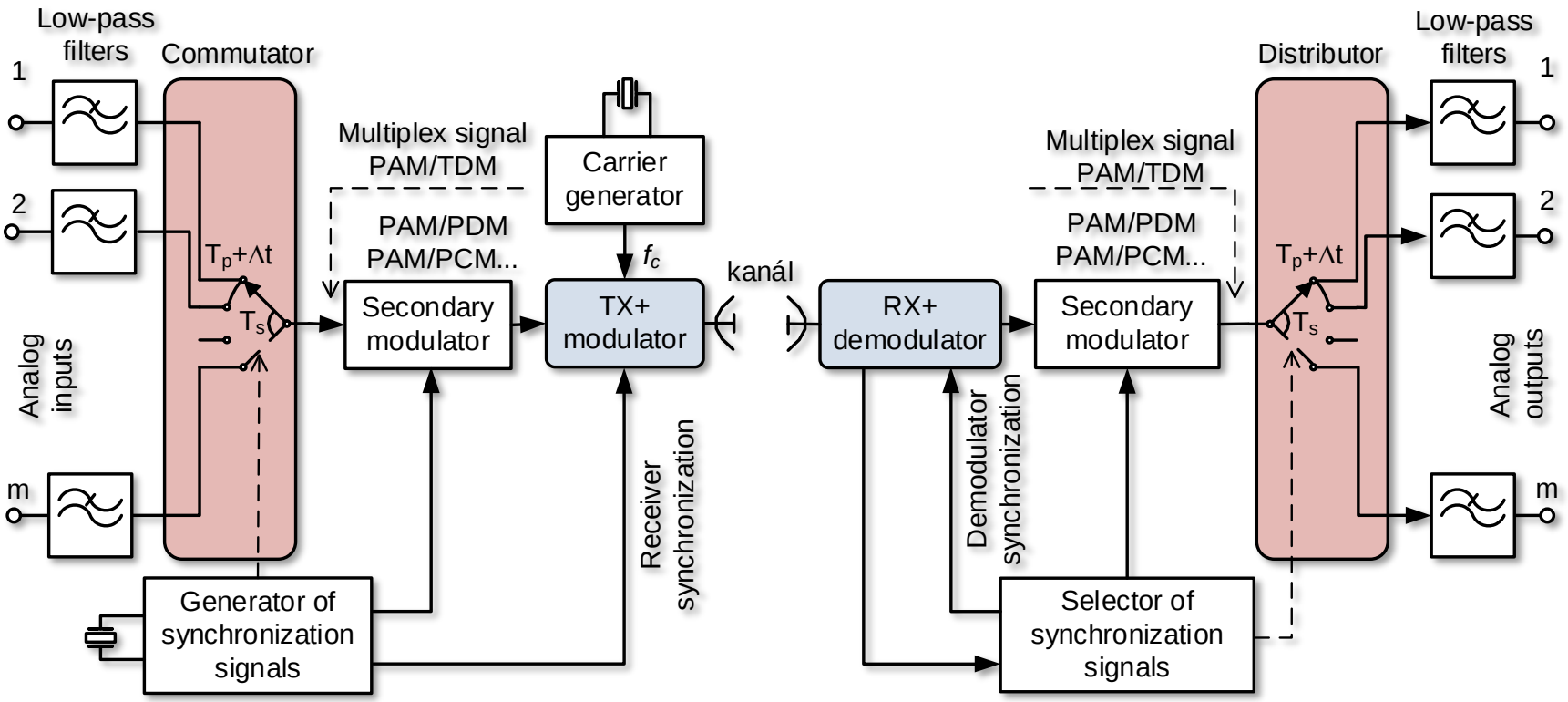
8.1 Deterministic Multiple access techniques overview

Frequency division multiple access - example



8.1 Deterministic Multiple access techniques overview

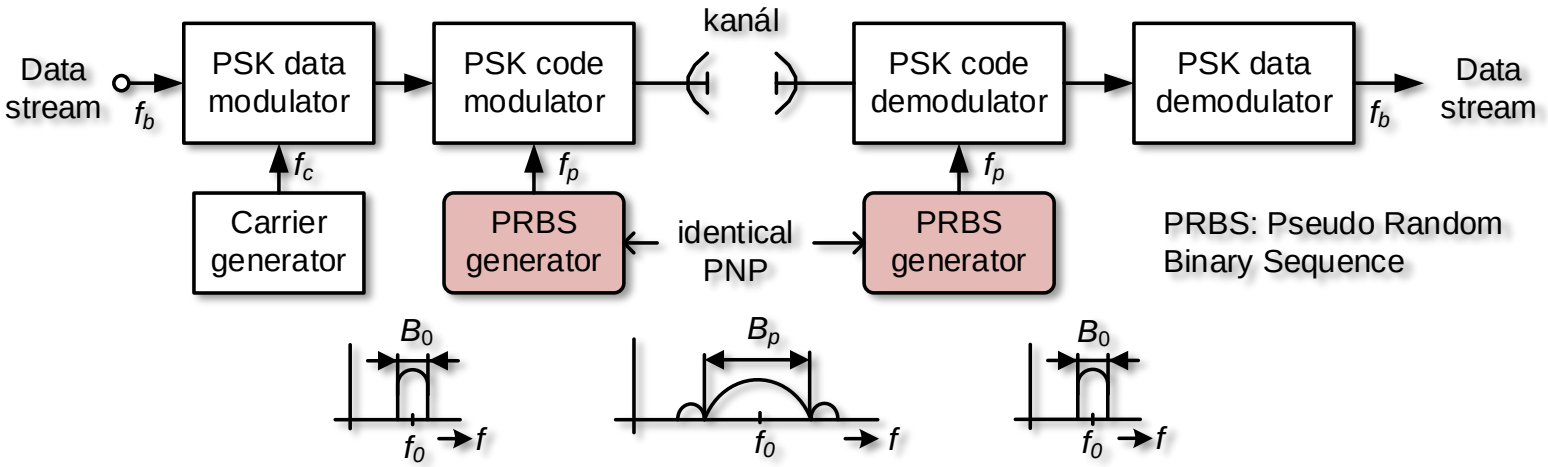
Time division multiple access - example



8.1 Deterministic Multiple access techniques overview

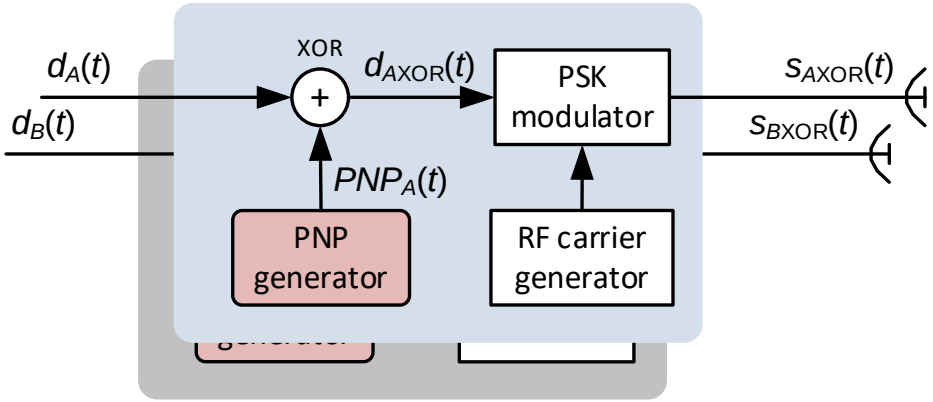
Code division multiple access – example

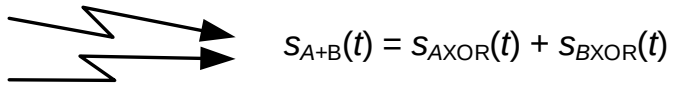
Direct sequence spread spectrum

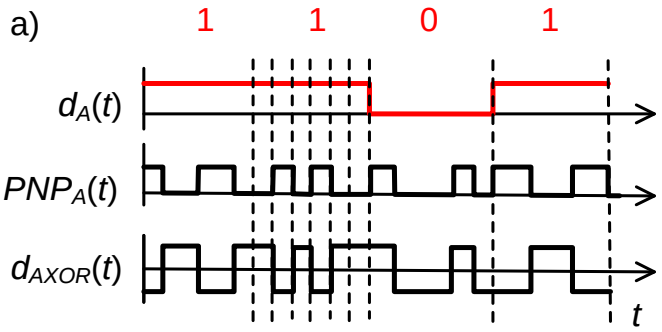


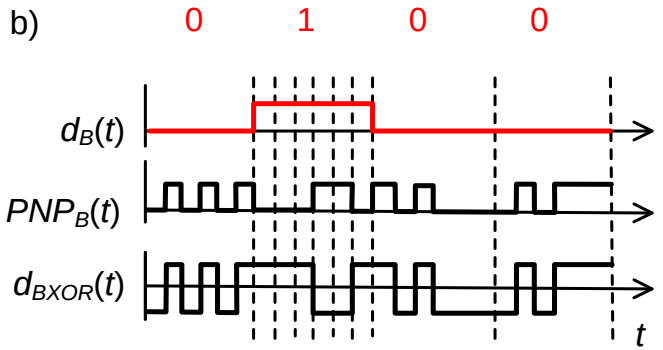
- Each user is distinguished by its own PRBS code.
- PRBS applied in TX on data modulated signal spreads spectrum of the output RF signal.
- PRBS code has to be synchronously generated in the receiver (rough synchronization = **acquisition**, fine synchronization = **tracking**).
- Process of de-spreading (PRBS adding) applied in RX enhances SNR and system resistance against both broadband and narrowband interference and noise in the channel.
- Requirements placed on PRBS are **impulse autocorrelation** function and **zero cross-correlation** function **(Hadamar, Walsh, Barker, Gold** and **Huffman sequences).**

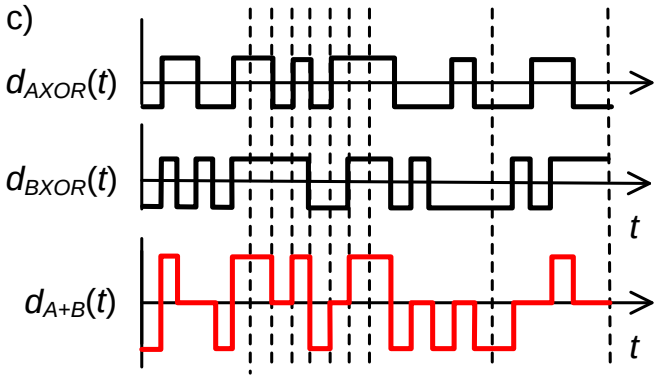
8.1 Deterministic Multiple access techniques overview











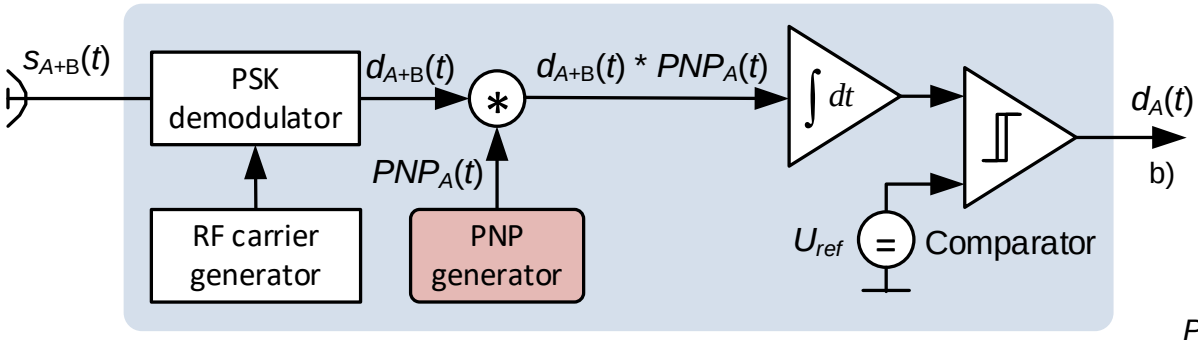
Example of creating two SS-DS systems.

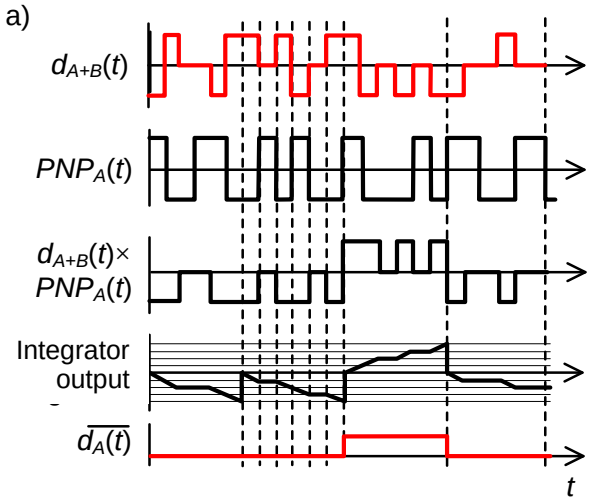
a) generating a transmitted signal A,

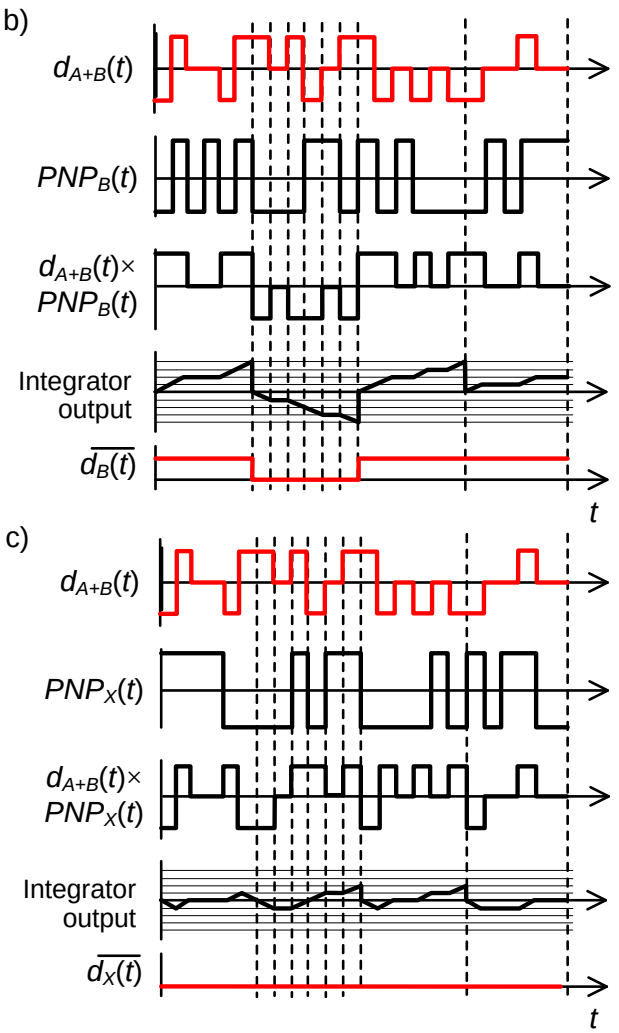
b) generating a transmitted signal B,

c) generating a final signal

8.1 Deterministic Multiple access techniques overview







Example of processing of SS-DS signals.

a) signal detection of transmitter A,

b) signal detection of transmitter B,

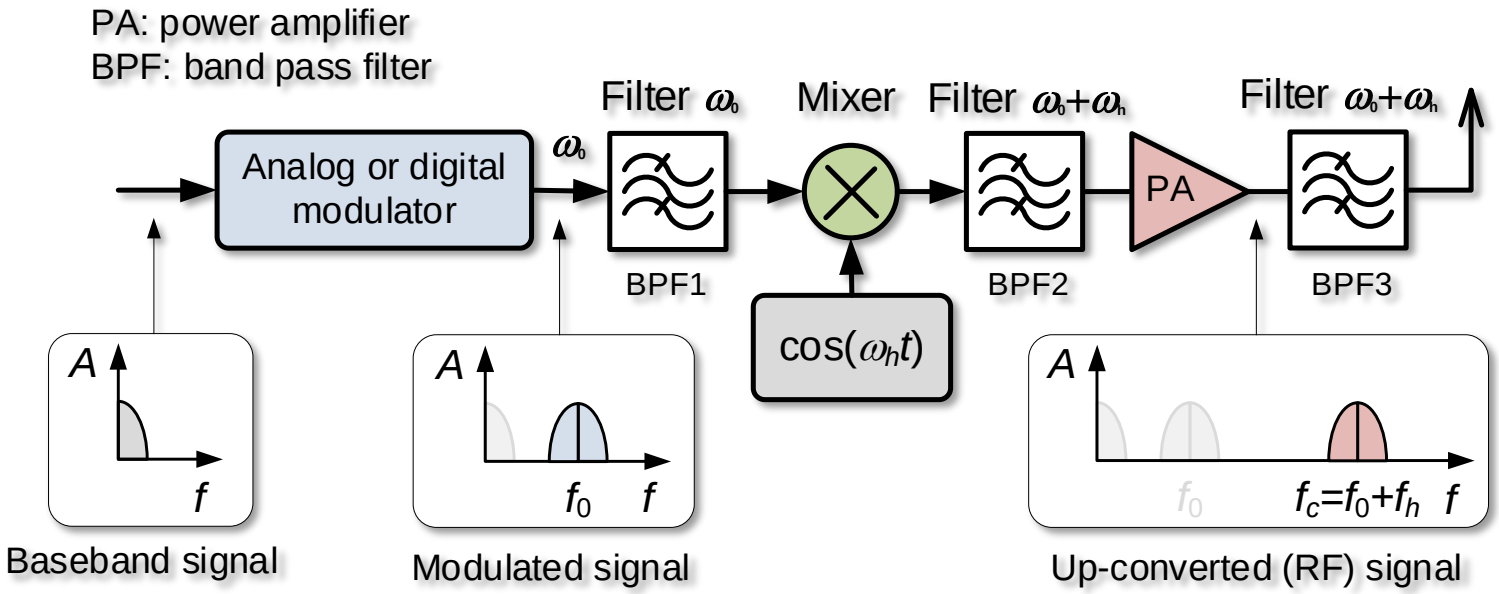
c) signal detection of another transmitter X

8.2 Stochastic Multiple access techniques overview

- **ALOHA: developed in 1971 at the University of Hawaii, used in satellite communication.**
  1. **Users transmit at any time they messages protected by an error detection code to a satellite.**
  2. **Users listen for an acknowledgment (ACK) from the satellite receiver. Transmissions from different users will sometimes overlap in time, causing reception errors. In this case the users receive a negative acknowledgment (NAK).**
  3. **When a NAK is received, the messages are simply retransmitted. Not immediately but after a random delay to avoid another collision.**
- **CSMA/CD (Carrier-Sense Multiple Access/Collision Detect): developed by the Xerox Corporation, used in LAN, Ethernet.**
  1. **The user must not transmit when the carrier is present.**
  2. **The user may transmit if not deferring until the end of the packet or until a collision is detected.**
  3. **If a collision is detected, the user must terminate packet transmission and transmit a short jamming signal.**
  4. **The user must wait a random delay time (similar to the ALOHA system) and then attempt retransmission.**

9. WIRELESS INTERFACE
9.1 Transmitter (TX, XMT)

The transmitter converts a signal from output of a modulator (or generally from baseband) into a radio frequency (RF) band, where it is then converted into EM field using antenna.



Frequency up-conversion is performed in a mixer using signal from local oscillator (heterodyne) with frequency f_h. BPF2 suppress the signal of differential frequency, BPF3 suppress the spurs of PA caused by nonlinearities.

9.1 Transmitter (TX, XMT)

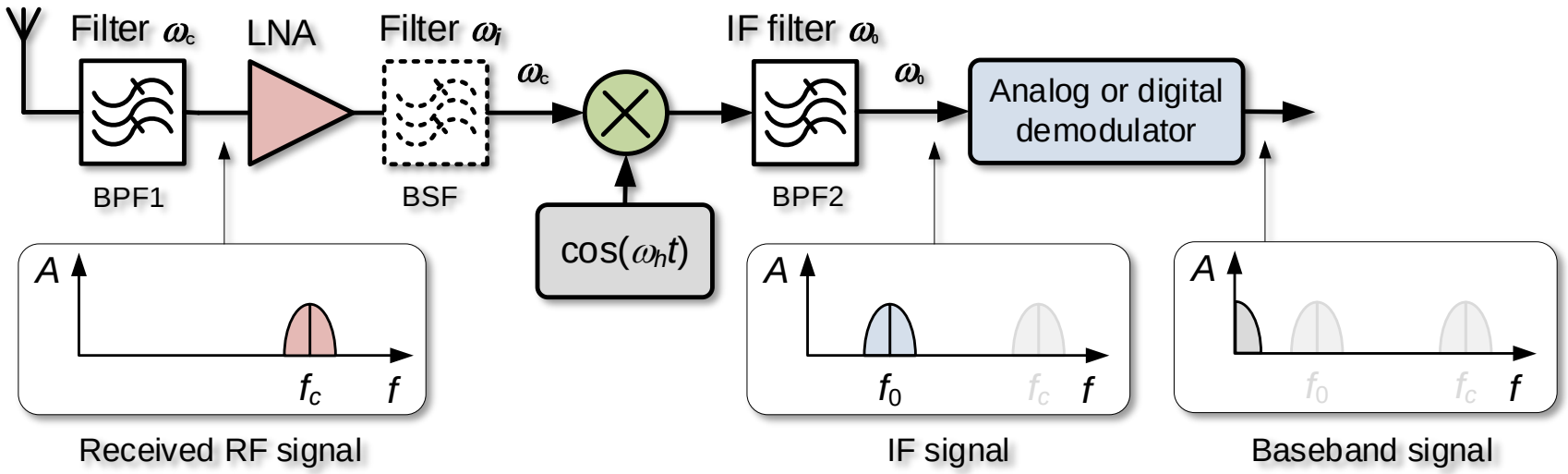
Principle of frequency up-conversion:

$$\cos\omega_0 \cos\omega_h = \tfrac{1}{2}\cos\underbrace{(\omega_0 + \omega_h)}_{\text{carrier freq.}} + \underbrace{\tfrac{1}{2}\cos(\omega_0 - \omega_h)}_{\text{supressed by the BPF2}}.$$

9.2 Receiver (RX, XMR)

Superheterodyne receiver converts EM field to RF signal at the carrier frequency f_c and then to an intermediate frequency (IF) f_0 (generally to the baseband).

LNA: low noise Amplifier, BPF: band pass filter, BSP: band stop filter

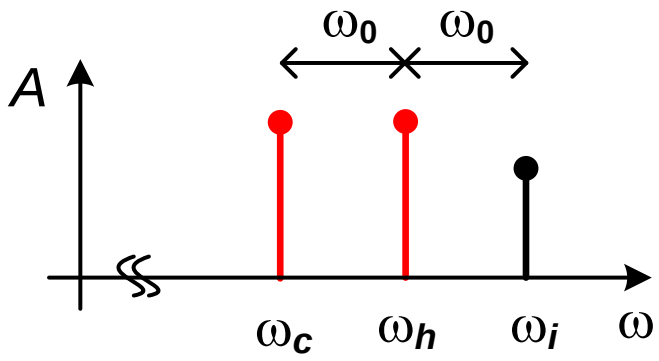


9.2 Receiver (RX, XMR)

Frequency down-conversion **is performed in a mixer using signal from the local oscillator (heterodyne) with frequency f_h. BPF1 selects required frequency band (transmitter) and eliminates the input noise, BPF2 suppress the signal of an additive frequency. Frequency f_i is the image frequency, which can cause reception of an undesired signal.**

Principle of frequency down-conversion:

$$\cos\omega_h \cos\omega_{c(i)} = \frac{1}{2}\cos\underbrace{\left(\omega_h + \omega_{c(i)}\right)}_{\text{Supressed by BPF}} + \frac{1}{2}\cos\underbrace{\left(\omega_h - \omega_{c(i)}\right)}_{\text{IF frequency } \omega_0}.$$



9.3 Radio frequency bands

Radio waves are electromagnetic waves of frequencies 10^4 Hz and higher.

Band	Frequency range (f)	Wavelength range (λ)
Very low frequency (VLF)	10 - 30 kHz	100 - 10 km
Long wave (LW)	30 - 300 kHz	10 - 1 km
Medium wave (MW)	300 - 3000 kHz	1000 - 100 m
Short wave (SW)	3 - 30 MHz	100 - 10 m
High frequency (HF)	30 - 300 MHz	10 - 1 m
Very high frequency (VHF)	300 - 3000 MHz	10- 1 dm
Ultra high frequency (UHF)	3 - 30 GHz	10 - 1 cm
Super high frequency (SHF)	30 - 300 GHz	10 - 1 mm
Extremely high frequency (EHF)	300 - 3000 GHz	1 - 0,1 mm

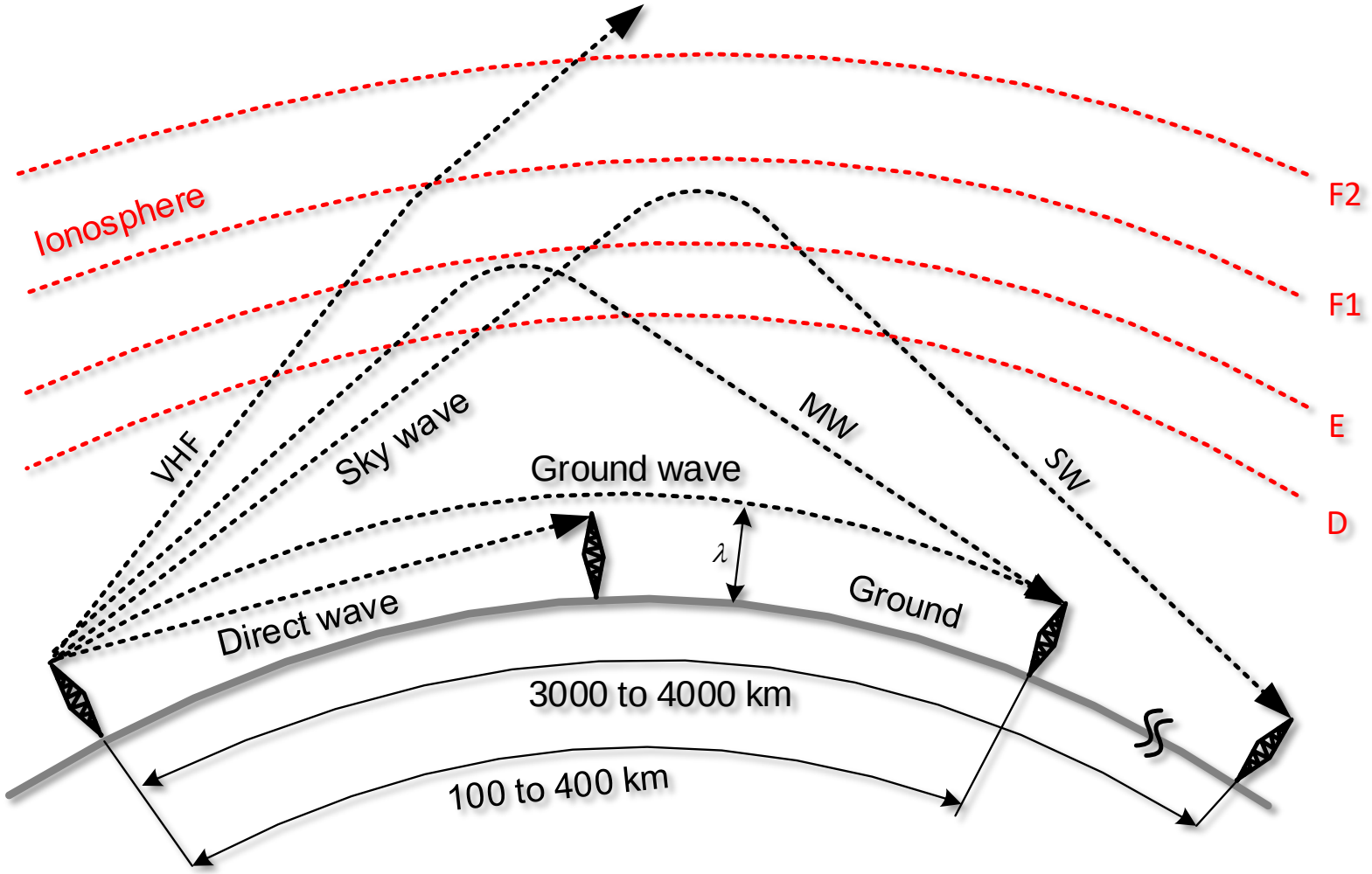
9.3 Radio frequency bands

Wave propagation types:

- **Ground (surface) waves: LW, MW, SW (during a day). Typical for the AM radio. They propagate along the surface and are absorbed by ground.**
- **Sky waves: MW, SW (2 MHz to 30 MHz). Typical for the AM (SSB) radio. Are reflected from the ionosphere formed by a few layers (D, E, F1, F2) with different properties. Suitable for communication at very long distance.**
- **Direct waves: VHF and higher frequencies. Typical for the TV broadcasting, microwave radio relay transmission, radars, etc. The waves behave like a light, can be shadowed and reflected.**

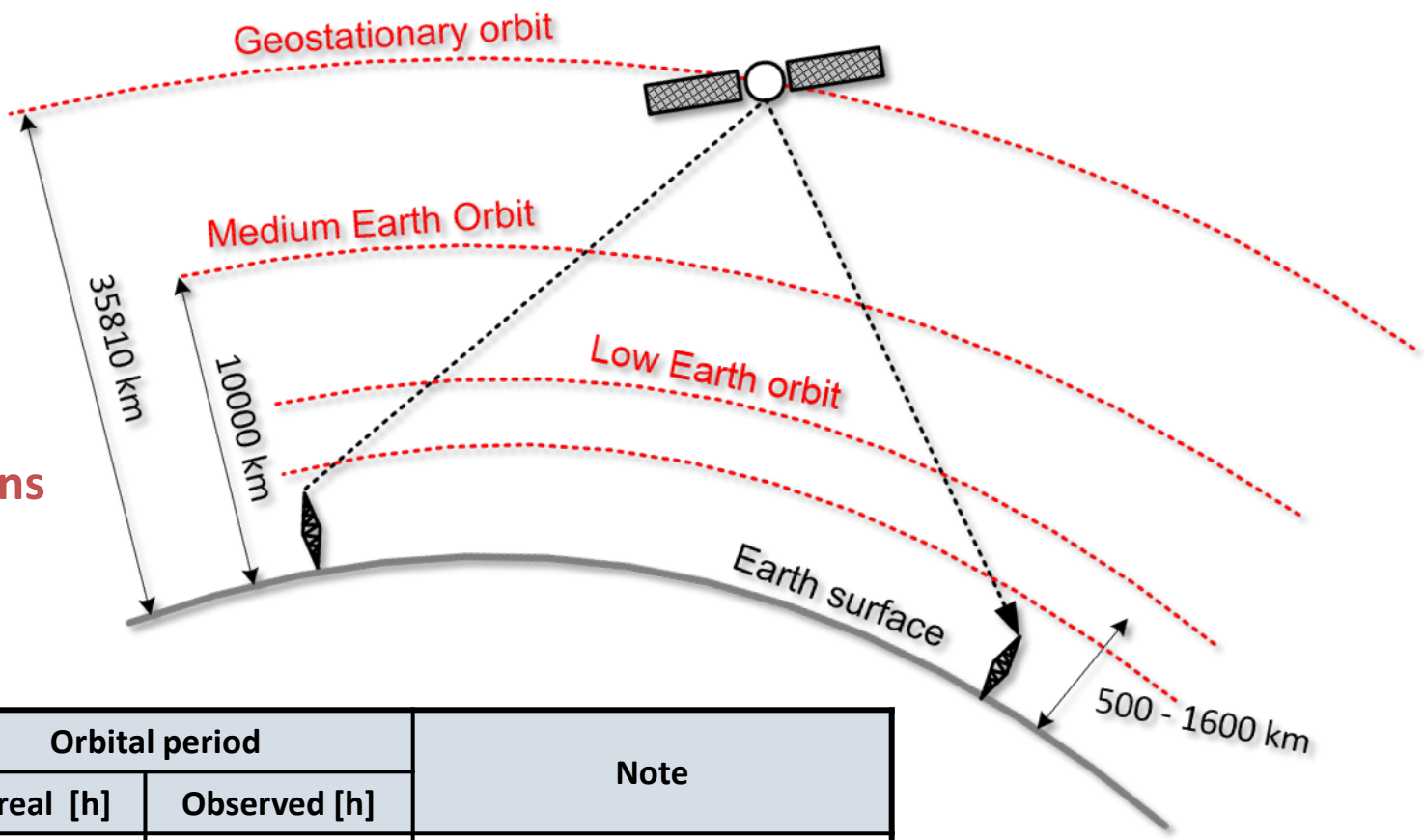
9.3 Radio frequency bands

Wave propagation types



9.3 Radio frequency bands

Long distance communications in UHF band



Orbit height [km]	Orbital period		Note
	Sidereal [h]	Observed [h]	
1600	2	2.2	Low Earth Orbit (LEO)
10000	6	8	Medium Earth Orbit (MEO)
16000	9.3	12	
35810	24	∞	Geostationary orbit

9.4 Friis transmission equation

$$P_T G_T \left(\frac{\lambda}{4\pi d} \right)^2 L_\varphi L_P \frac{G_R}{kT_0} = \frac{P_R}{N_0}$$

$P_T G_T$:	Effective isotropic radiated power (EIRP).
G_T:	Transmitter antenna gain (related to isotropic dipole).
λ:	Wavelength.
d:	Distance between transmitter and receiver antennas.
$N_0 = kT_0$:	Power spectral density of noise.
G_R:	Receiver antenna gain (related to isotropic dipole).
P_R:	Received power.
L_φ:	Polarization loss.
L_P:	Loss due to imperfect antenna alignment.
k:	Boltzmann constant.

9.5 Transmission techniques

- **Simplex:** communication that is performed in one direction only. Used e.g. in TV and radio broadcasting.
- **Half-duplex:** system enables communication in both directions, but only in one direction at a particular time (not simultaneously). Used e.g. in land services – ambulance, army, emergency rescue.
- **Full-duplex:** system allows communication in both directions simultaneously. Typical application in land-line telephone networks, radio telephone networks (GSM), Ethernet using of two (even only one) physical pairs of twisted cable, …

9.6 Circuit/packed-switched networks

- **Circuit switching** establishes dedicated communications channel (circuit) through the network for two nodes before they may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the entire duration of the communication session.
- **Packet switching** splits the data to be transmitted into small units, called packets. Packets are labelled with the destination and may be routed independently through the network via a different paths. Packet switching shares available bandwidth between multiple communication sessions.

10. SYNCHRONIZATION

10.1 Synchronization techniques overview

- **Carrier Recovery:** circuit used to estimate and compensate for frequency and phase deviation between a received carrier wave and the wave generated by receiver local oscillator for the purpose of coherent demodulation.
- **Symbol Timing Recovery:** Recovery of the received symbols clock in order to achieve optimum symbol detection and signal demodulation.
- **Frame Synchronization:** almost all digital data streams have some kind of frame structure. Frame synchronization is the process by which a specific frame alignment markers (known bit sequences) are identified in a stream of incoming framed data.
- **Network Synchronization:** for communications systems that involve many users accessing a central communication node (satellite communication systems) the network synchronization techniques have to be performed together for all users. Synchronization techniques can be centralized to a communication node or (more often) to terminals.

10.2 Carrier recovery

Recovery of the carrier frequency and phase. Two different approaches are used:

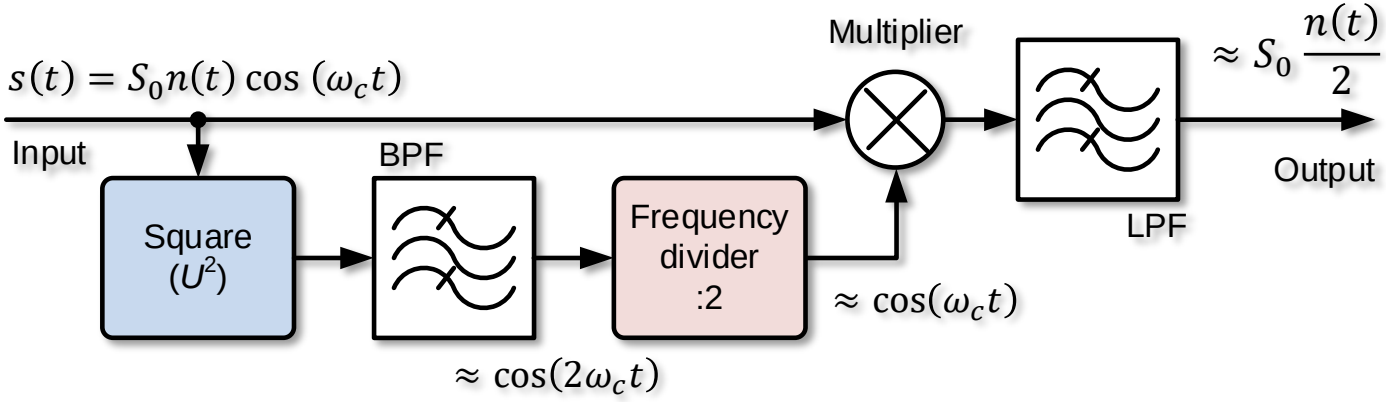
- **Unsuppressed carrier recovery: used for coherent AM (QAM) demodulation, consists in AM signal amplification, limitation, phase locking using PLL (*Phase Locked Loop*) and filtering.**
- **Suppressed carrier recovery: used for coherent PSK, QAM_{SC} and FSK demodulation. Consists in use of a squaring loop or Costas loop.**

Example: squaring loop in BPSK demodulation

$$s_1^2(t) = a^2 S_0^2 \cos^2(\omega_c t)$$

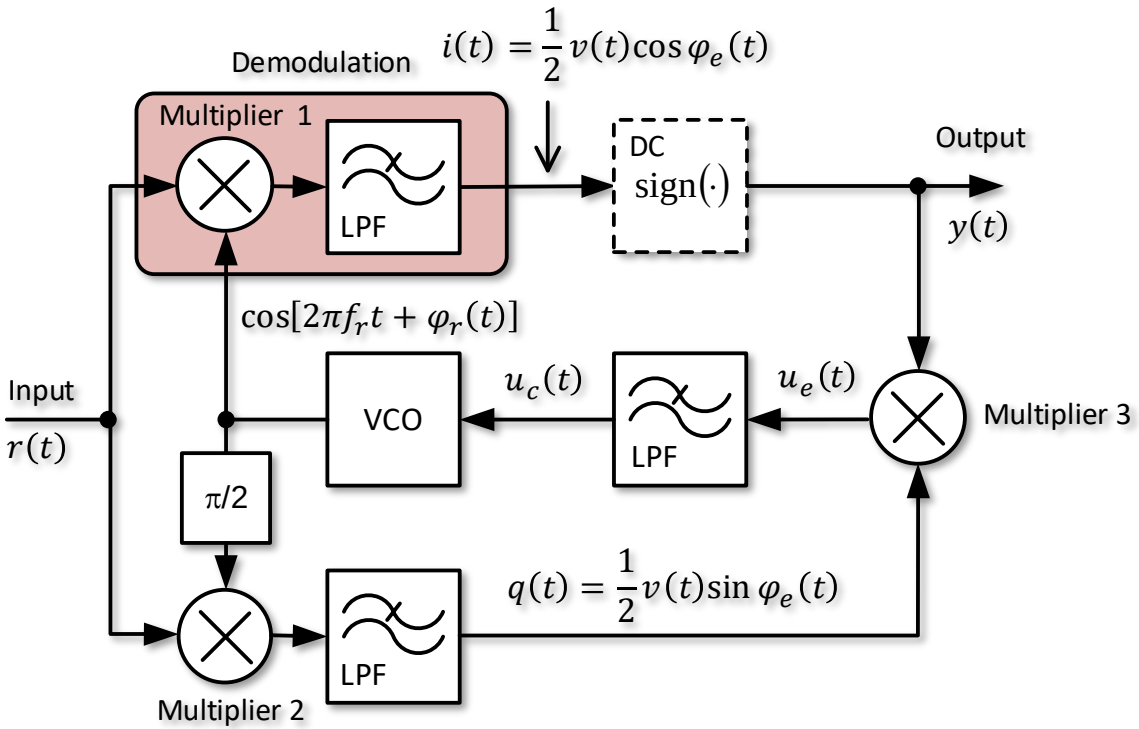
DC component — double frequency term

$$s_0^2(t) = (-a)^2 S_0^2 \cos^2(\omega_c t) = s_1^2(t) = a^2 S_0^2 \left[\frac{1}{2} + \cos(2\omega_c t)\right]$$



10.2 Carrier recovery

Costas loop for BPSK demodulation



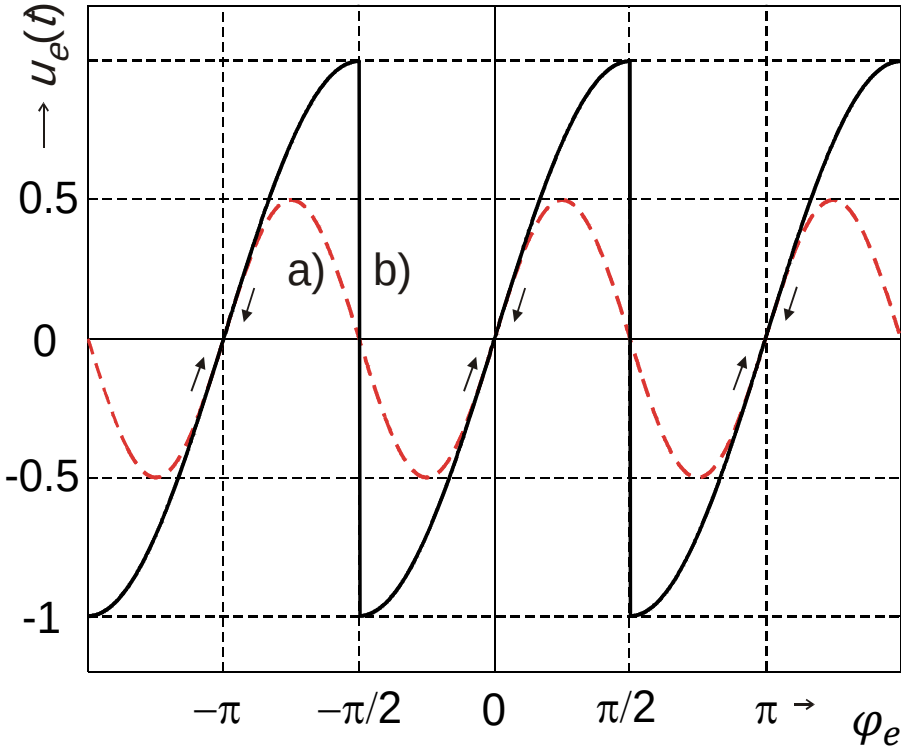
DC: Decision Circuit (Comparator)
LPF: Low-Pass Filter
VCO: Voltage Controlled Oscillator

Error voltage at N3 output: $u_e(t) \approx \sin\varphi_e(t)\big|_{\varphi_e \to 0}$

Output demodulated signal: $u_o(t) = \text{sign}\left[\frac{1}{2}n(t)\cos\varphi_e(t)\right] = \text{sign}[n(t)]\Big|_{\varphi_e(t)\to 0}$

10.2 Carrier recovery

Error voltage $u_e(t)$ dependence on phase difference a) without DC, b) with DC.

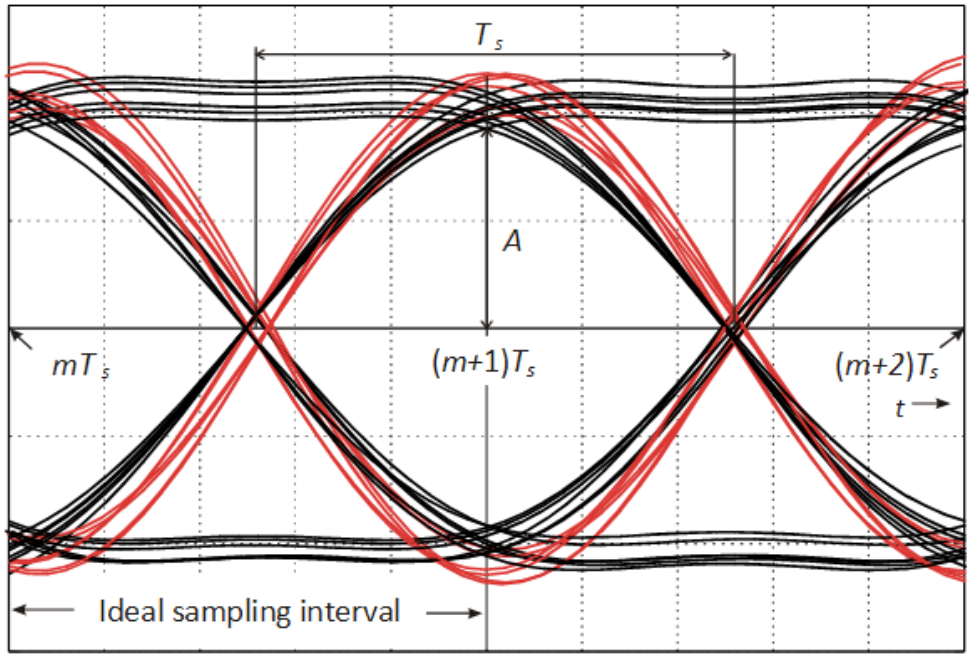


- **Costas loop can be used also for another modulation formats (*M*QAM or *M*PSK $M > 4$) , but in a modified connection.**

10.3 Symbol Timing Recovery

Optimal sample points of demodulated signal are multiples of T_s, where the symbol amplitude A is maximal (maximal opening of the eye).

Eye diagram



Two fundamental symbol synchronization techniques:

- **Data-aided**
- **Non data-aided**

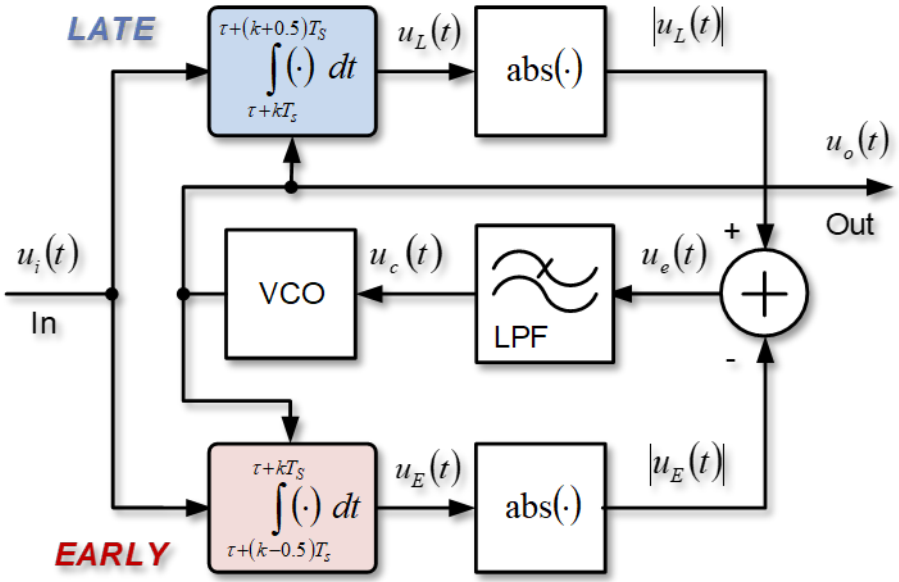
10.3 Symbol Timing Recovery

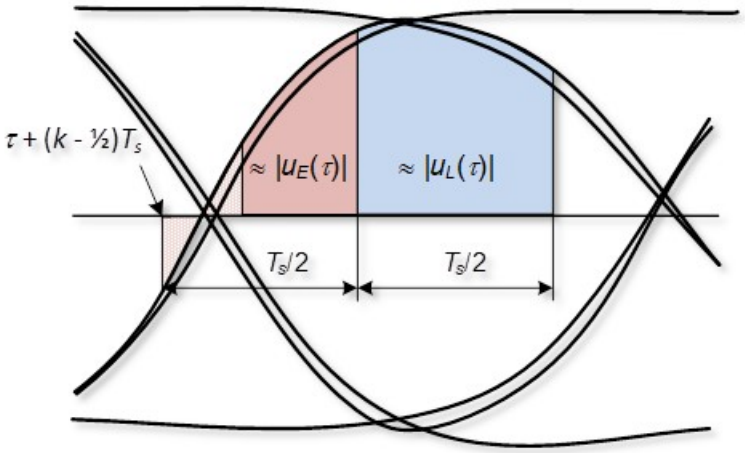
- *Data-Aided*: an additional information on symbol stream timing is transferred together with the symbols or by an auxiliary channel using
  - ✓ Time multiplex: known symbol sequences are inserted into the data stream. Receiver compares them with the same stored in internal memory and estimates the sampling period.
  - ✓ Frequency multiplex: required information (symbol period) is transferred on an auxiliary carrier.

- *Non Data-Aided*: no extra information is transferred together with the symbols. Information on sampling points are *extracted* from data stream.
  - ✓ Open-loop synchronizers: recover a replica of the transmitter data clock directly from operations on the incoming data stream.
  - ✓ Closed-loop synchronizers: attempt to lock a local data clock to the incoming signal by use of comparative measurements on the local and incoming signals (Early-late synchronizer). Closed-loop methods tend to be more accurate, but they are much more costly and complex.

10.3 Symbol Timing Recovery

Early-late synchronizer

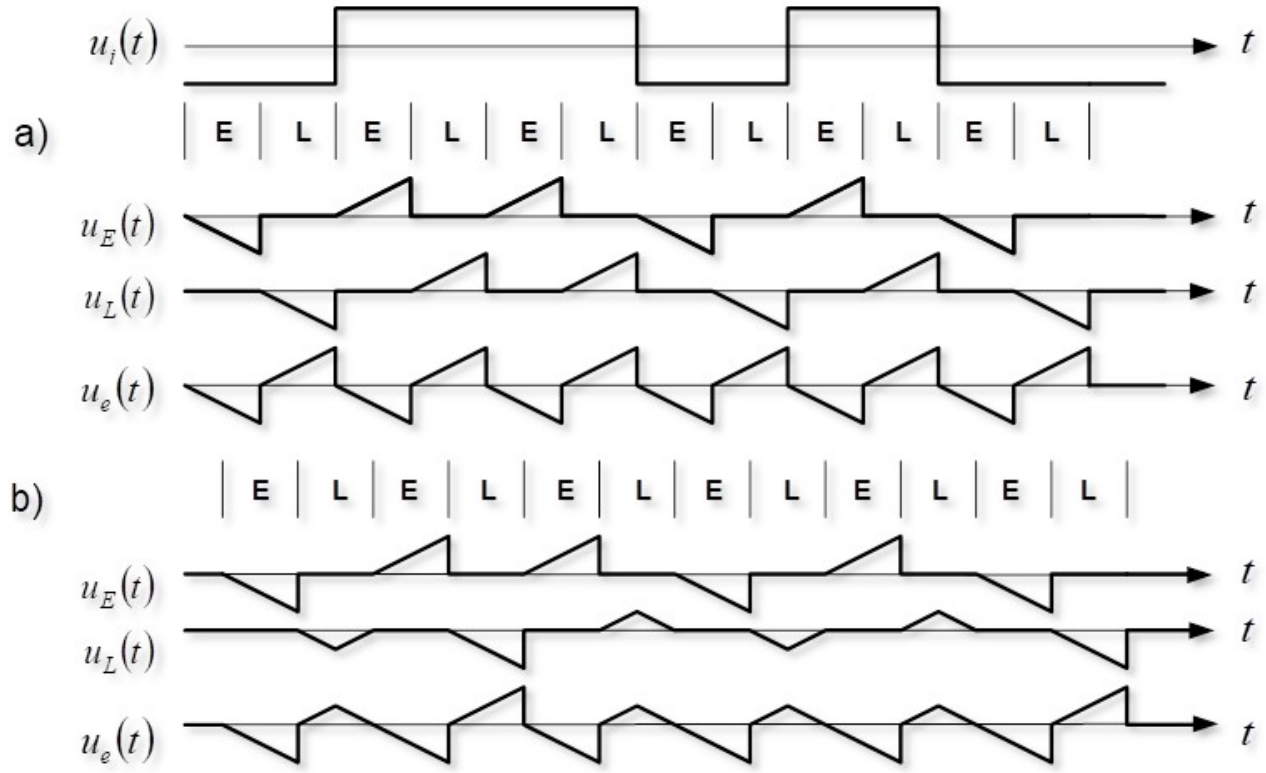




Difference between the *Early* and the *Late* integrators determines the VCO input (correction) voltage. When both integrator outputs are equal (integrating areas are the same, i.e. $u_E(\tau) = u_L(\tau)$, the correction voltage is zero.

10.3 Symbol Timing Recovery

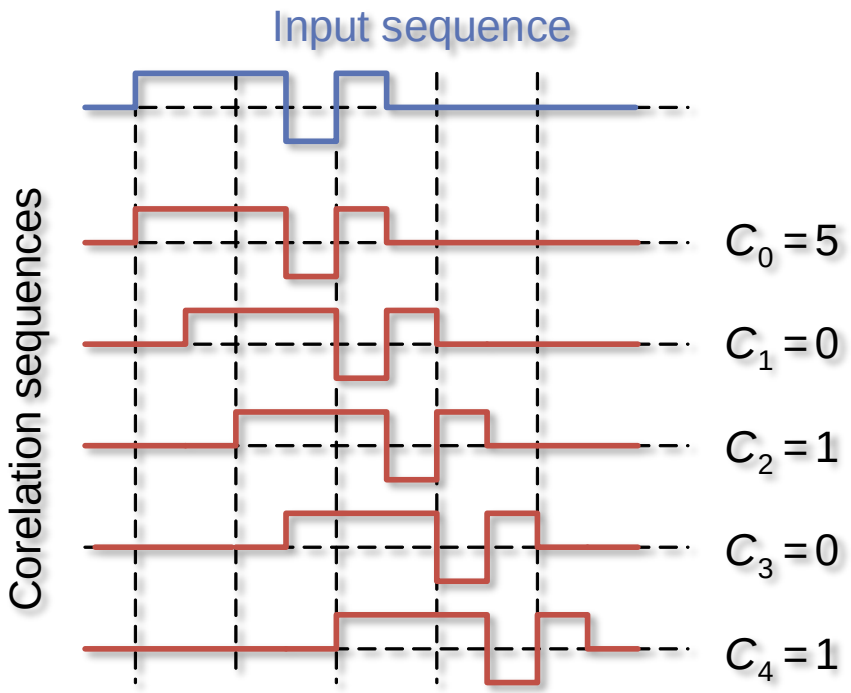
Early-Late STR signals



a) STR is in the locked state
b) STR is not locked

10.4 Frame synchronization

- It is based on frame alignment marker insertion into the frame header.
- Receiver knows the alignment marker (bit sequence).
- Marker is searched in the data stream using correlator (acquisition).
- Typical bit sequences Barker, Willard, Newman, Hoffman and Linder sequences (correlator output amplitude is ± 1 except correlation maximum)



10.5 Network synchronization

Synchronization is usually performed on the terminal side.

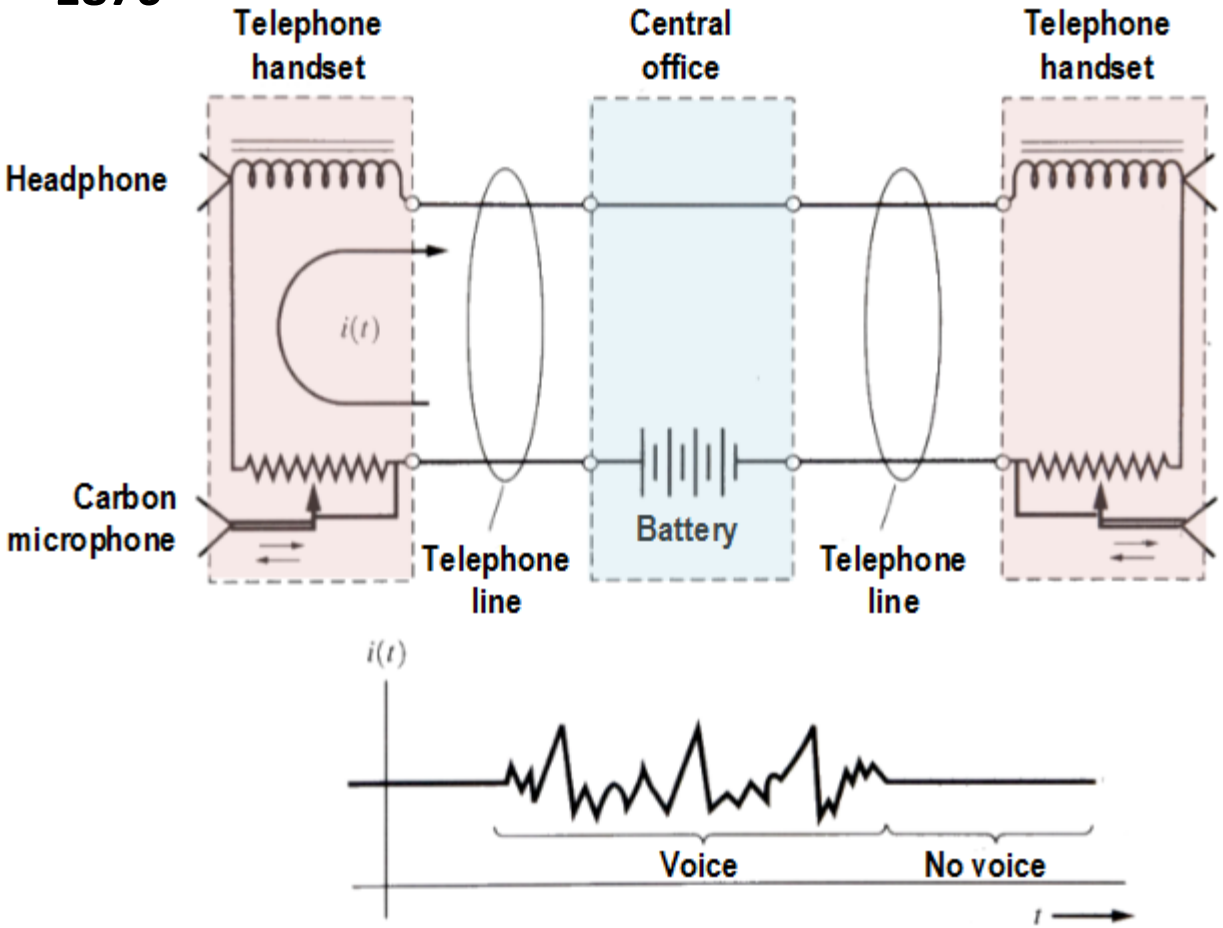
- **Open-loop system: do not use any return link for an error correction. Channel parameters have to be perfectly known (distance, speed,…), predictable, and link configuration has to be geometrically fixed. It uses pre-correction technique.**
- **Closed-loop system: there is special *return link* transferring information on synchronization (on carrier frequency/phase and STR error).**
- **Quasi-closed-loop system: correction parameters are obtained by monitoring of the return data link.**

11. WIRED COMMUNICATION SYSTEMS

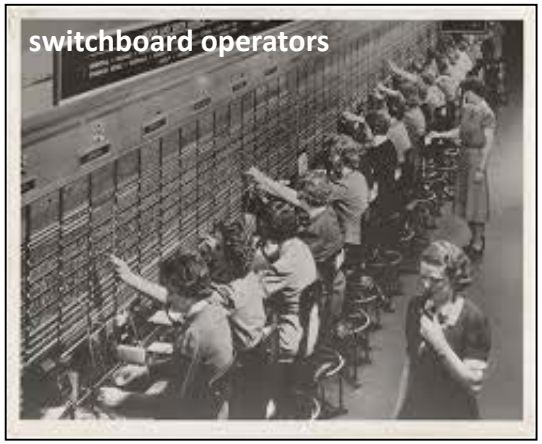
11.1 Telephone systems

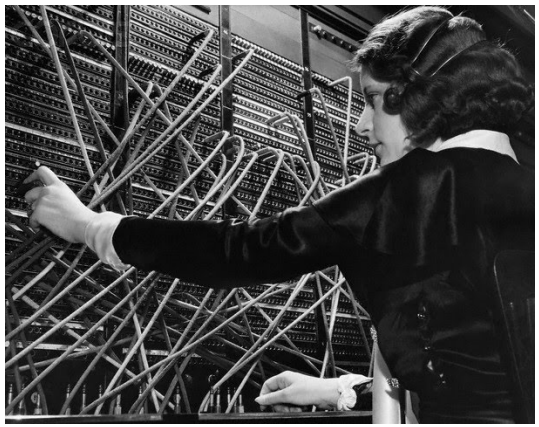
11.1.1 Voice transmission

- **First land-line telephone system was invented by Alexander Graham Bell in 1876**



Central office - history



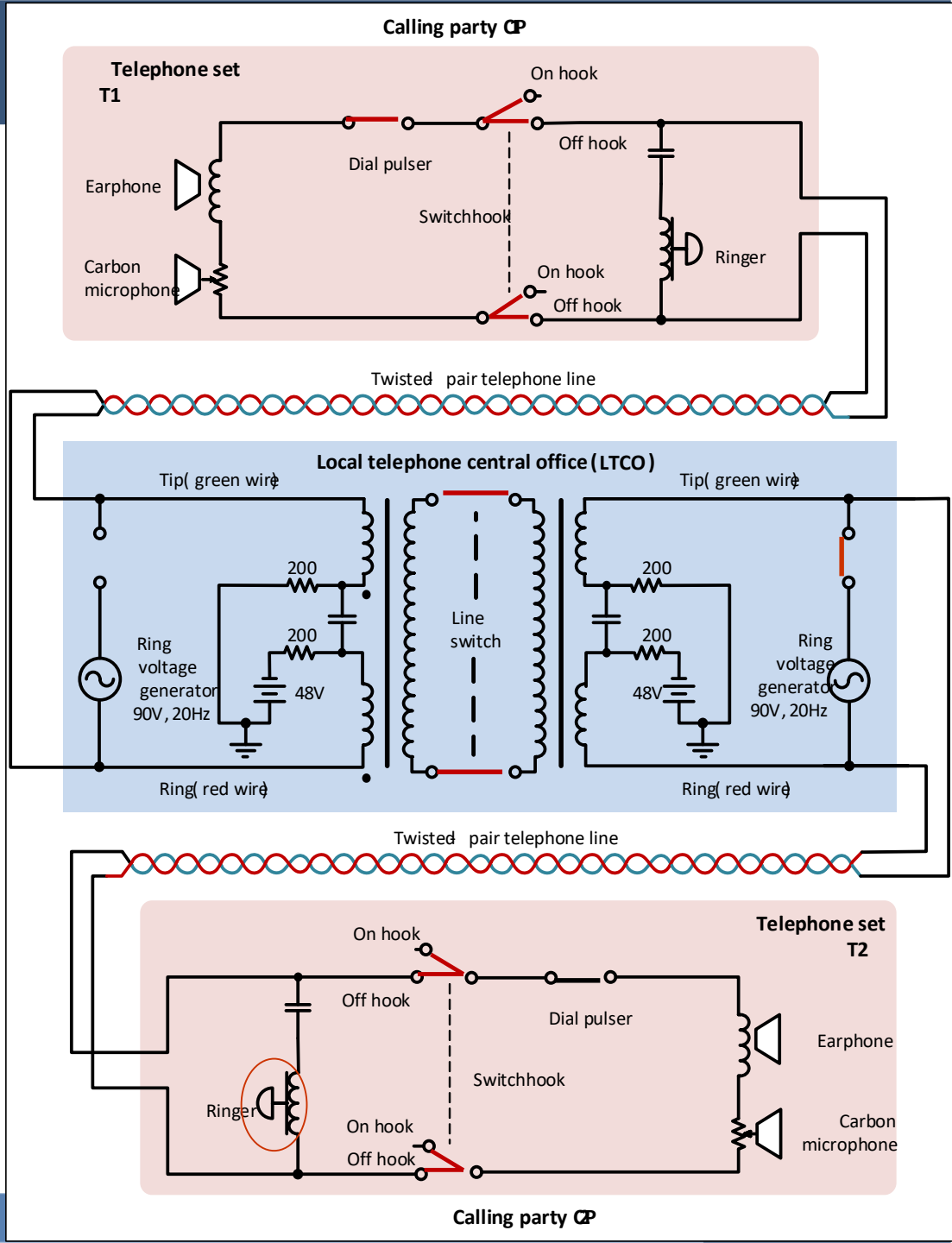


11.1.1 Voice transmission

Local loop system supplying PSTN (*Public switched telephone network*)

Operation:

1. **CP1 removes the telephone handset.**
2. **LTCO detects DC current and generates dial-tone on the T1 line.**
3. **CP1 dials the number using pulse or touchtone dialing.**
4. **After LTCO receives complete T2 number sequence, switches on the ring generator on T2 line.**
5. **If the CP2 removes the handset, LTCO detects DC current and establishes hardwire connection.**

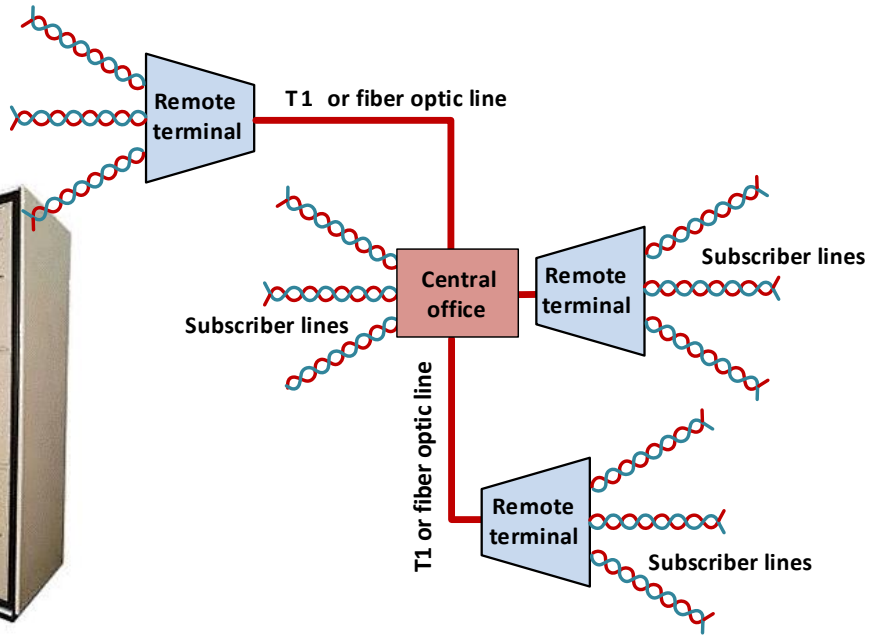


11.1.1 Voice transmission

Requirements made on telephone system:

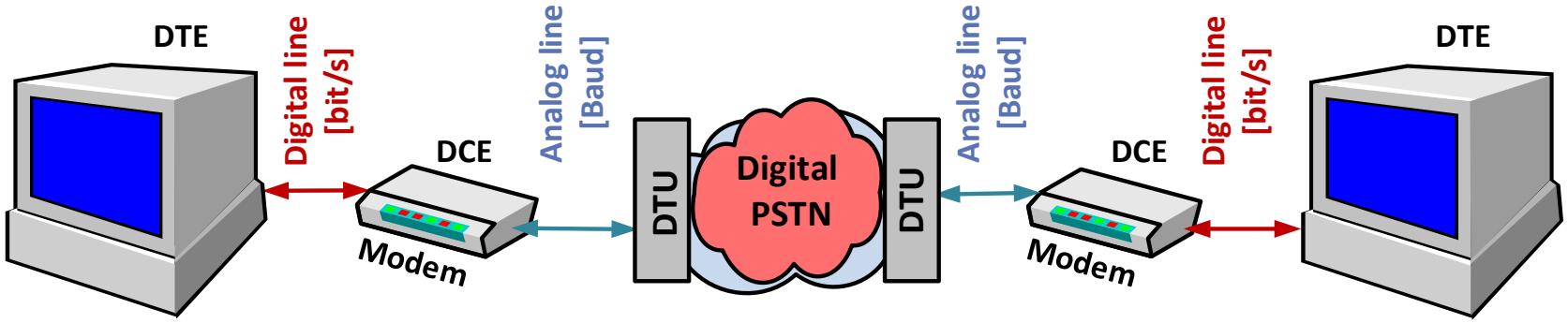
- **Interconnection of many subscribers:**
  - ✓ using telephone system with remote terminals, multiplexing of the subscriber calls (FDM – older, TDM – recent),
  - ✓ using digital central office and remote terminals (necessary for TDM) with A-law or μ-law ADCs.
- **Long distance connection:** using fiber optic lines with TDMA in „transport networks“, and four-wire circuit in the „last mile“ connection (allows using amplifiers in both directions).
- **Simple managing:** touch control using DTMF (*Dual Tone Multiple Frequency*).

Lower tone [Hz]	Higher tone [Hz]		
	1209	1336	1477
697	1	2	3
770	4	5	6
852	7	8	9
941	*	0	#



11.1.2 Data transmission – standard PSTN modems

- **Modem (*Modulator - Demodulator*) allows communication between remote computers using existing telephone copper wires. It is device of the *DCE (Data Communications Equipment)* type.**
- **Computer *DTE (Data Terminal Equipment)* is interconnect by the modem using serial RS 232 line or USB (*Universal Serial Bus*) line.**



Modem standards complying CCITT recommendation (duplex, asynchronous)

- **V.22, V22bis: data rate of 1200 b/s (2400b/s V22bis),**
- **V.32, V.32bis, V.34: 9600 b/s, V32bis: 14400 b/s - 1200 b/s, V34 28000b/s.**

11.1.2 Data transmission – standard PSTN modems

Standards complying BELL recommendation

- **Bell 212A, Bell103, VFC: 1200 b/s, 300, 28800 b/s.**

Standards complying ITU recommendation

- **V.90, V.90plus: 56/33 kb/s (downstream/upstream), 56/45 kb/s.**

Hardware implemented data compression and error correction protocols:

- **V.42/V.42bis: error correction and data compression to 4:1,**
- **V.44: optimized for the Internet browsing. Compression rate to 8:1,**
- **MNP-5: compression rate to 2:1.**

Communication protocols:

- **Earlier: Xmodem, Ymodem, Zmodem, Kermit.**
- **Later: TCP/IP.**

11.1.2 Data transmission – standard PSTN modems

Modem realizations

- Hardware modems (*Hayes compatible*): own microprocessor, multiplatform system (Windows, Linux, DOS, OS/2), AT commands configurable (Atention).
- Software modems: PC controlled using special SW, cheap.

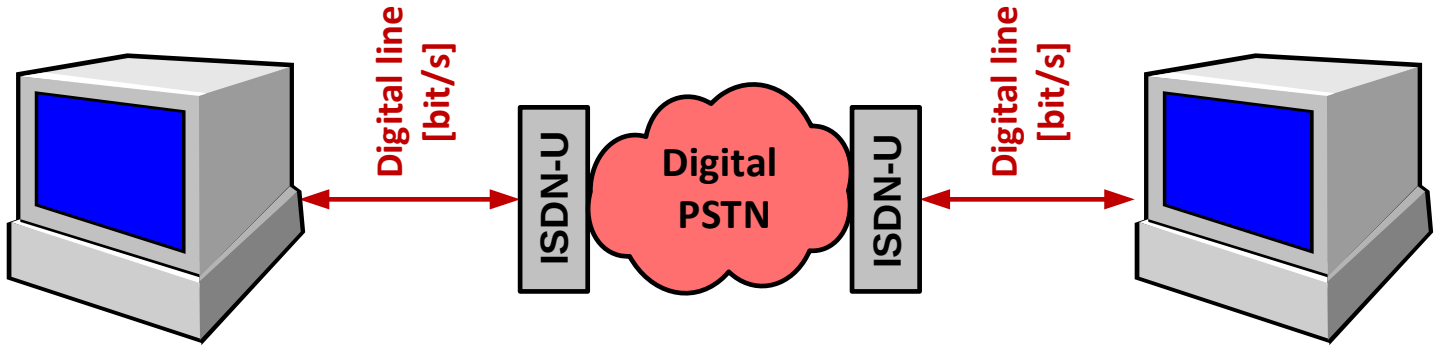
Transfer rates of PSTN modems

Bit rate [bps]	Baud rate [Bdps]	Number of modulation states	Bits per symbol	Standard
2400	600	16	4	V.22bis
9600	2400	16	4	V.32
14400	2400	124	6	V.32bis
28800	2400-3200	512	9	V.34
56000	8000	128	7	V.90, V.92

11.1.3 Data transmission – ISDN (*Integrated Service Digital Network*)

ISDN characteristics

- **Introduced in 1990. It includes set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the digital PSTN.**
- **It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data).**
- **It is dominantly focused on problems of the „last mile“ communication.**
- **Local loops and central ISDN office are digital.**



11.1.3 Data transmission – ISDN (*Integrated Service Digital Network*)

ISDN types:

- **Narrowband or Basic Rate Interface (BRI) ISDN: a two 64 kbit/s service data ('B' or bearer channels) are delivered over a pair of standard telephone copper wires together with 16 kbit/s signaling data ('D' channel or data channel). Total payload rate 2B+D = 144 kbit/s.**
- **Wideband or Primary Rate Interface (PRI) ISDN:**
  - **23 B channels per 64 kBit/s and single D channel 64 kbit/s, 23B + D = 1536 kbit/s delivered on one or more T1 carriers 1544 kbit/s (USA, Japan).**
  - **30 B channels per 64 kBit/s and single D channel 64 kbit/s, 30B + D = 1984 kbit/s delivered on one or more E1 carriers 2048 kbit/s (Europe).**

Telecommunication ISDN services: telephony (BW = 3.1 and 7 kHz), Fax, Videotelephony, data transmission, Internet services, other (SMS, e-mail, …).

11.1.3 Data transmission – ISDN (*Integrated Service Digital Network*)

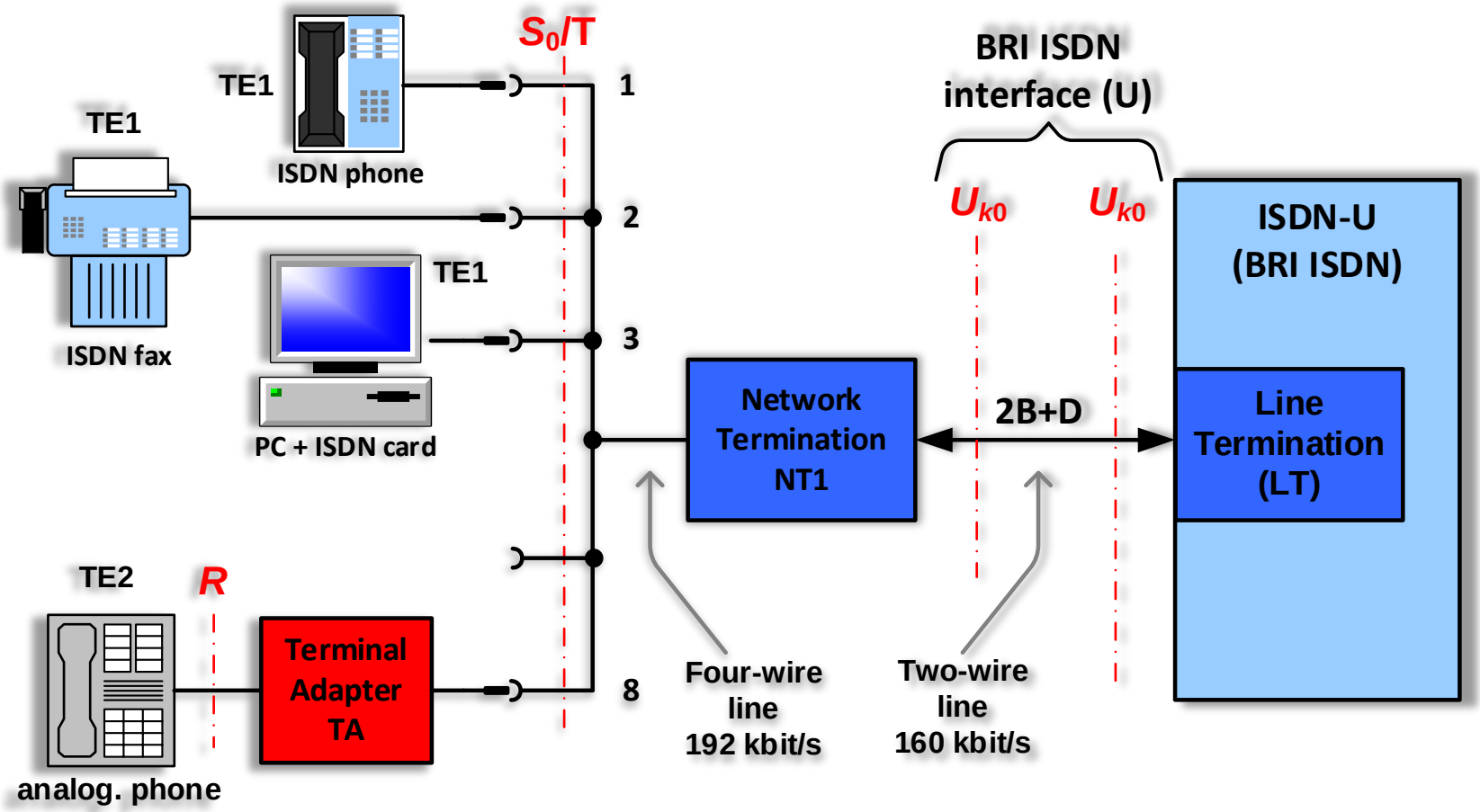
ISDN user terminals:

- **Terminal Equipment 1 (TE1): device with ISDN interface (phone, PC + card,…).**
- **Terminal Equipment 2 (TE2): device with analog interface (phone, FAX).**
- **Terminal Adapter (TA): allows connection of TE2 to ISDN network.**
- **Network Termination (NT1): connects terminal equipment to line termination (LT) equipment in the provider's telephone Exchange. Converts *U* interface to *S* bus, S_0 bus.**
- **Network Termination (NT2): private branch Exchange with to *S* bus, S_0 bus input interface.**

ISDN device connection (to NT1):

- **Typical for home applications.**
- **Subscriber has MSN (*Multiple Subscriber Numbering*) numbers, that may be assigned to TEs.**
- **Maximum two devices can work at the same time.**

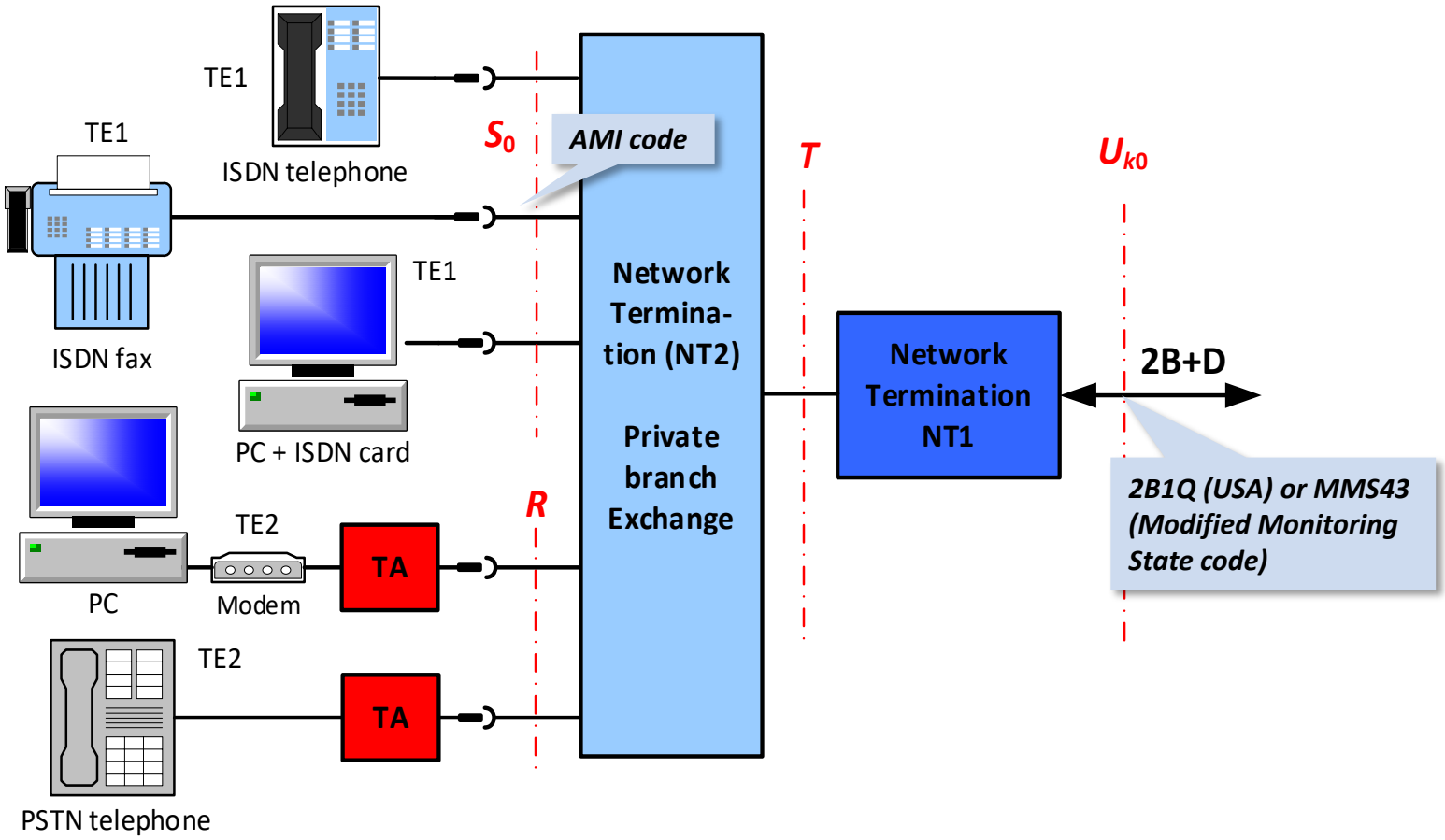
ISDN device connection (to NT1) cont.



11.1.3 Data transmission – ISDN (*Integrated Service Digital Network*)

ISDN device connection (to NT2):

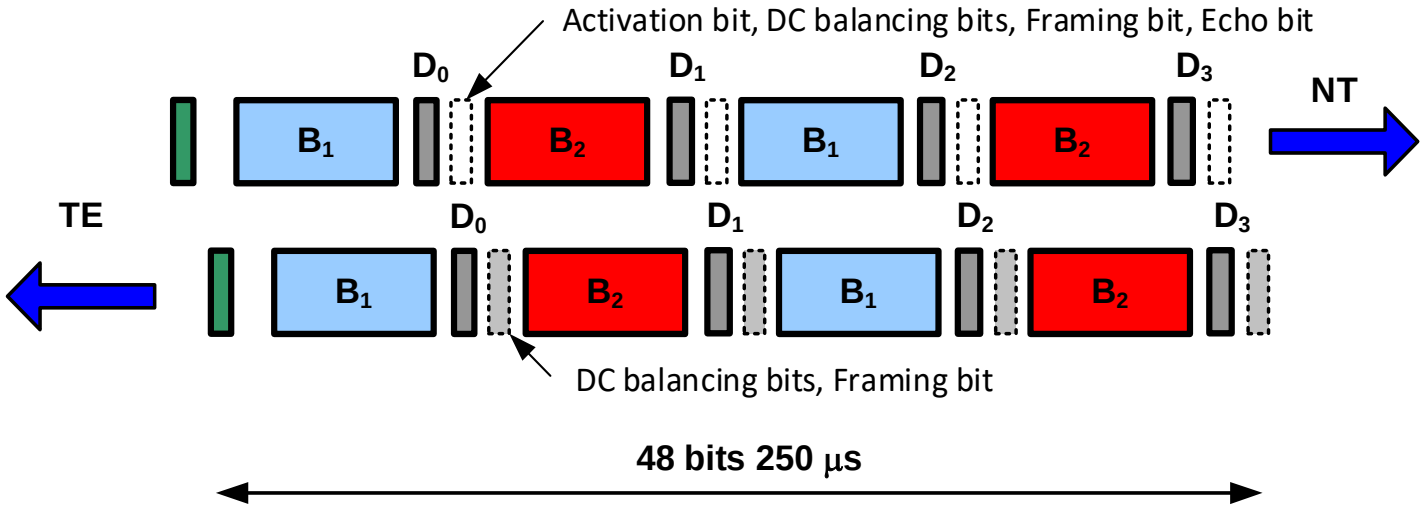
- **Suitable for small companies. NT2 works as a private automatic branch exchange. Some TE2 equipment can be connected to the NT2 without TA.**



11.1.3 Data transmission – ISDN (*Integrated Service Digital Network*)

Bit rates at S_0:

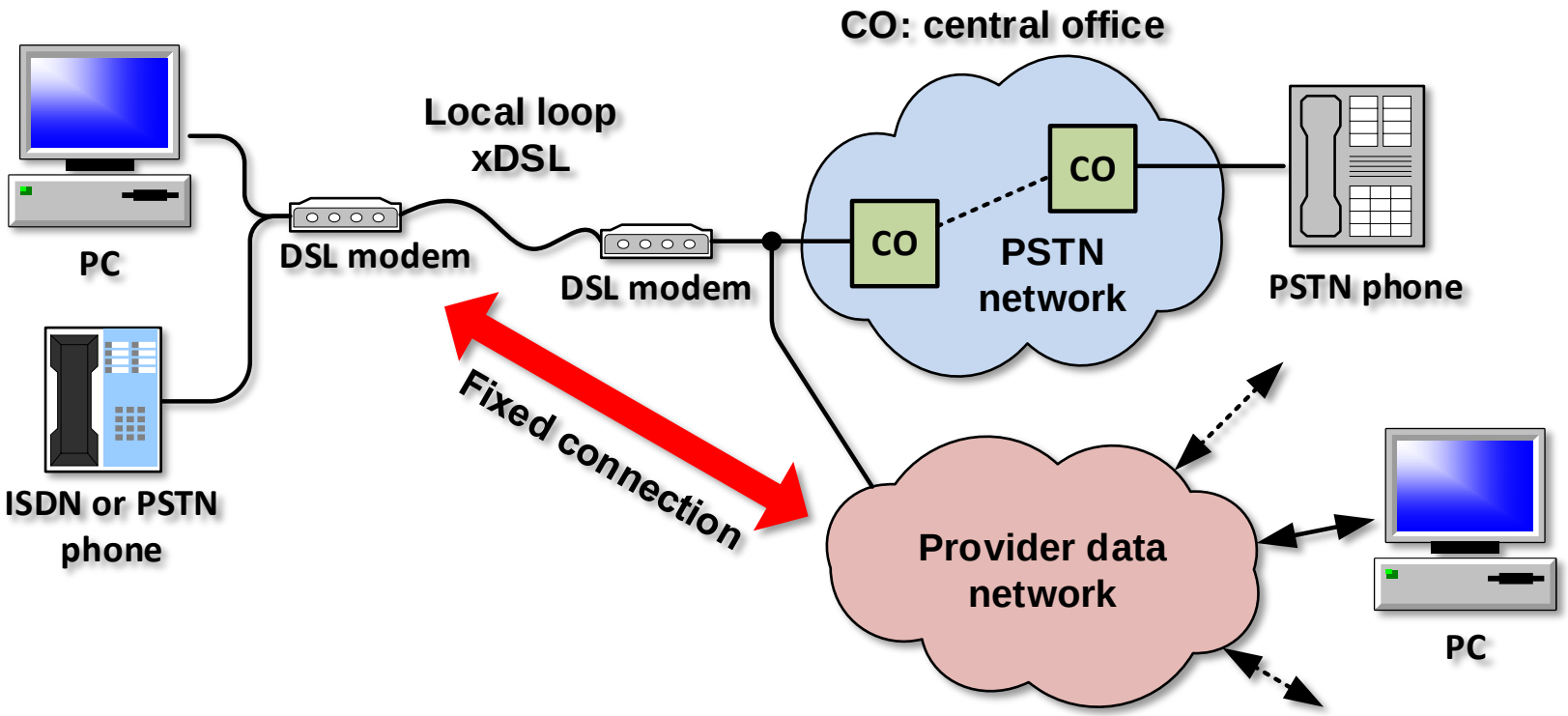
B_1+ B_2 bearer channels:	128 kbit/s
Signaling data channel:	16 kbit/s
Framing and maintennace channel:	48 kbit/s
Total	192 kbit/s



Framing bit provides synchronization.
Load balancing bit adjusts the average bit value.
Echo bit is used for contention resolution when several terminals on a passive bus contend for a channel.
Activation bit activates devices.

11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

Technology that provide Internet access by transmitting digital data over the wires of a local telephone network (physical pair of wires). High data rate transmission is achieved because local lines operate usually up to few tens of MHz ($f_{max} \approx 30$ MHz). To utilize such frequency band, special DSL modems and special provider network are required.



11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

Why PSTN is problematic to use?

Coupling transformers and hybrid devices (used in digital central officess) in a telephone central offices have cut-off frequency of $f_{max} = 3.4$ kHz $\Rightarrow$ data rate max. 56 kbit/s for 50 dB SNR (V.90 modem).

DSL variations:

- **ISDN DSL: one bidirectional twisted pair 144 kb/s, uses 2B1Q line code.**
- **HDSL (*High bit rate DSL*): two twisted pairs 1.544 Mbit/s (up to 4 km), uses 2B1Q line code or QAM_{SC}. Full duplex.**
- **SDSL (*Symmetrical DSL*): HDSL modification, one twisted pair 2×0.768 Mbit/s.**
- **ADSL (*Asymmetrical DSL*): two twisted pairs 6 Mbit/s downstream and 640 kbit/s upstream (up to 4 km), ADSL BW 25/138 kHz ÷ 1100 kHz. Variants: G.DMT, G.Lite.**
- **ADSL 2 *Asymmetrical DSL 2(+)*: two twisted pairs 12(24) Mbit/s downstream and 640 kbit/s upstream (up to 4 km),**
- **VDSL (*Very high bit rate DSL*): two twisted pairs 25 Mbit/s (up to 1 km) or 51 Mbit/s (up to 0.3 km), downstream and 3.2 Mb/s upstream, double bandwidth.**

11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

Characteristics of the G.DMT DSL technology

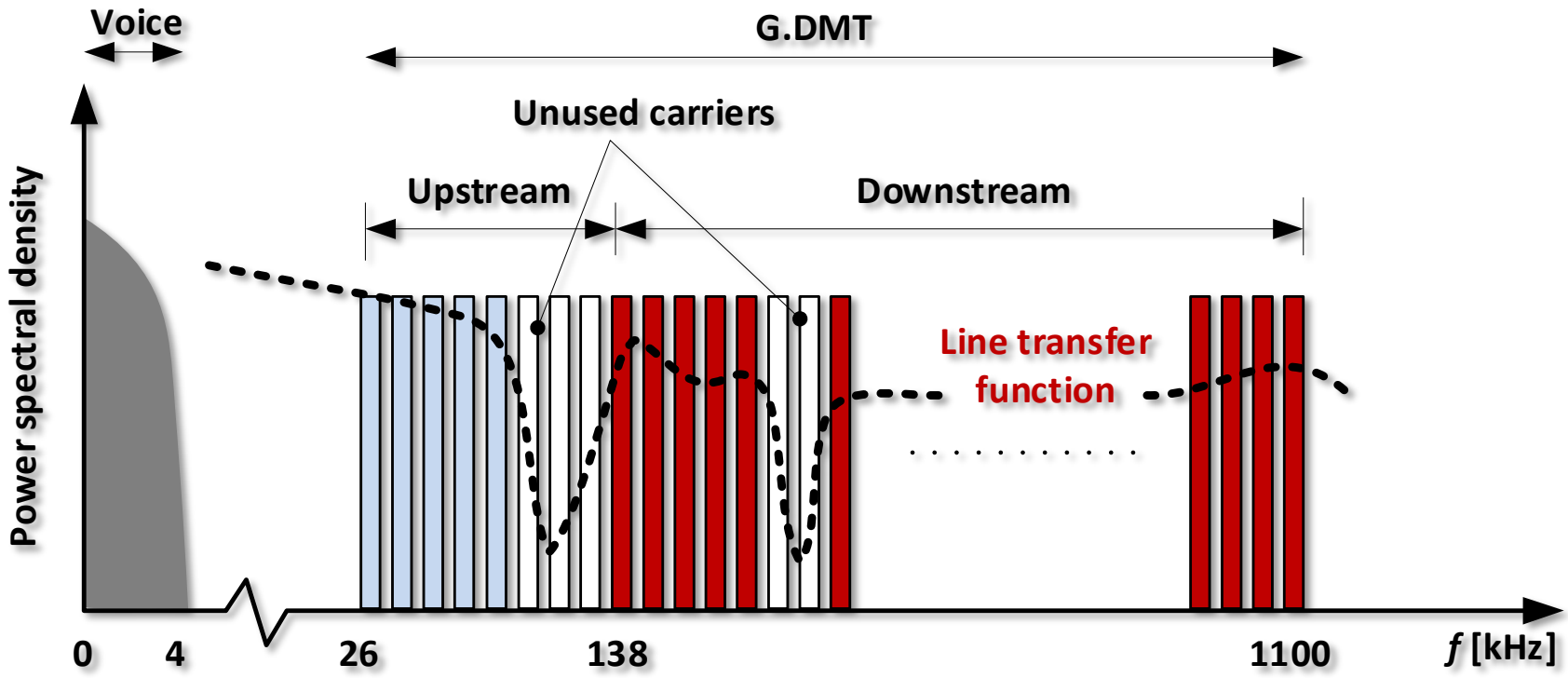
- It is based on the DMT (*Discrete MultiTone*) modulation with 256 carriers distant by 4.3125 kHz.
- The carriers are modulated by 32768 QAM (15 bits per carrier) ⇒ 6.1 Mbit/s downstream (138 - 1100 kHz) a 640 kBit/s upstream (26 - 138 kHz).

Spectrum of ADSL is given by standard:

- Annex A: is designed for the PSTN analog network (see above).
- Annex B: is designed for simultaneous DSL and ISDN communication. Due to broader bandwidth of ISDN the ADSL downstream starts at 138 kHz and upstream at 276 kHz.

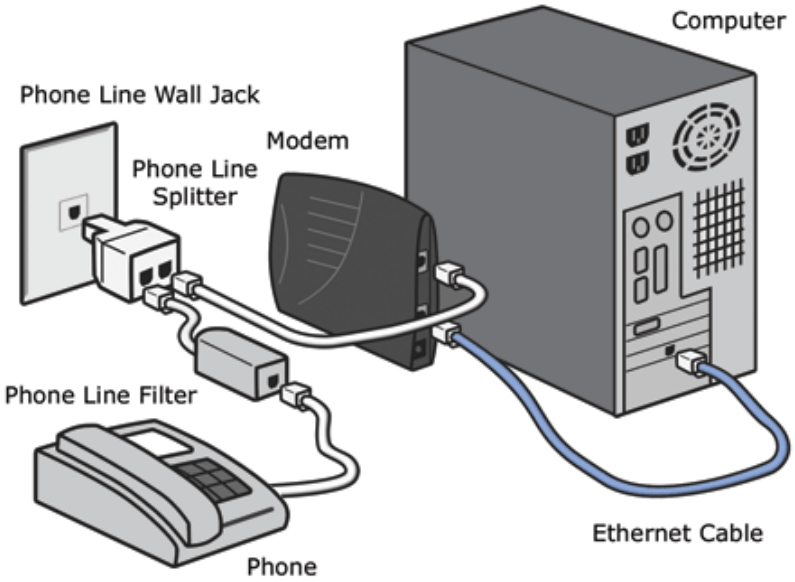
11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

Preparation of transmission: the line transfer function is measured and the carriers lying at the frequencies where the line has a high attenuation are excluded. Number of the QAM levels depends on the SNR at given frequency.

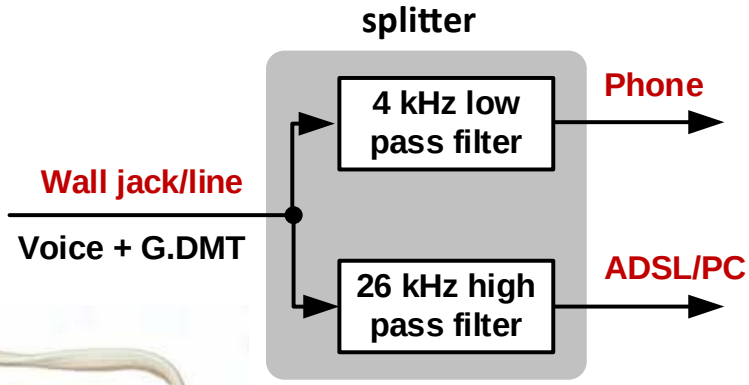


11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

Connection PC to ADSL (VDSL)



Wideband phone line splitter with phone line filter (cutting off the DSL signal) can be replaced by frequency dependent splitter.

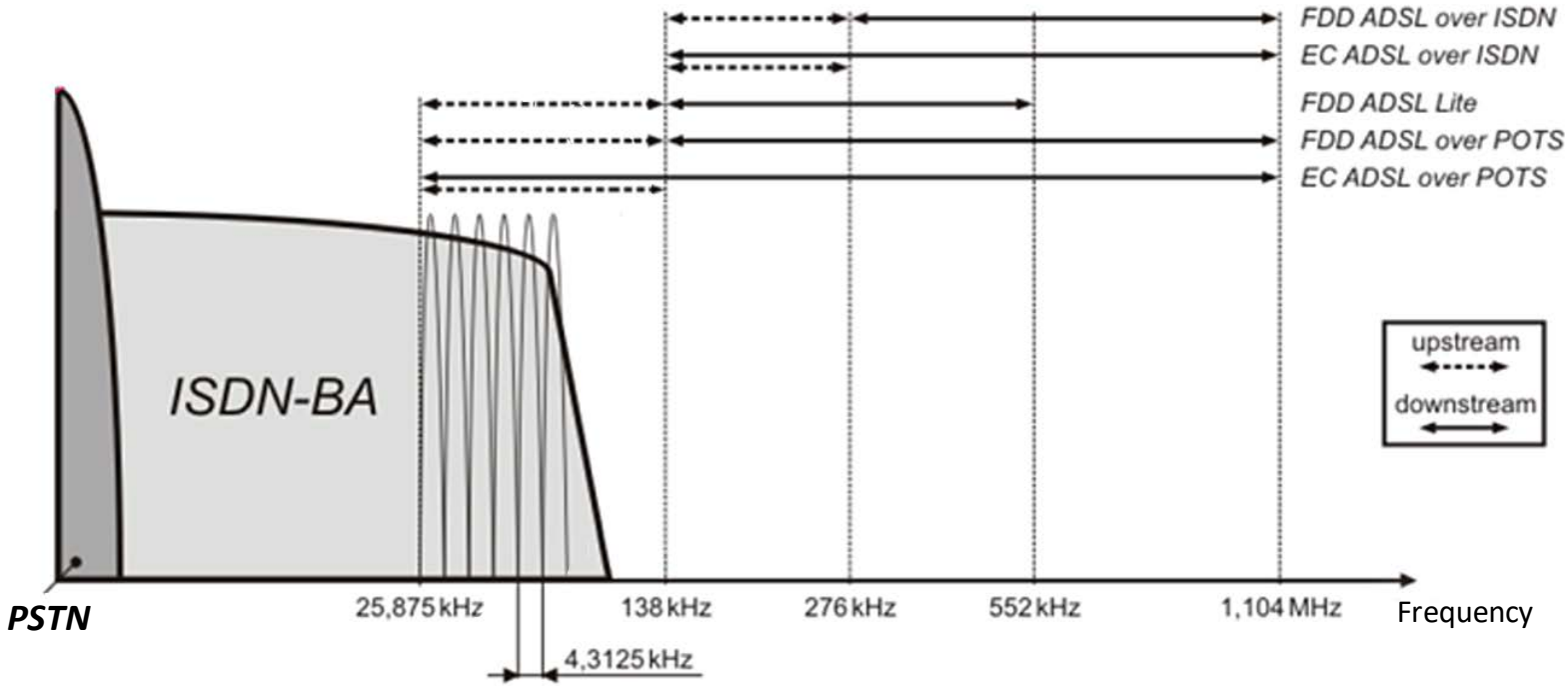


Characteristics of the G.Lite DSL:

It works without the line filter (phone and DSL share the same band). G.Lite DSL uses DMT with 128 carriers each modulated by 512 QAM (8 bits per carrier). It offers 1.5 Mbit/s downstream and 512 kbit/s upstream and distance up to 6 km.

11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

ADSL standards



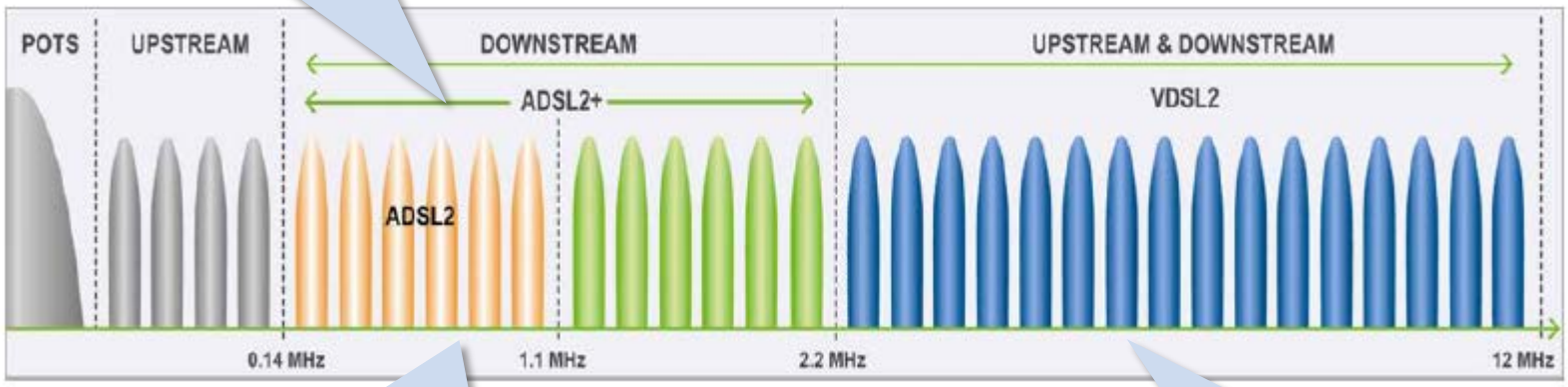
ADSL frequency spectrum depends on the standard:

- **Annex A: ADSL over POTS (see page 173).**
- **Annex B: ADSL over ISDN. Due to higher ISDN bandwidth, the ADSL frequency spectrum is moved to 138 kHz (upstream) and to 276 kHz (downstream). The upper frequency is equal to the one in the Annex A.**

11.1.4 Data transmission – DSL (*Digital Subscriber lines*)

ADSL, ADSL2 and VDSL spectrum

ITU G.992.5 (also referred to as ADSL2+, G.dmt.bis+, and G.adslplus)



ITU G.992.3 is an ITU (International Telecommunication Union) standard, also referred to as ADSL2 or G.dmt.bis

ITU G.993.2 (also referred to as very high-speed digital subscriber line VDSL2)

12. WIRELESS COMMUNICATION SYSTEMS

12.1 Satellite communications

12.1.1 C band communications

Why C band?

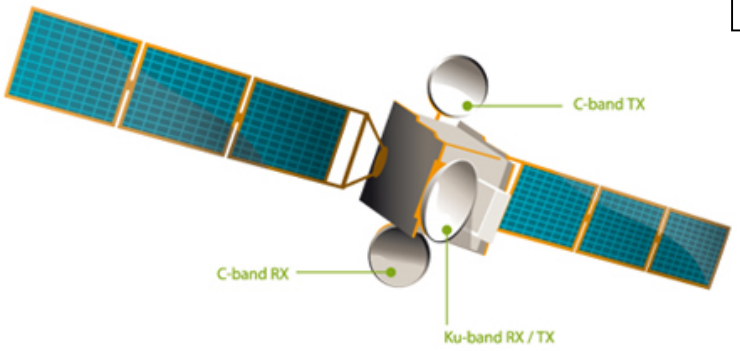
- **low cosmic noise,**
- **relatively cheap TX and RX,**
- **low atmospheric attenuation.**

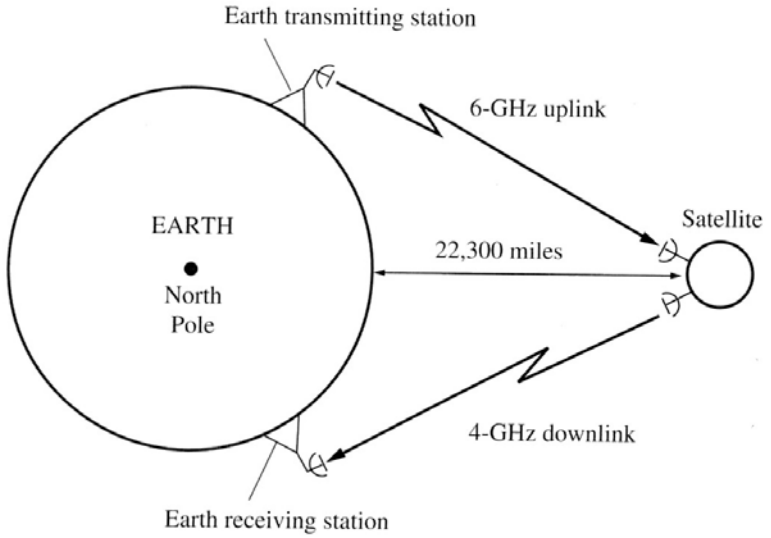
Utilization:

- **TV broadcasting and data service.**

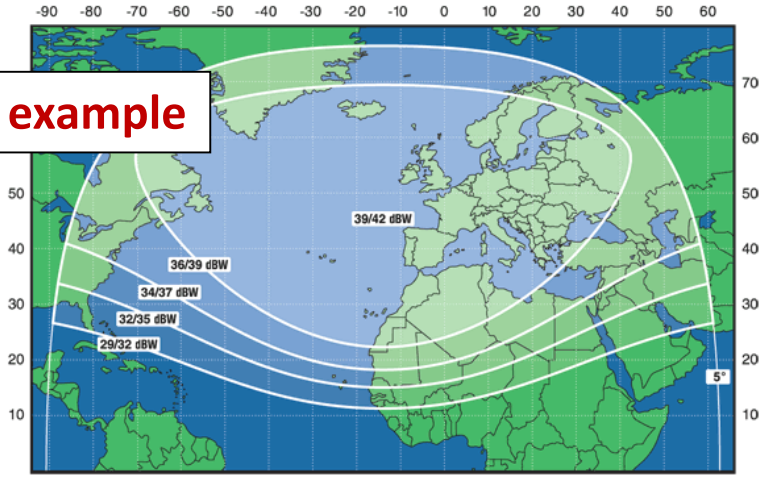
Properties:

- f_{cd} = 3.7 - 4.2 GHz **(downlink),**
- f_{cu} = 5.925 – 6.425 GHz **(uplink),**
- **channel bandwidth = 36 MHz,**
- **channel spacing: 40 MHz.**



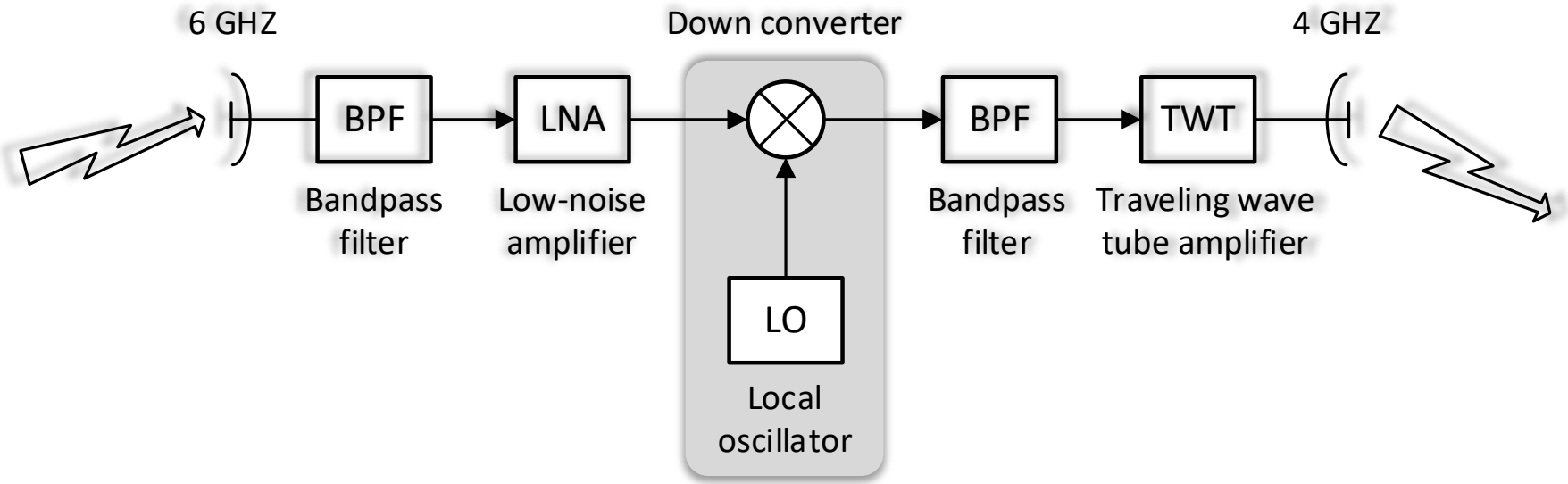


Coverage example



12.1.1 C band communications

Block diagram of satellite transponder (without demodulation)



Communication parameters (Standard C - band)

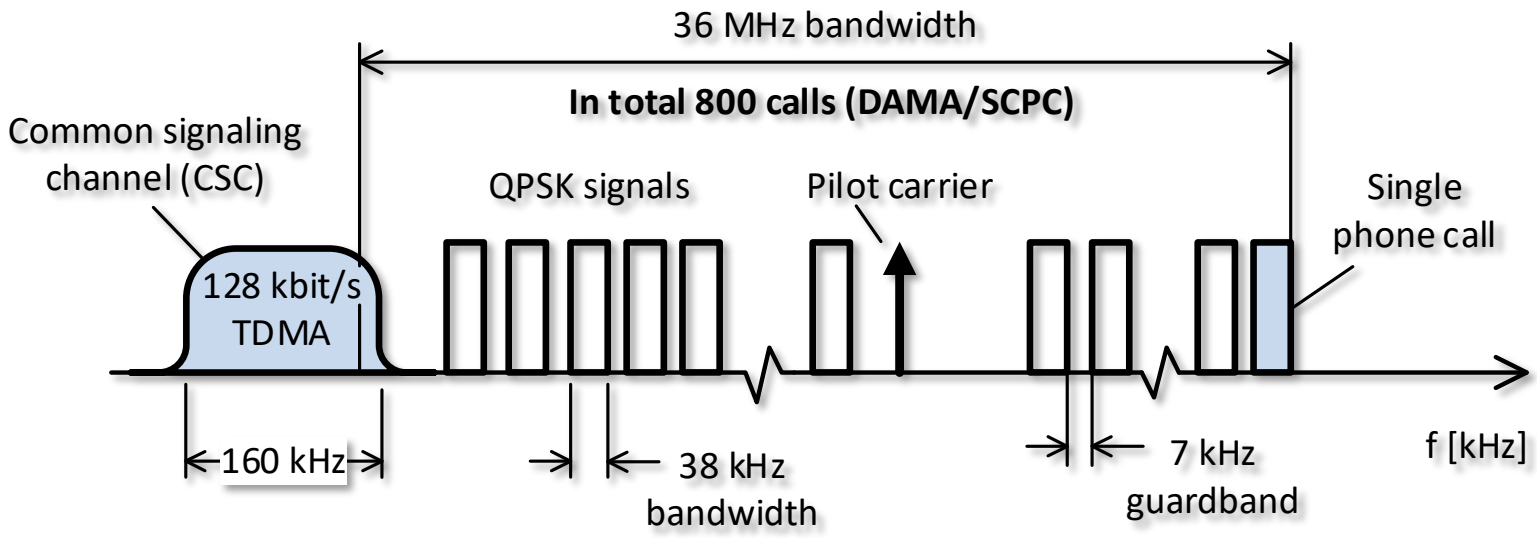
- **Channel number:** **24 (12 vertical polarization, 12 horizontal polarization – mutually shifted by 20 MHz).**
- **Labelling:** **C1, C2, …**
- **Uplink and downlink bandwidth:** **12 × 36 MHz + 12 × 4 MHz + 20 MHz = 500 MHz.**
- **Frequency distance between uplink and downlink:** **2225 MHz.**
- **Typical antenna diameter:** **2,5 - 3,5 meter.**

12.1.1 C band communications

C-band modifications with extended spectrum: Extended C-Band, INSAT / Super-Extended C-Band, Russian C-Band, LMI C-Band.

Satellite system for data and telephone signals retransmission

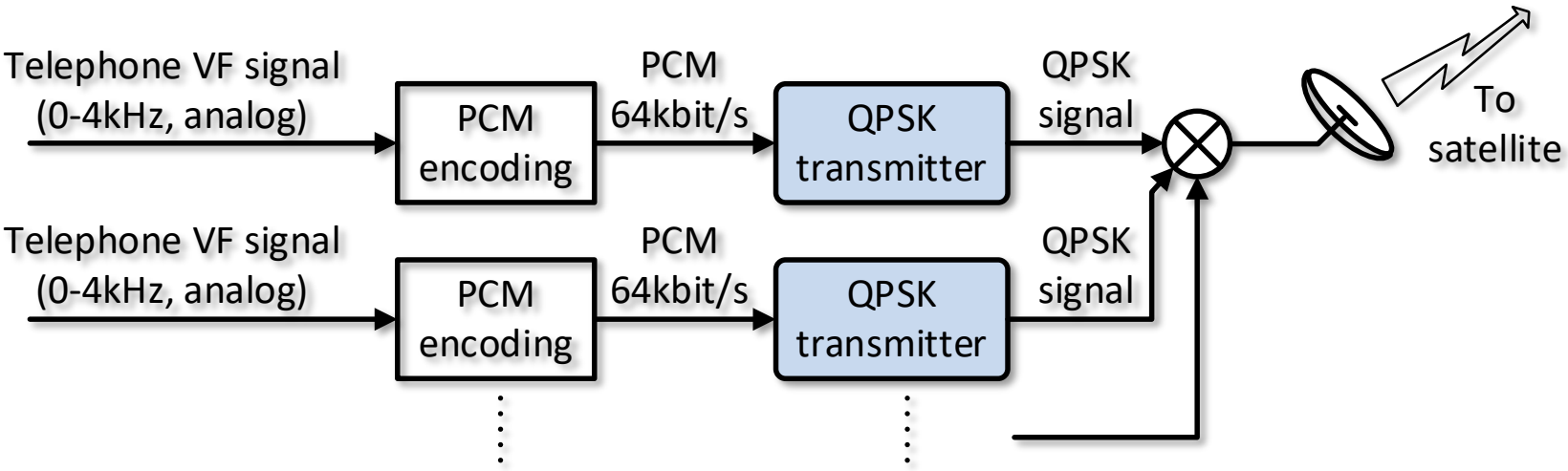
Access type: DAMA (*Demand Assigned MA*) = combination of SCPC (*Single Channel per Carrier* - similar to FDMA)/TDMA.



Structure of CSC TDMA signal

CSC consists of 128kbps PSK signal shared among the Earth terminals using TDMA format. 49 different Earth terminals may be accommodated in the frame (time slots A, B, C,...)

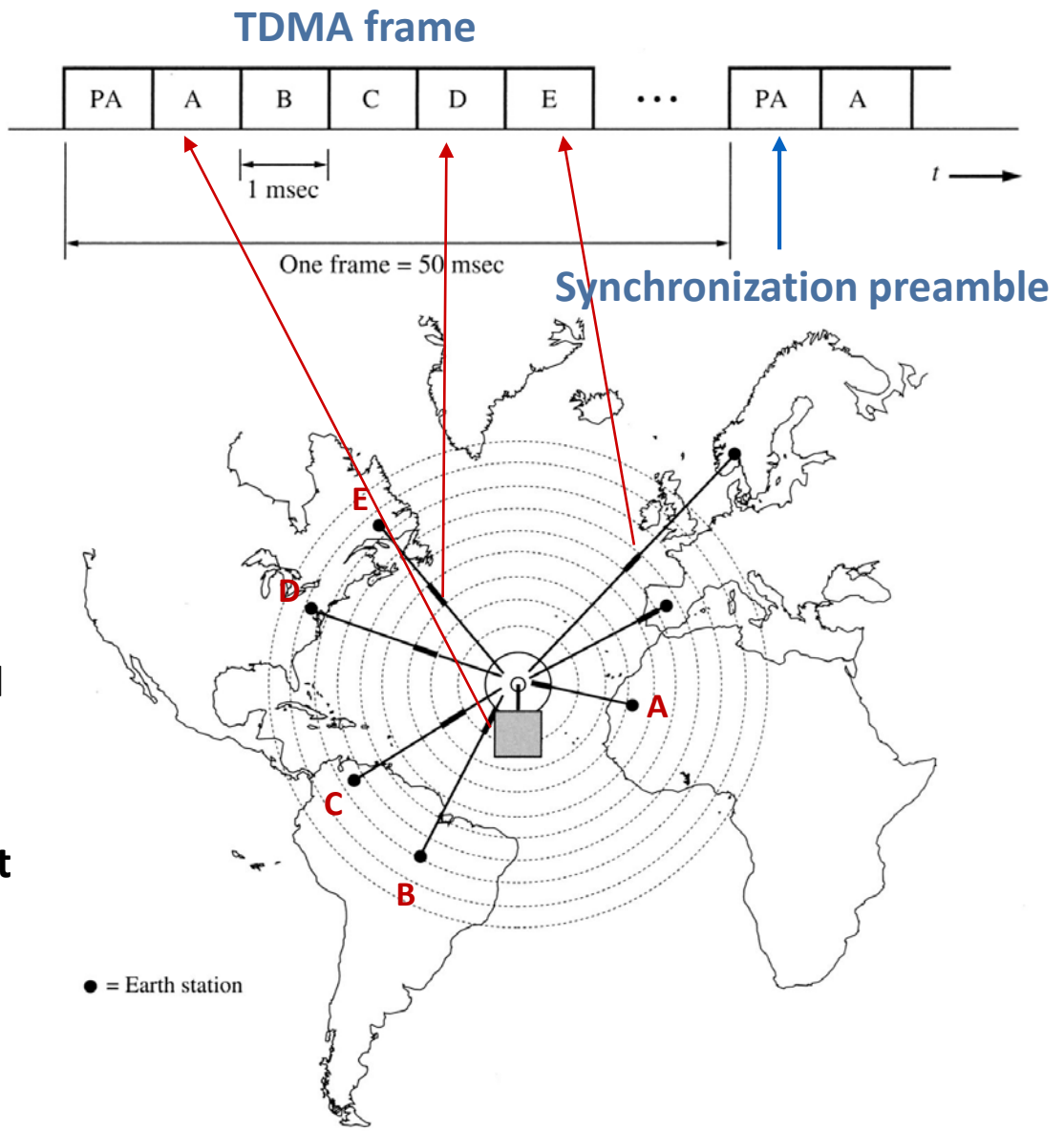
Intelsat / DAMA (SPADE system)



12.1.1 C band communications

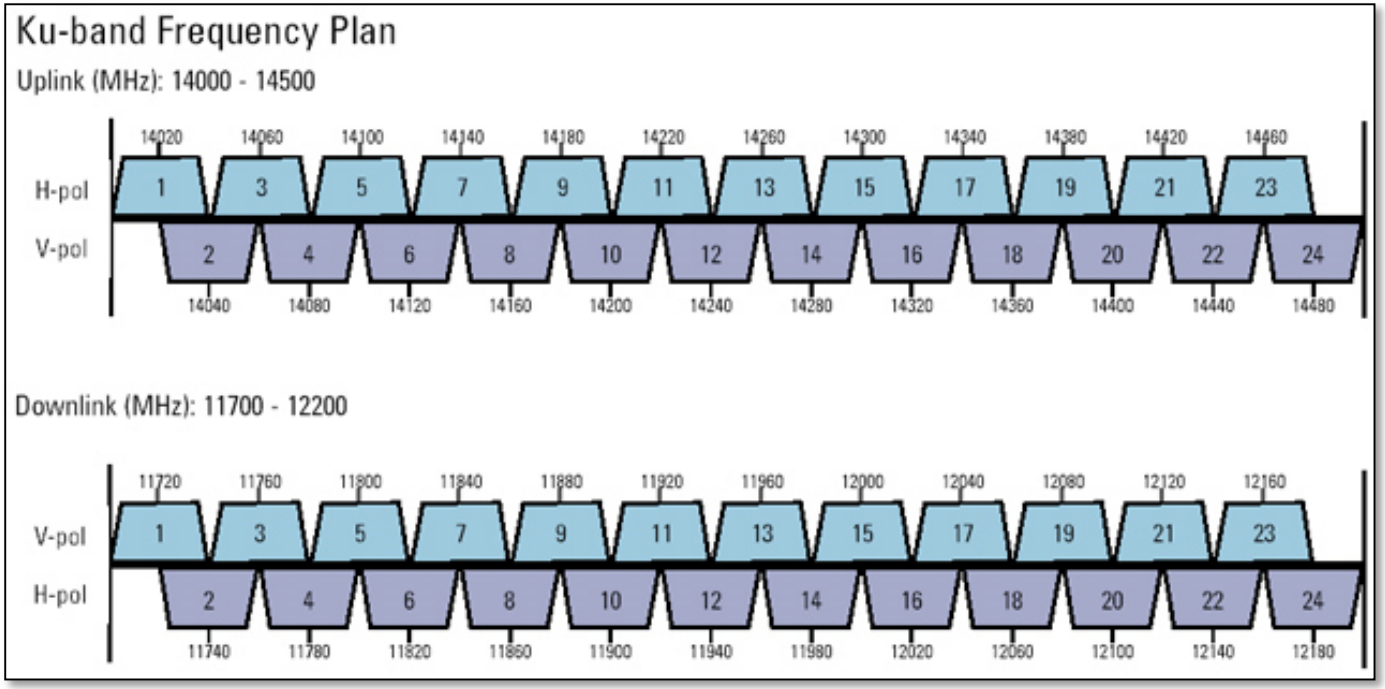
Let terminal B wishes to call D:

1. **B selects randomly any free QPSK frequency and transmits this frequency info along the address of call destination D in B-TDMA slot.**
2. **If assumed that the frequency has not been selected by another station, D will acknowledge the request in its D-TDMA slot.**
3. **When the same freq. is required by another terminal, the busy signal is received at station B.**
4. **When the call is over, disconnect signal is transmitted in the TDMA slot and carrier is returned for reuse.**



12.1.1 C band communications

C band shares frequencies used also by another satellite systems, WLANs (WiFi), cordless phones and radar systems for the weather monitoring ⇒ possible interferences ⇒ searching for the other bands ⇒ K_u.

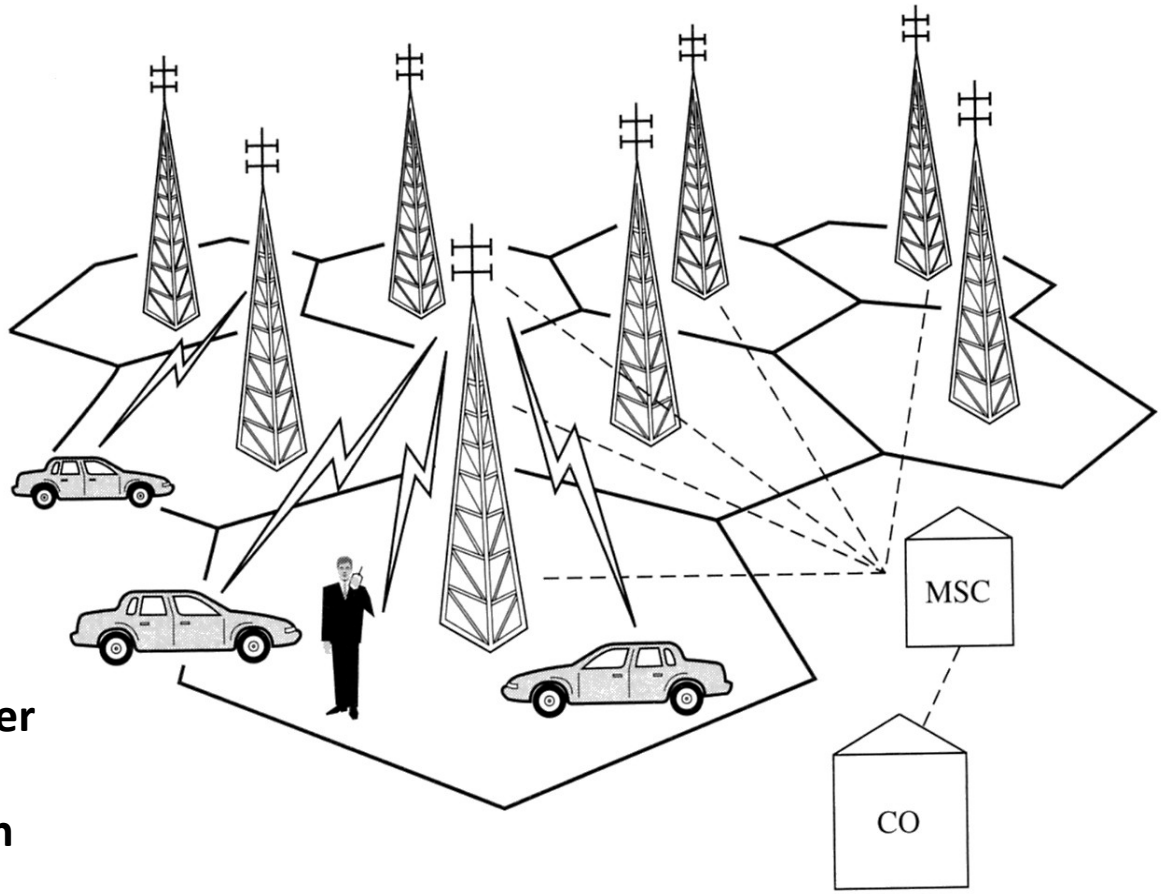


Ku band is primarily used for satellite communications, most notably for fixed and broadcast services, and for specific applications such as *NASA*'s Tracking Data Relay Satellite used for both space shuttle and *International Space Station (ISS)* communications.

12.2 Radiotelephone systems
12.2.1 Mobile cellular systemsc

Advantages of cellular systems

- Large number of users
- High spectrum efficiency (reuse the same frequency used by distant BTS)
- Superior sound quality
- Use of mobile stations



MSC: Mobile Switching Center
CO: Central Office
BTS: Base Transceiver Station

12.2.1 Mobile cellular systems

Mobile cellular technology overview

- **1. generation (1G): analog phones with FM modulation,**
- **2. generation (2G): fully digital utilizes various digital access protocols, including CDMA, TDMA,**
- **3. generation (3G): UMTS/IMT-2000 (*International Mobile telecommunication in the year 2000*),**
- **4. generation (4G) accepted definition in IMT-Advanced, offers data rates of up to approximately 150 Mbit/s.**

Generation	Technology	Bitrate	Real bitrate
2G	**HSCSD (*High Speed Circuit Switched Data*)**	**115 kb/s**	**30 kb/s**
2.5G	**GPRS (*General Packet Radio Service*)**	**171 kb/s**	**60 kb/s**
2.75G	**EDGE (*Enhanced Data rates for Global Evolution*)**	**384 kb/s**	**80 kb/s**
3G	**UMTS (*Universal Mobile communication Service*)**	**42 Mb/s**	**200 kb/s**
4G	**LTE (*Long Term Evolution*)**	**150Mb/s**	**10 Mb/s**

12.2.1 Mobile cellular systems

1G Cellular systems “brick phones” and “bag phones”

- Standard: NMT (*Nordic Mobile Telephone*)
- Modulation: FM/FSK (for signalization)
- Multiple access: FDMA, (*Frequency Division MA*)
- Number of channels: 832 (AMPS), 200 (NMT-450)
- Channel spacing: 30 kHz (AMPS), 25 kHz (NMT-450)
- Frequency: 824-894 MHz (AMPS), 453-468 MHz (NMT-450)

Signalization: phone number, channel number, phone identification,…

Establishment of connection:

1. Dialing the number and its transmission to the BTS.
2. Verification of the calling and called party numbers in MTS (authorization).
3. Channel allocation for the call.
4. Called party ringer activation.
5. Calling parties interconnection and start the call tariffication.
6. Release the channel after call termination.

12.2.1 Mobile cellular systems

2G Cellular system GSM

Primary GSM-900 Band (Phase 1):

- **Uplink frequency: 890 MHz to 915 MHz.**
- **Downlink frequency: 935 MHz to 960 MHz**
- **Multiple access: FDMA, FDD, TDMA.**
- **Frequency Division Duplex frequency: 45 MHz**
- **Number of channels: 124 with bandwidth 200 kHz. 124 FDMA channels × 8 TDMA (timeslot) = 992 access channels.**

GSM 1800:

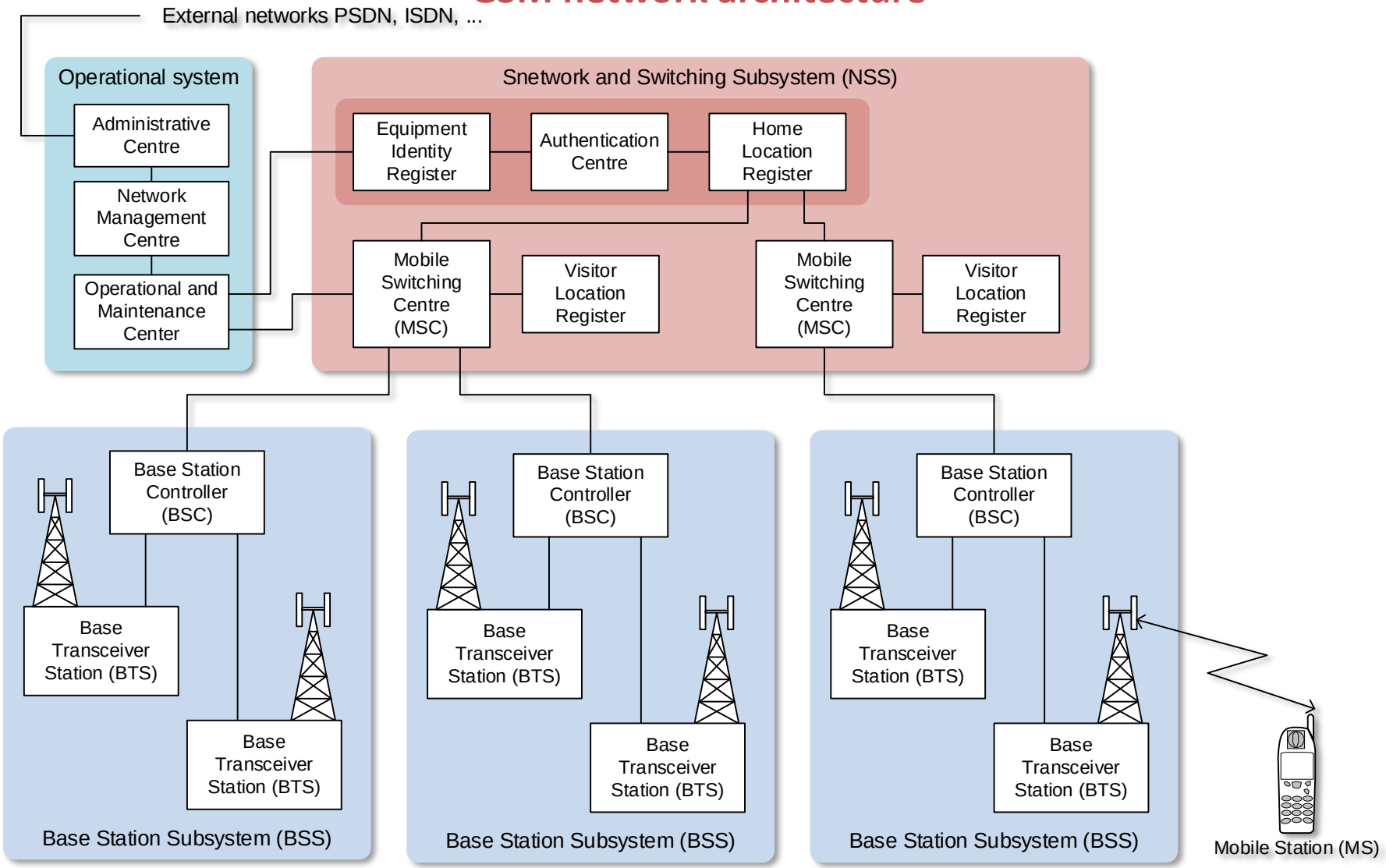
- **Uplink frequency : 1710 MHz to 1785 MHz**
- **Downlink frequency : 1805 MHz to 1880 MHz**
- **Frequency Division Duplex frequency : 95 MHz**
- **Number of channels: 374 with bandwidth 200 kHz.**
- **Number of channels : 374 × 8 = 2992.**

Signal processing in GSM Cellular system

- **Source coding:** 20 ms segmentation, RPE – LTP (*regular pulse excitation – long-term prediction*) coding, 13 kbit/s.
- **Encryption:** using special key and algorithm (Kc and A5) the two encryption words are formed - Su (for uplink) a Sd (for downlink). They then are added to the data stream (using XOR) – stream ciphering.
- **Channel coding:** time interleaving, parity and convolutional coding, 22.8 kbit/s.
- **Equalization:** training sequence and control bits insertion, 33.854 kbit/s $\Rightarrow$ 270.833 kbit/s in 8 time slots.
- **Modulation:** GMSK ($BT_b = 0.3$)

12.2.1 Mobile cellular systems

GSM network architecture



12.2.1 Mobile cellular systems

Network and Switching Subsystem:

- **Mobile Switching Centre: performs the switching of calls between the mobile and other fixed or mobile network users.**
- **Home Location Register: database used for storage and management of subscription (service profile, location information, and activity status).**
- **Authentication Centre: database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering.**
- **Visitor Location Register: temporary information about subscribers who have just moved in the area of the particular MSC.**
- **Equipment Identity Register: database that contains a list of all valid mobile equipment on the network.**

Operational system:

- **Authentication Centre: authenticate each SIM card that attempts to connect to the GSM core network (typically when the phone is powered on).**
- **Operational and Maintenance Centre & Network Management Centre: manage the operation and maintenance of the BSS and NSS hardware, monitor mobile stations and perform tariffing.**

12.2.1 Mobile cellular systems

Base Station Sub-System:

- **Base Transceiver Station:** radio transceivers that define a cell and handles the radio link protocols with the MS.
- **Base Station Controller:** manages the radio resources for BTSs. It handles radio channel setup, frequency hopping, and handover.

3G Cellular system UMTS

- Networks based on the GSM standard.
- Supports maximum theoretical data transfer rates of 42 Mbit/s when HSPA+ (*High Speed Packet Access*) is implemented in the network.
- Due to the W-CDMA technique it requires new base stations and new frequency allocations (W-CDMA is modification of DS-SS technology).
- **Frequency bands:** 850 MHz, 900 MHz, 1700 MHz/1900 MHz/2100 MHz (depending on country and provider).

12.2.1 Mobile cellular systems

Long term evolution (LTE)

High speed standard for mobile phones and data terminal developed by the 3GPP (3rd Generation Partnership Project). It extends the GSM/EDGE and UMTS/HSPA network technologies.

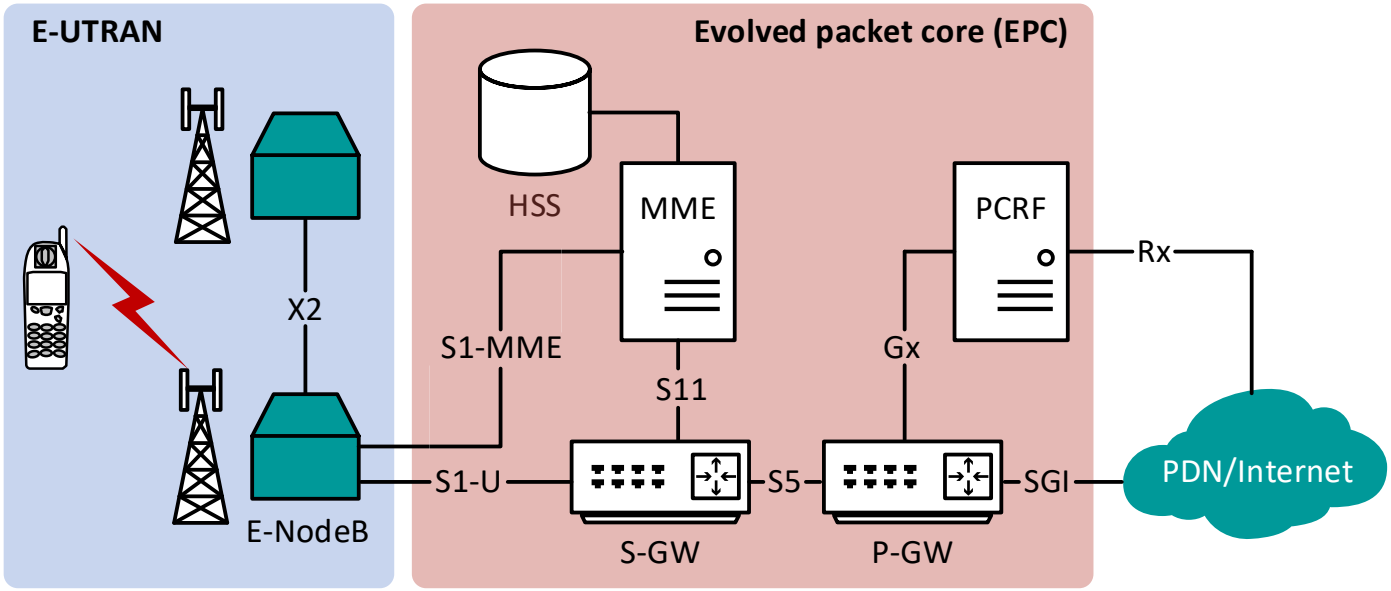
LTE main advantages:

- **Increased carrier capacity (coverage within a few decibels of the Shannon limit)**
- **Reliable connectivity**
- **High-speed data rates**

LTE characteristics:

- **Downlink modulation scheme: QPSK, 16-QAM, 64-QAM, 256-QAM**
- **Uplink modulation scheme: QPSK, 16-QAM, 64-QAM (depending on the UE, see below)**
- **Frequency Division Duplex (FDD) or Time Division Duplex (TDD)**
- **Implementation of advanced MIMO technique**
- **FDD/TDD carrier aggregation (Release 12)**
- **Massive MIMO and beamforming (Release 12)**

LTE Architecture



- **Mobility Management Entity (MME)** handles all of the signaling exchanges between the UEs and the EPC, as well as those between the eNodeBs and the EPC. The MME has the following functions:
  - ✓ Authentication: enables UEs to authenticate to the network
  - ✓ Mobility management: allows the subscriber mobility within the network
  - ✓ Location update: keeps track of the subscriber location within the network
  - ✓ Handover support: enables handover between eNodeBs
  - ✓ Bearer establishment – establishes bearers through a gateway router to the Internet.

12.2.1 Mobile cellular systems

- **User Equipment (UEs)** is mobile station**.**
- **eNodeB:** a part of the E-UTRAN radio access network, the component that allows UEs to connect to the LTE network**.**
- **S-GW** (*Serving Gateway*) acts like an anchor for handover between neighboring eNodeBs routes and routes all the user data packets.
- **P-GW** (*Packet Data Network Gateway*) provides the UE's connectivity to external **PDN** (*Packet Data Network*), acting like the point of exit and entry of traffic for the UE.
- **Home Subscriber Server (HSS)** is a central database that contains subscription-related and user-related information.
- **Policy and Charging Rules Function (PCRF)** ensures the service policy and sends Quality of Service (QoS) information for each session begun and accounting rule information.
- **Policy and Charging Enforcement Function (PCEF)** performs policy enforcement and service data flow detection, allowing data flow through the implemented P-GW.
- **S1 interface** connects the E-UTRAN and the EPC for both the user and the control planes.
- **S1-AP interface** connects the eNodeB to the MME and is based on IP transmission.
- **X2 interface** provides connectivity between two or more eNodeBs. It have the same structure as the S1 interface.

12.3 Wireless data networks

- *WLAN (Wireless Local Area Network),* links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), 0.9, 2.4 a 5 GHz, IEEE 802.11 standard WiFi (100m), IEEE 802.16 (40 km) Wi-Max, HiperLAN/2 5.7 GHz, 54 Mbps.
- *WWAN (Wireless Wide Area Network),* telecommunications network that links across metropolitan, regional, or international boundaries using leased telecommunication lines, 0.85, 2.4 GHz, Mobitex, CDPD (*Cellular Digital Packet Data*).
- *WLL (FWA) (Wireless Local Loop (Fixed Wireless Access))*. Wireless stationary communications link (*"last mile"* connection) for delivering PSTN or Internet access to telecommunications customers (public services), LMDS (*Local Multipoint Distribution System*), 28GHz, 1GHz BW, MMDS (*Multi-channel Multipoint Distribution System*), 2.5GHz, 200MHz BW.
- PAN (*Personal Area Network*): systems for data transmission among devices such as computers, telephones and personal digital assistants, Bluetooth 2.4 GHz IEEE 802.15.1, 1 Mbps, TDMA, HomeRF 2.4 GHz, CSMA/TDMA.

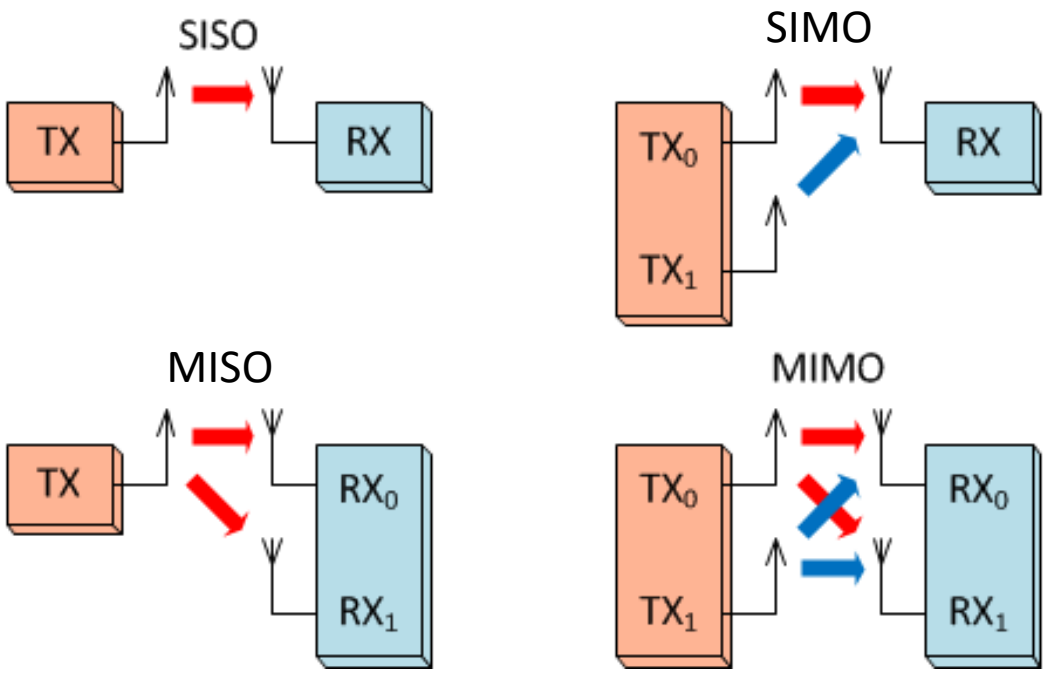
12.3 Wireless data networks
12.3.1 Wireless Local Area Network - WiFi

WiFi standards	802.11a	802.11b	802.11g	802.11n
Bit rate [Mb/s]	54	11	54	200
Modulation techniques	OFDM	CCK	OFDM& CCK	OFDM/ MIMO
Frequency [GHz]	5.1 - 5.3	2.4 - 2.497	2.4 - 2.497	5 a 2.4
Introduced	1999	1999	2003	2009

- **CCK (*Complementary code keying*) is a variation of DS SS based on on M-ary Orthogonal Keying and utilizes *poly-phase complementary codes*. Carrier modulation format is QPSK.**
- **OFDM (*Orthogonal frequency-division multiplexing*) is a method of encoding and modulation digital data on multiple carrier frequencies. Each sub-carrier is modulated with a conventional modulation scheme (such as QAM or PSK) at a low symbol rate.**

12.3.1 Wireless Local Area Network - WiFi

- **MIMO (*Multiple-input and multiple-output*): use of multiple antennas at both the transmitter and receiver sides to improve data throughput and link range without additional bandwidth or increased transmit power (by spreading the same total transmit power over the antennas to achieve an array gain that improves the spectral efficiency and/or to achieve a diversity gain that improves the link reliability).**

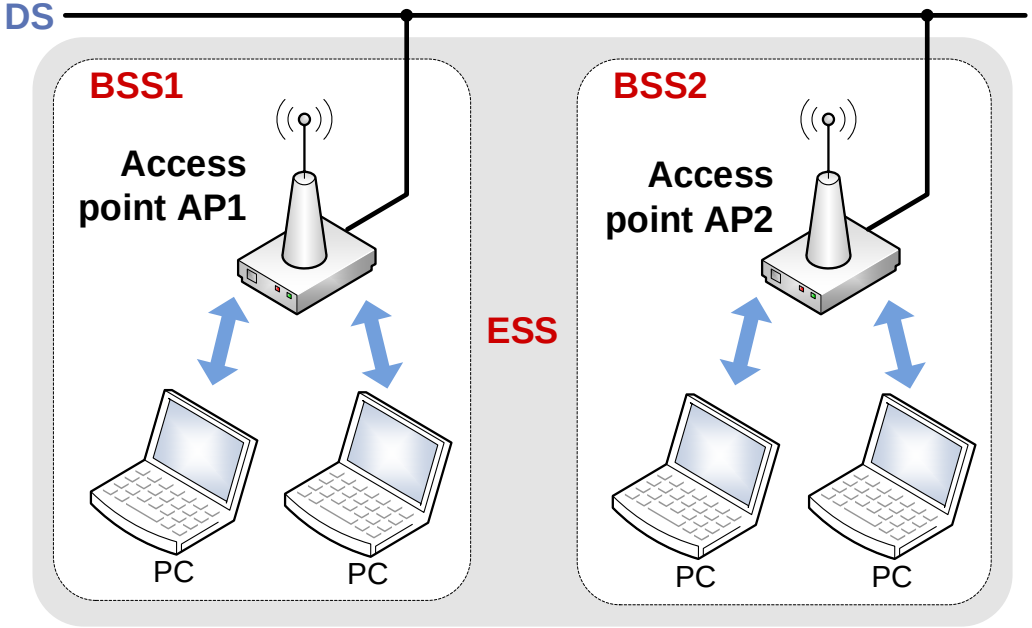


S = single
M = multiple
I = input
O = output

Tx_0 and Tx_1 transmits different information

WiFi network configuration

- Ad hoc mode, a peer-to-peer mode making it possible to connect two computers equipped with wireless adapters to one another bidirectionally.
- Infrastructure mode, making it possible to connect computers to a wired network using a device called an access point (AP)
  - Computers are grouped into a cell called BSS (*Base Station Set*).
  - Cells are grouped into ESS (*Extended Station Set*).
  - Communication of computers from different ESS is possible via DS (*Distributed system*) – Internet.



12.3.1 Wireless Local Area Network - WiFi

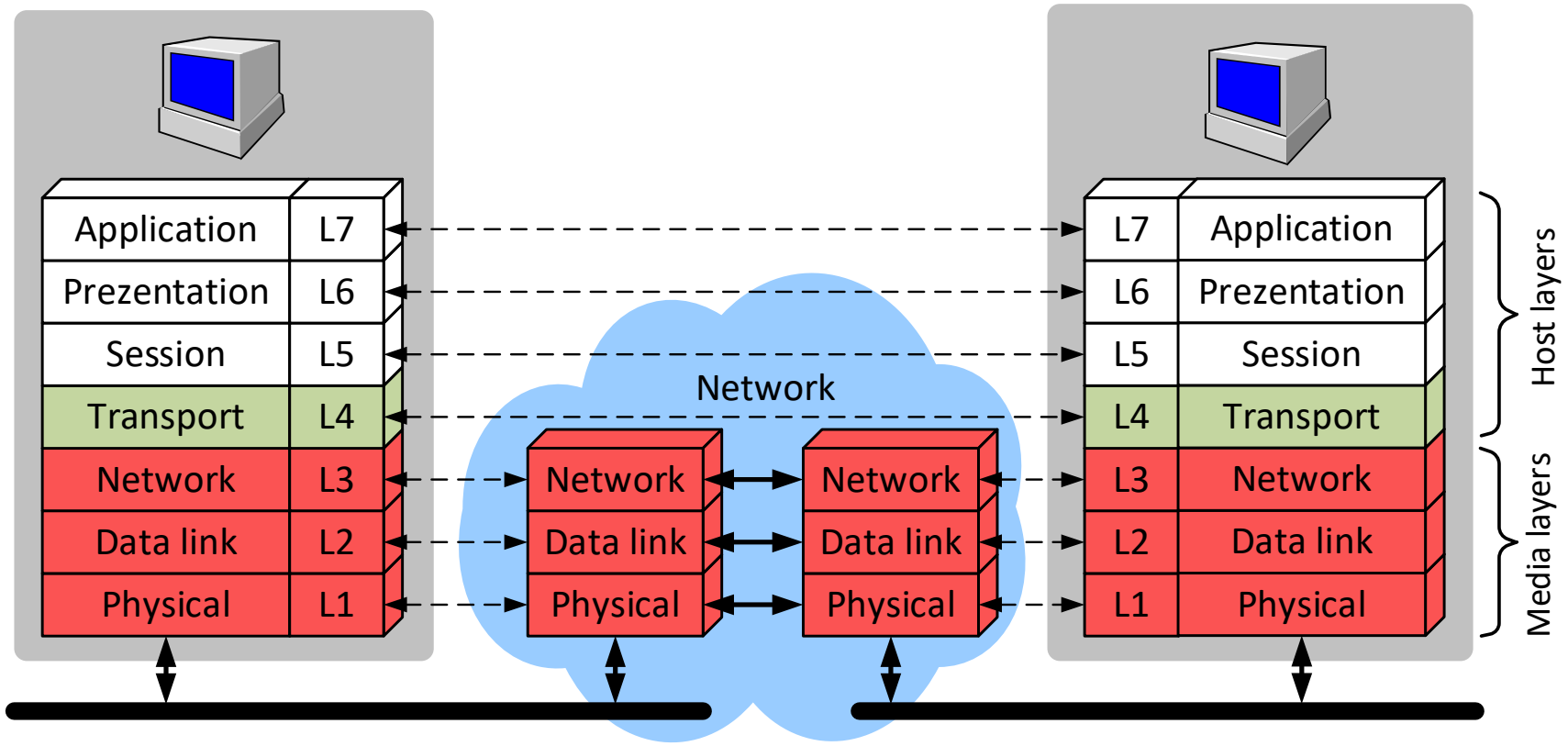
WiFi security protocols

- *WEP* (*Wired Equivalent Privacy*) uses a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change, stream enciphering using the RC4 algorithm.
- *WPA* (*Wifi Protected Access*) dynamically generates a new unique 128-bit key for each 802.11 frame using the RC4 algorithm. WPA also includes a message integrity check designed to prevent an attacker from capturing, altering and/or resending data packets.
- *WPA 2* introduces CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*), a new AES (*Advanced Encryption Standard*) - based encryption mode with strong security.

13. DATA TRANSMISSION IN COMPUTER NETWORKS

13.1 Open System Interconnection Model

The *Open Systems Interconnection model* (OSI) characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. OSI groups the functions into seven logical layers:



13.1 Open System Interconnection Model

Layer	Data unit	Function
Application	Data	Network process to application. Interaction with software applications that implement a communicating component.
Presentation	Data	Data representation, encryption and decryption techniques, conversion of machine dependent data to machine independent data (data translating between application and network formats).
Session	Data	Control the dialogues between computers. Establishing, managing and terminating sessions between the local and remote application.
Transport	Segment	Reliable delivery of packets between nodes on a network, control the reliability of a given link through flow control, error control and segmentation/desegmentation.
Network	Packet/ Datagram	Addressing, routing and (not necessarily reliable) delivery of datagrams (variable length data sequences) between nodes on a network.
Data link	Bit/Frame	A reliable direct point-to-point data connection. Definition of frame synchronization, detecting and possibly correcting errors techniques.
Physical	Bit	A (not necessarily reliable) direct point-to-point data connection. Specification of voltage levels, connectors, pins, transmission medium, impedance, cable specifications, flow control, etc.)

13.2 Computer Network Types

Different types of computer network designs can be categorized by their *topology, data rate, protocol used, scope, scale,* or *access* to other computers.

Common examples of area networks categorized by their scale are:

- **Personal Area Network (PAN): small computer network used by a single person within a building. It usually includes one or more computers, peripheral devices, telephones, and other personal (entertainment) devices.**
- **Local Area Network (LAN): network generally limited to a single building (network in an individual office building). It can accommodate up to thousands of computers and allows easy sharing of resources, such as data storage and printers. LAN often combines wireless and wired connection of network nodes.**
- **Metropolitan Area Network (MAN): network across an entire city or small region. Depending on the configuration it covers an area from 5 to 50 km across.**
- **Wide Area Network (WAN): occupies a very large area, such as an country, continent, or the entire world.**

13.2 Computer Network Types

Examples of area networks categorized by the computer access are:

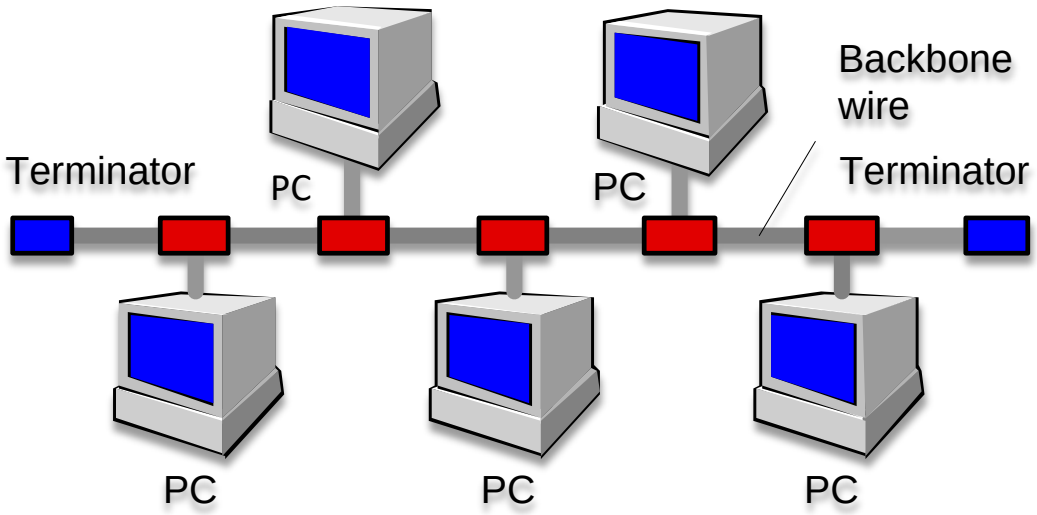
- **Client/server:** distributed system consisting of both client and server software. A client initiates a connection and generates a service request. The server fulfills the service and replies with requested data to the client.
  Example of the client software: **web browser or E-mail client.**
  Example of the server software: **web server, FTP server, E-mail server, print server, etc.**

- **Peer-to-peer:** each node has the same privileges and can initiate and manage a communication session. Each node has both the server and the client capabilities and share resources of other nodes.

13.2 Computer Network Types

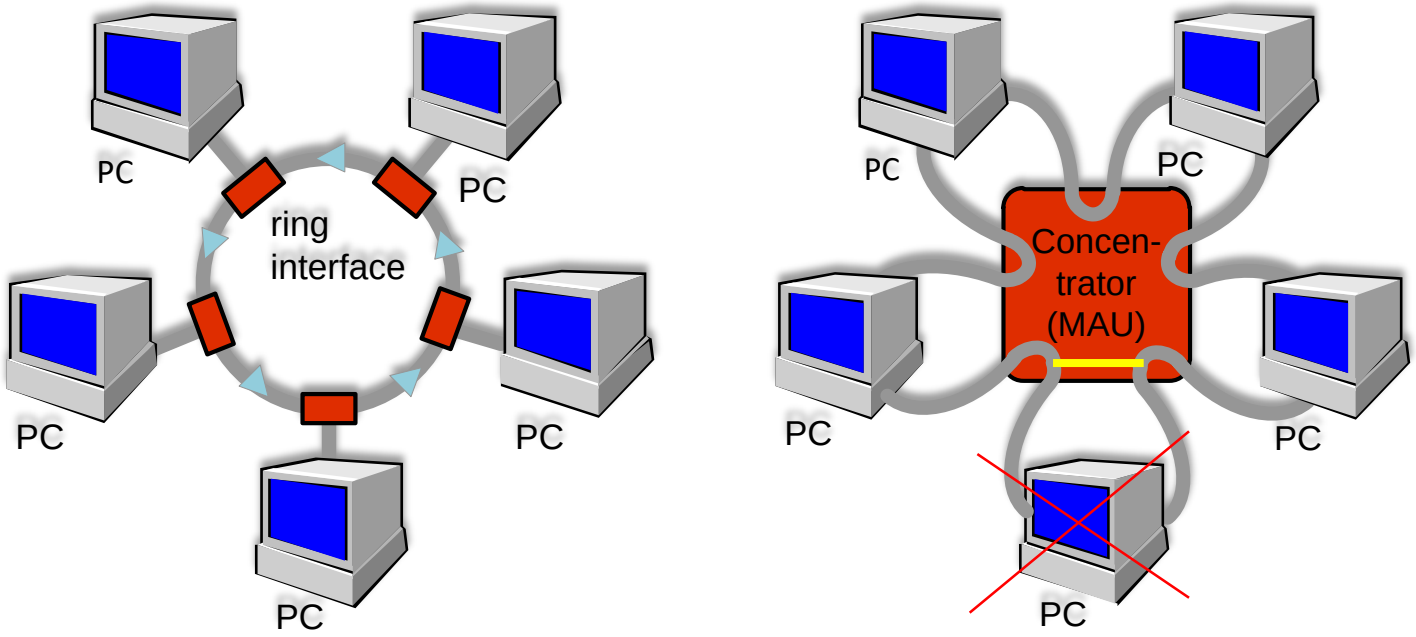
Specific types of area networks categorized by the topology are:

- **Bus topology:** uses a common backbone wire (coaxial cable) to interconnect all devices. A device requiring to communicate with another device sends a broadcast message onto the wire and only the intended device actually accepts and processes it. Bus topology suffers from difficult failure detection and limited range. Example: **Ethernet 10Base-2.**



13.2 Computer Network Types

- **Ring topology:** computers are connected in a circle. A data packet (Token) generated by some node is examined by the next node. If the address match to the address of the node, the packet is copied, otherwise it is passed on to the next node until it reaches back the originating node, where is discarded.



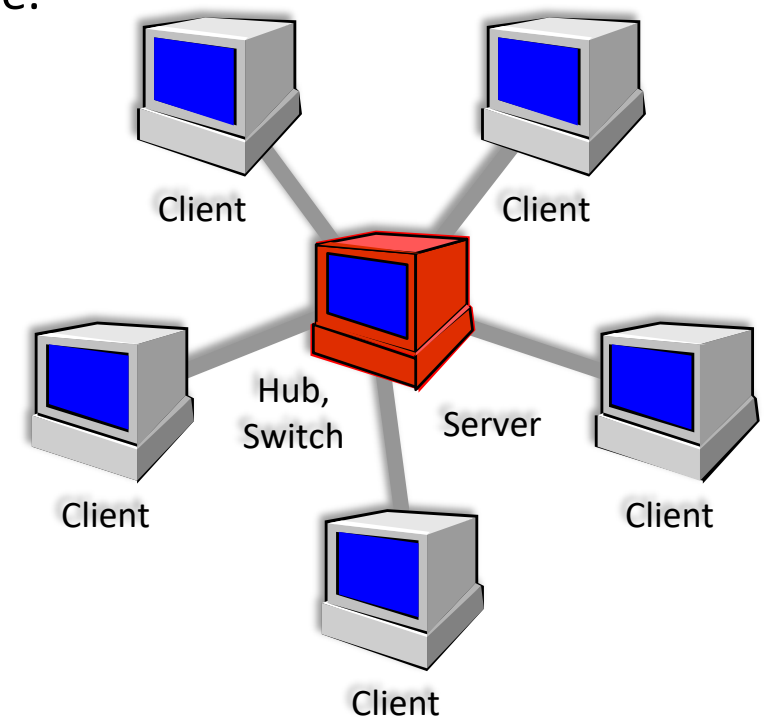
Example: IBM Token Ring, FDDI (*Fiber Distributed Data Interface*).

A failure of any node causes breakdown of the entire network. Therefore the modification increasing the network reliability was developed. It is based on the concentrator **MAU (*Multiple Access Unit*)** that bypasses the failed node.

13.2 Computer Network Types

- **Star topology:** all communication passes via a central node (PC, hub, switch). The central node acts as the server and the peripherals are the clients. The star topology uses a structured cabling that allows a simple adding of additional nodes. The disadvantage of this topology is that the server represents a potential source of the entire network failure.

  Examples: **Ethernet 10Base-T, 100Base–T.**

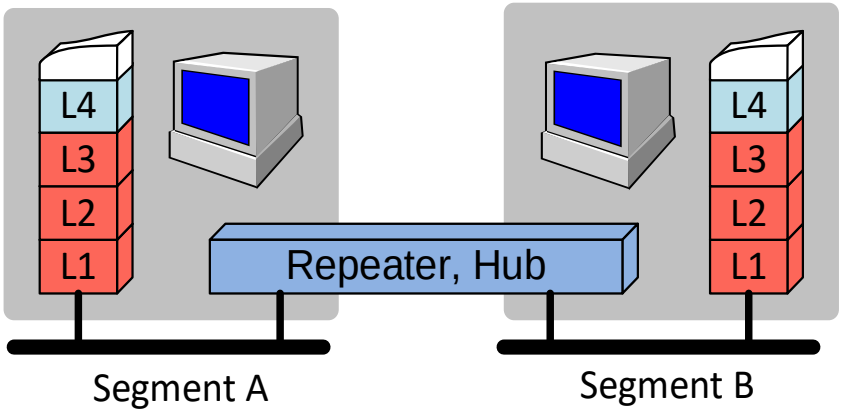


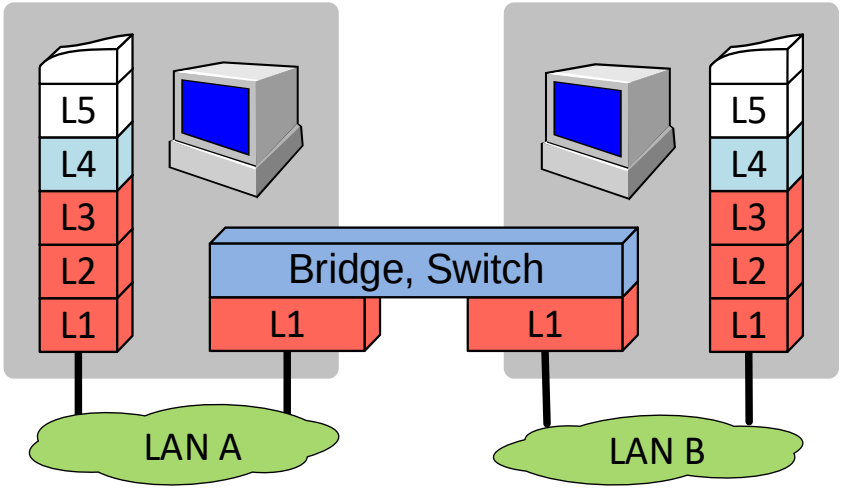
The network topology can be

- **logical:** defines how devices appear connected to the user,
- **physical:** corresponds to the actual interconnection with wires and cables.

13.3 Active components in computer network

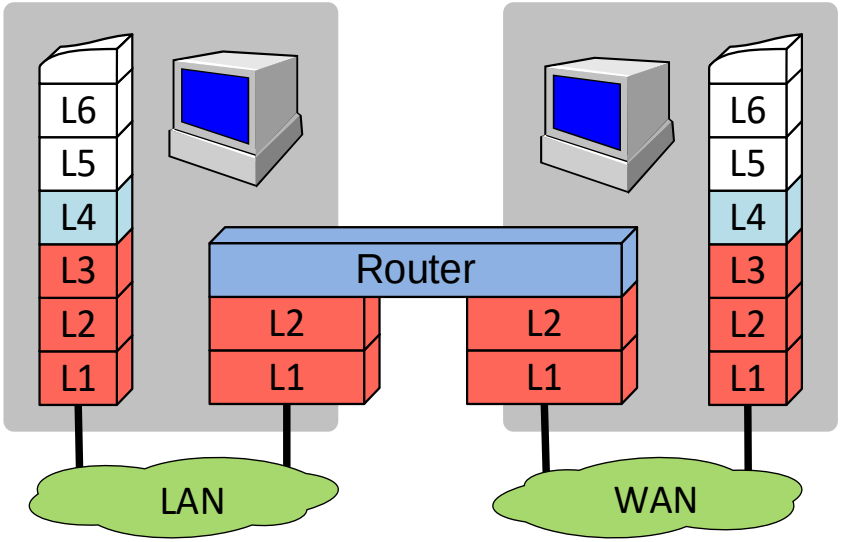
- **Repeater:** extends the reach of cabling, interconnects two network segments, amplifies and regenerates data and sends them away. It works at **L1**.
- **Hub:** interconnects a few network segments at **L1**, receives, amplifies and regenerates data and sends them to all other computers connected to a hub.
- **Bridge:** filters and forwards packets between two LANs or two segments of the same LAN at **L2** (reads the address and transmits only those packets whose address belongs to the destination LAN).
- **Switch**: the same device as bridge, but usually with multiple ports.





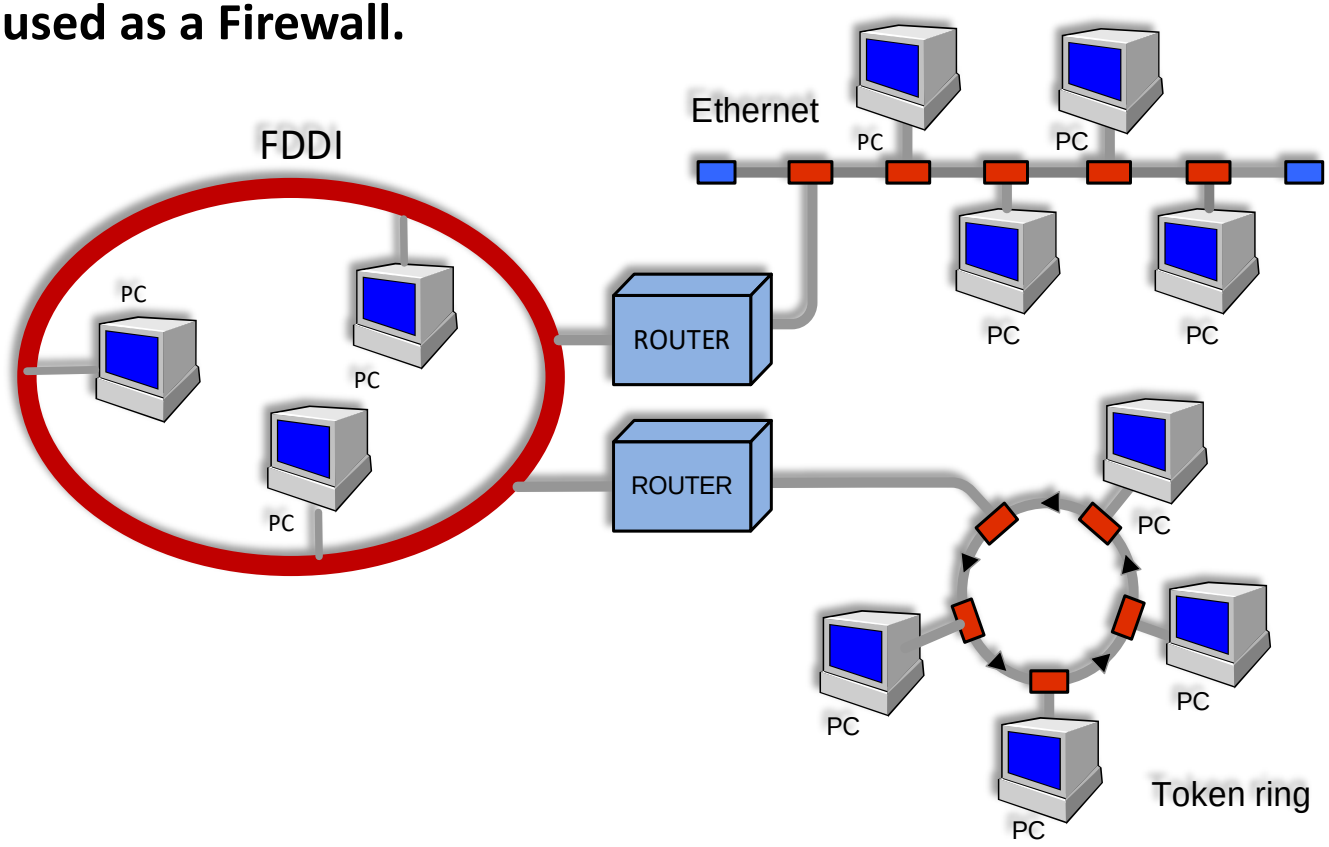
13.3 Active components in computer network

- **Router:** device at **L3** that collects information about the connected networks, selects the best path to forward packets (looking for the best path between addresses), and isolate each LAN into a separate subnet.



13.3 Active components in computer network

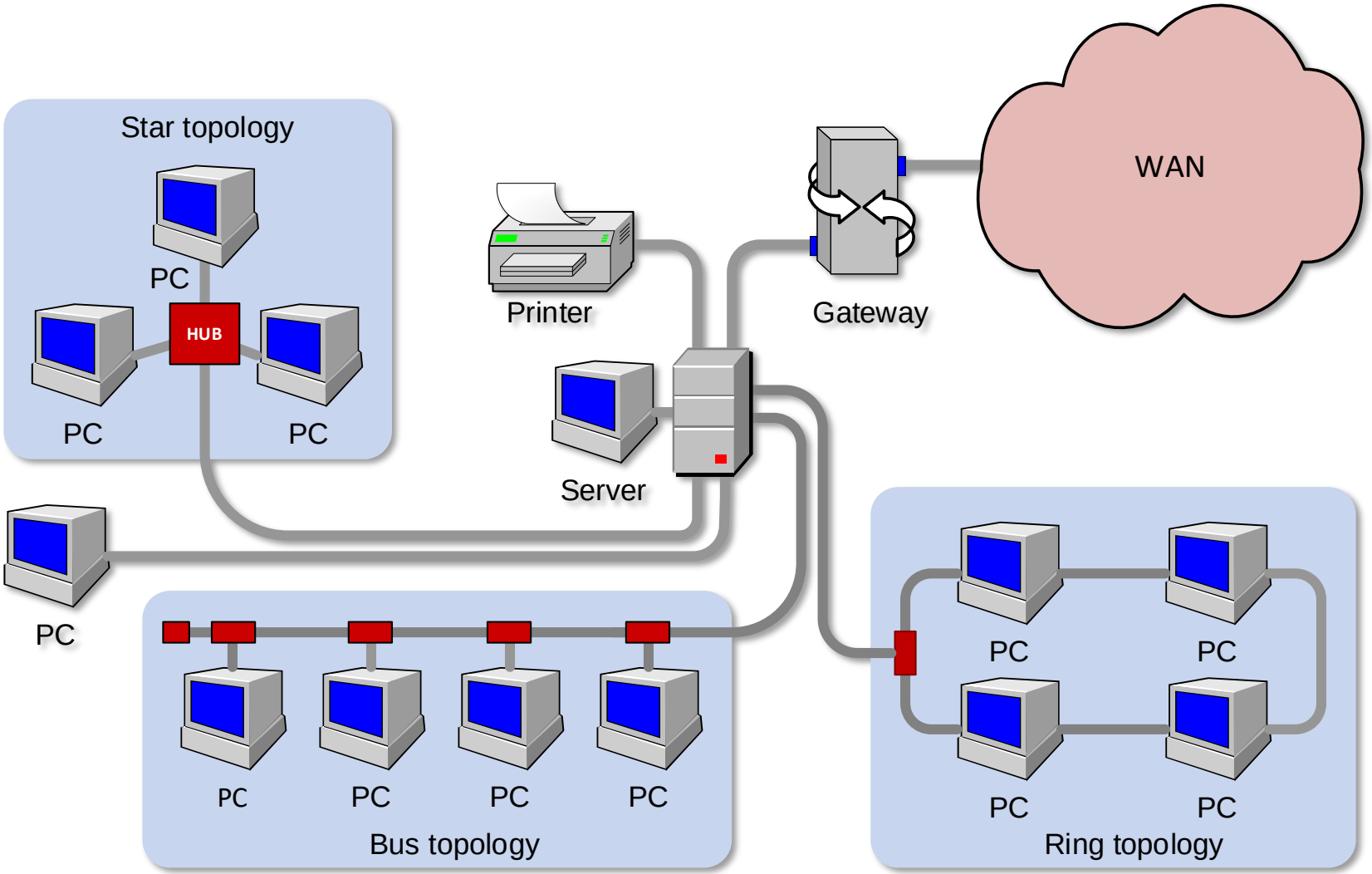
A typical use of the router is to connect a LAN to the Internet. Due to filtering it can be used as a Firewall.



Gateway: router that interconnects networks with different protocols. It can contain devices such as protocol translator, impedance matching devices, rate converter, etc. It can for example route data between a GSM network and the Internet. Gateway works at the application layer.

13.4 Local Area Networks (LANs)

Various topologies LANs and their connection to the wide area network



- Developed at Xerox PARC between 1973 and 1974.
- Standard IEEE 802.3: access method CSMA/CD applied to the bus network.
- Standard IEEE 802.3x (Ethernet II): applied to the twisted pair or fiber optic cable.

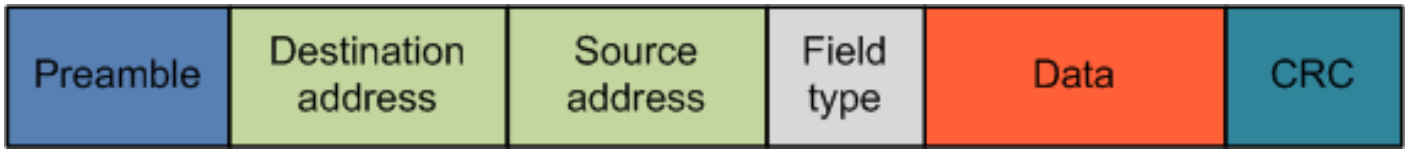
Transmission media

10Base	2	Thin Ethernet (coax)	185 m
	5	Thick Ethernet (coax)	500 m
	T	Twisted Pair	100 m
	FL	Multi-Mode Fiber Optic	2 km
100Base	TX	Twisted pair	185 m
	FX	Multi-Mode Fiber Optic	400 m

OSI layers

	datagram name
L 4	data segment
L 3	data packet
L 2	Frames (IEEE 802.3) Frames (IEEE 802.11) Cell (ATM)
L 1	Chip

Frame structure

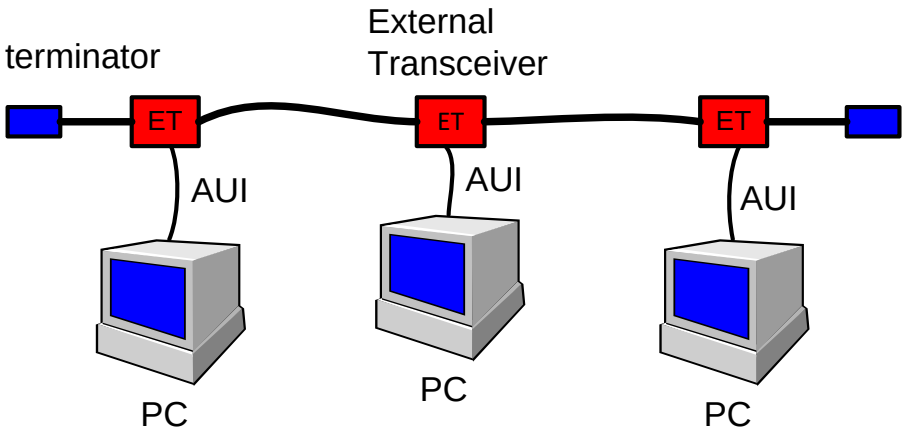


- **Preamble:** 8 byte. Bit sequence for frame synchronization.
- **Destination address:** 6byte, physical (MAC) address of target device,
- **Source address:** 6byte, physical (MAC) address of source device
- **Field type:** 2 byte, its value > 1500 corresponds to the Ethernet II frame (Internet Protocol (IP) datagram, Address Resolution Protocol (ARP), etc.). value > 1500 correspond to the Ethernet IEEE802.3. frame. Minimum frame length is 64B, (data 46B). Maximum frame length 1500B.
- *Media Access Control* (MAC) address: unique identifier assigned to network interfaces.

Ethernet network examples

Thick Ethernet 10Base – 5

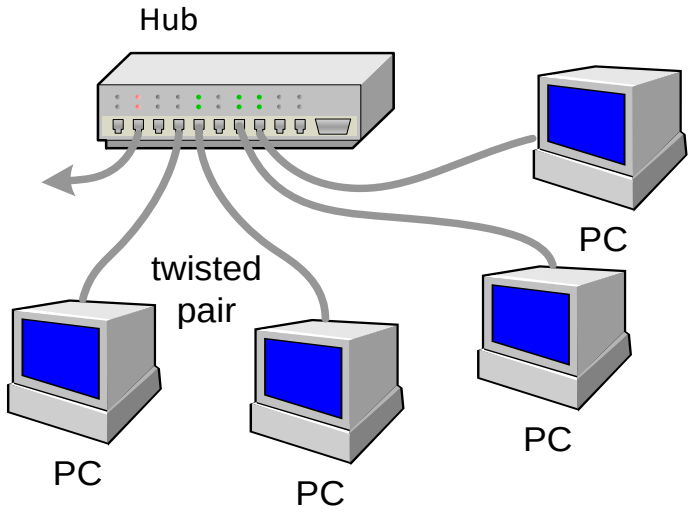
Uses thick 50 Ω coaxial cable



AUI: Attachment Unit Interface

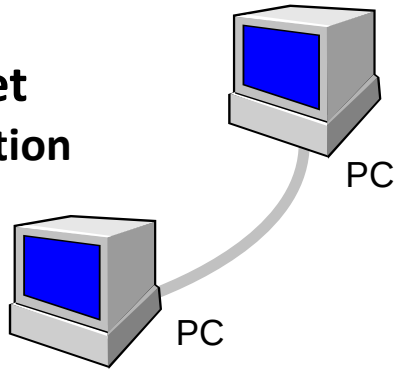
Twisted pair Ethernet 10Base – T, Fast Ethernet 100Base – T

Twisted pair impedance is 100 Ω



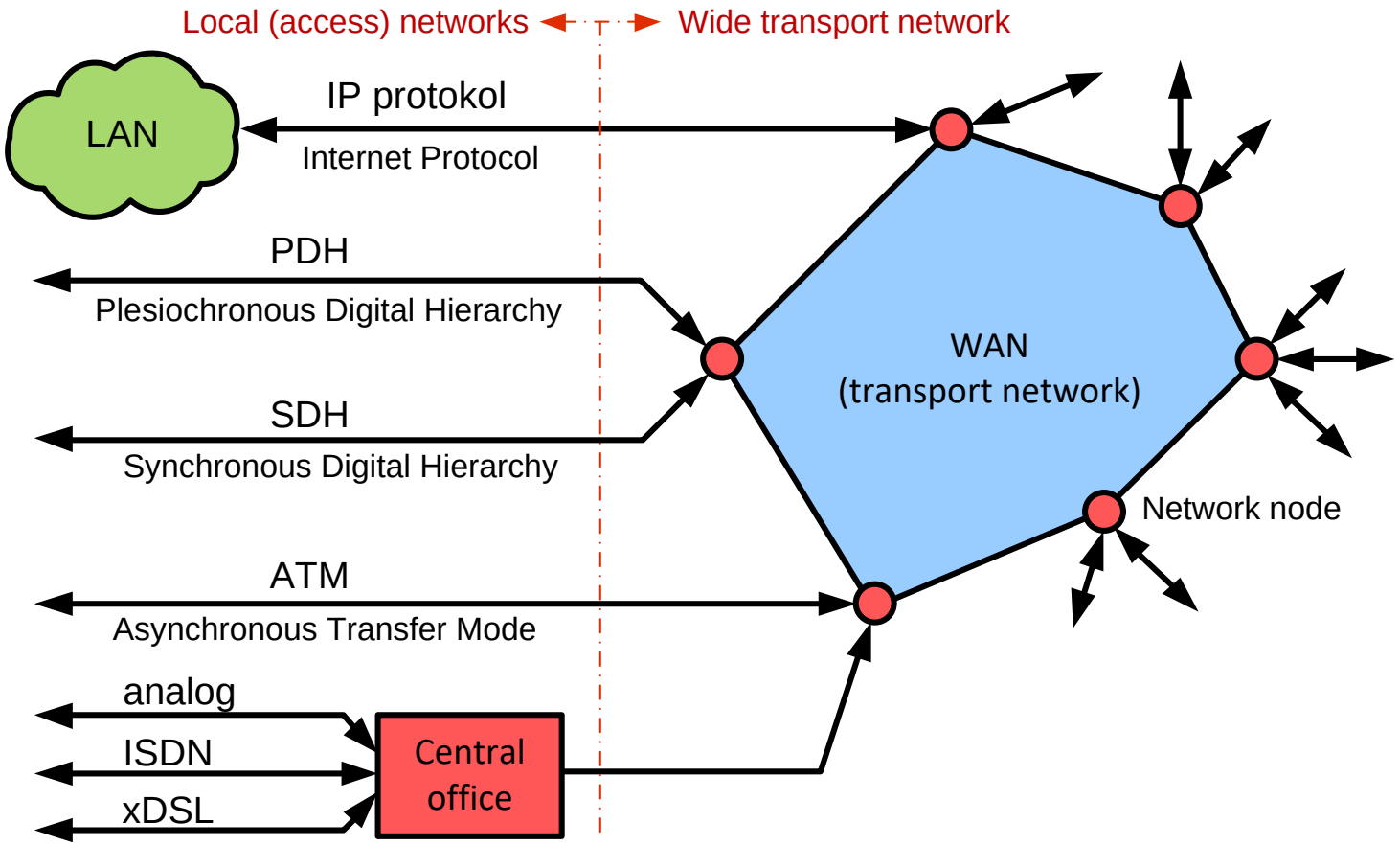
100Base – FX Ethernet

For point to point connection using optical fiber



13.5 Wide Area Networks

WANs (known as transport network) provide transport, multiplexing, switching, management, supervision and survivability of transmission channels carrying client data. They are intended for huge amount of data transmission at very high bit rate and are usually realized by optical or satellite broadband technologies.



13.6 Access Networks

- **Synchronous (*Synchronized*) digital hierarchy (SDH)**

  All of the clocks are synchronized to a master reference clock. They may be out of phase with each other but they will run at exactly the same frequency.

- **Plesiochronous (*Almost Synchronized*) digital hierarchy (PDH)**

  All of the clocks run at the same frequency to a defined precision. These clocks are not synchronized to each other so the data streams will run at slightly different rates.

- **Isochronous (*Synchronized*)**

  An Isochronous data stream has the timing information embedded in it (e.g. a G.704 stream). These data streams can be carried over Synchronous or Plesiochronous networks.

- **Asynchronous (*Not Synchronized*)**

  The clocks are not synchronized. The transmitter and the receiver have independent clocks that have no relationship with each other.

Aleš Prokeš

prokes@feec.vutbr.cz

Faculty of Electrical Engineering and Communication
Brno University of Technology

Technicka 12, CZ-616 00 Brno, Czechia

Tel: +420 54114 6581