Universitatea Politehnica Timişoara

Lecture 1. Data communications: Basic concepts, terminology and theoretical foundations

Objectives

- Improve your knowledge on data communications principles and foundations

Main Reference

[1] William Stallings, *Data and Computer Communications*, Eighth edition, Pearson Prentice Hall, 2007.

Basic Principles

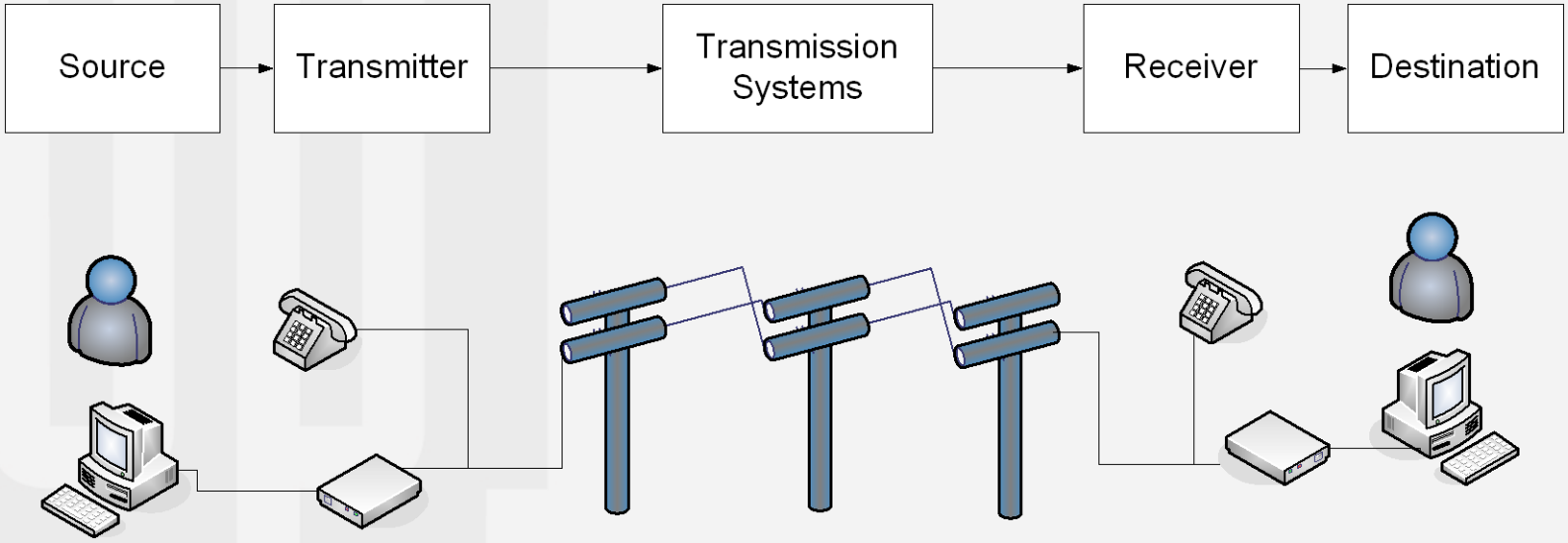
Data communications

- deals with the transmission of data between two electronic devices
- covers concepts such as:
  - data transmission
  - transmission media
  - signal encoding
  - interfacing
  - data link control
  - multiplexing

Basic Model

Consists of:

- **Source** – generates data to be transmitted
- **Transmitter** – encodes information
- **Transmission systems** – line or complex network connecting source and destination
- **Receiver** – converts the received signal in an interpretable form for destination
- **Destination** – takes incoming data



Data transmission

Transmission media:
- **Guided** – along a physical path, e.g. twisted pair, optical fiber
- **Unguided** – without a guided path, e.g. wireless

Direct link - path between two devices with no intermediate devices

Guided transmission:
- **Point to point** – direct link between two and only two devices sharing the same medium
- **Multipoint – more than two devices share the same medium**

Transmission type:
- **Simplex** - transmission in only one direction
- **Half-duplex** - transmission in both directions but not at the same time
- **Full-duplex** - transmission in both directions at the same time

Data transmission

Data encoding – how data should be represented, e.g. bits, characters etc.

Transmission channels:

- **analog** – transmits continuous signals (smooth, no discontinuities)
- **digital** – use digital encoding, transmits discrete signals (preserve different constant levels), data transmitted as bits

Transmission synchronization:

- **synchronous** – time occurrence of each signal representing a character is related to a fix time interval
- **asynchronous** – each character is individually synchronized (using start and stop bits)

Signal representation: periodic signals

If and only if $s(t+T)=s(t), t \in (-\infty,+\infty)$

e.g. sine wave: $s(t)=A\sin(2\pi ft+\phi)$

A – **amplitude**, peak value (strength)

f – **frequency**, repeat rate

T – **period**, the amount time until signal repeats

φ - **phase**, the relative position in time, within a period

λ – **wavelength**, the distance occupied by a single cycle

v – **velocity** of the signal (usually we used light speed) $\lambda = vT$

Time-domain representation

The signal is represented as a function of time

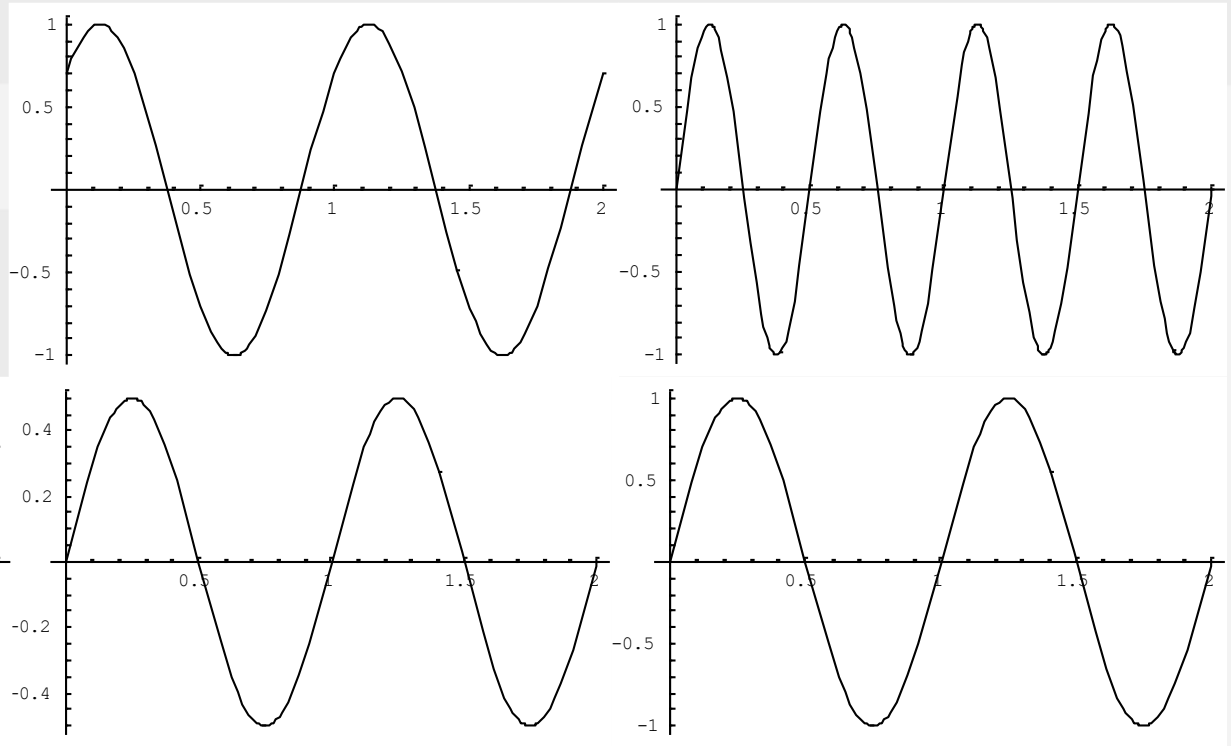
Take a look at the following signals in time-domain, and identify them in plots

$$s_1(t) = \sin(2\pi t)$$

$$s_2(t) = 0.5 \cdot \sin(2\pi t)$$

$$s_3(t) = \sin(2\pi 2t)$$

$$s_4(t) = \sin\left(2\pi t + \frac{\pi}{4}\right)$$

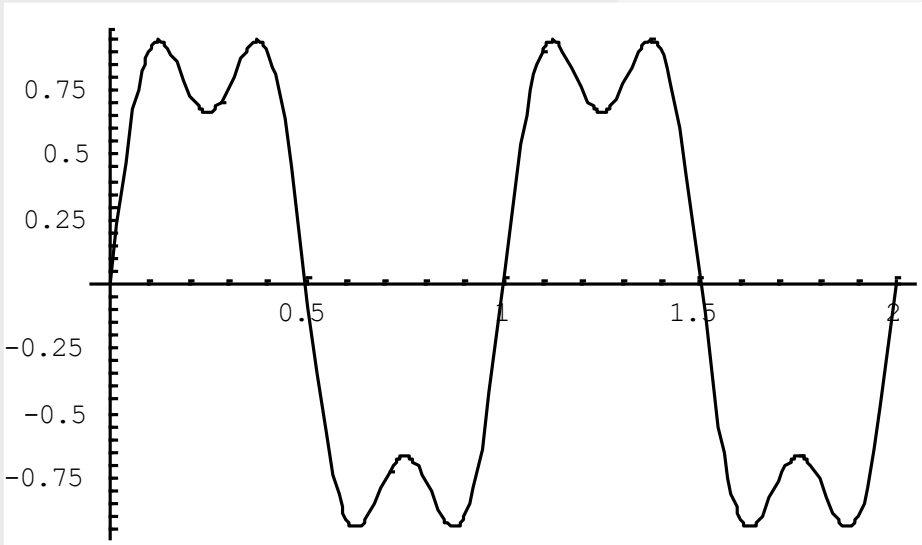


Frequency-domain representation

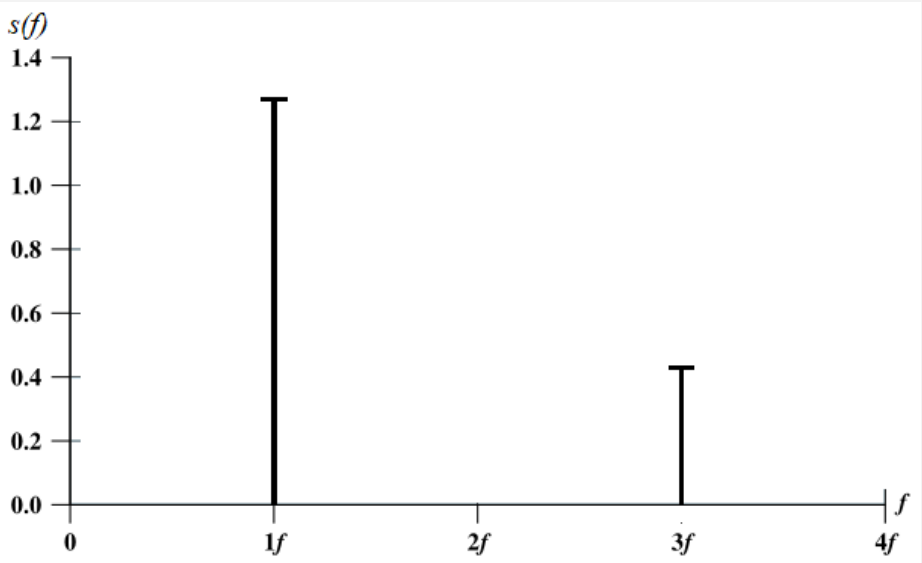
Signals can be also expressed as a function of frequencies

A real signal is made up of many components of various frequencies.

$$s(t) = \sin(2\pi f t) + \frac{1}{3}\sin(2\pi 3 f t)$$



Time domain



Frequency domain

Signal properties

Spectrum – the range of the frequencies in a signal
Absolute bandwidth – the width of the spectrum
Effective bandwidth (or just bandwidth) – the band of frequencies that contain most of the energy in the signal
DC component – components that have a zero frequency
Baseband signals – signals whose range of frequencies is measured from 0, for baseband signals bandwidth is equal to the upper cutoff frequency
Data rate - in data communication and computing is the quantity of data that is conveyed or processed per unit of time,

Remark: in computer networks and computer science bandwidth (digital bandwidth) is defined as the capacity for a given system to transfer data over a connection; and measured as a bit rate expressed in bits per seconds, e.g. Kb/s Mb/s etc (this is actually the data rate). The previous definition of bandwidth is often used in signal processing

Bandwidth and data rate

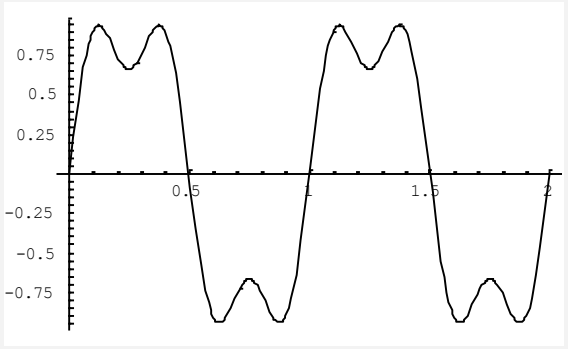
Suppose we are transmitting a square wave with *f=2 MHz* which corresponds to an alternating sequence of 0's and 1's

For the given *f* we have a data rate of *4Mbps* since 2 bits are sent in each period

$$T = \frac{1}{f} = 0.5 \times 10^{-6}$$

Now suppose we are approximating the square wave with the sum of the first 2 terms of the Fourier transform, i.e.

$$s(t) = \sin(2\pi ft) + \frac{1}{3}\sin(2\pi 3ft)$$



A bandwidth of 4Mhz is required since:

$$3ft - ft = 2ft = 4Mhz$$

Decibels

The decibel is a logarithmic unit of measurement that expresses the difference between two signal levels:

$$N_{db} = 10 \log_{10} \frac{P_1}{P_2}$$

Exercise:

- For a power loss of 3 db, what is the loss in percents between the power levels?
- If an amplifier has 30 db power gain what is the is the voltage ratio of the input and output?

Maximum data rate on ideal channels (no noise)

Universitatea Politehnica Timişoara

Nyquist has proved that the number of pulses that can be put on a telegraph line is:

$$f_P \leq 2B$$

2B (B- bandwidth) is also called Nyquist rate

Hartley stated that the number of distinct pulses that can be transmitted is limited by the signal amplitude and precision to distinguish between different levels of amplitude, i.e.

$$M = 1 + \frac{A}{\Delta V}$$

From this, the maximum data rate can be computed as follows (Hartley's law)

$$R = f_P \log_2 M \Rightarrow R \leq 2B \log_2 M$$

Maximum data rate on noisy channels

Universitatea Politehnica Timişoara

Shannon proved that the maximum data rate on a noisy channel (also called channel capacity) is:

$$C = B\log_2\left(1+\frac{S}{N}\right)$$

Where:

- C – channel capacity
- B – bandwidth
- S – signal power
- N – noise power

S/N is also called signal to noise ratio

By comparing Hartley's law and Shannon's channel capacity, we can compute the maximum number of distinguishable levels as:

$$M = \sqrt{1+\frac{S}{N}}$$

Example: Consider a 3000 MHz channel bandwidth with 30db signal to noise ratio, what is the channel capacity? How many distinguishable levels can be transmitted?

Data vs. Signals

Signals are used to represent **data.**
Both analog and digital signals can be used to represent digital or analog

	Analog Signal	Digital Signal
Analog Data	Two alternatives: • signal occupies the same spectrum as the analog data • analog data encoded to occupy a different portion of spectrum	Analog data encoded using a codec to produce a digital bit stream.
Digital Data	Digital data encoded using a modem to produce analog signal	Two alternatives: • signal consists of two voltage levels to represent the two binary values • digital data are encoded to produce a digital signal with desired properties.

(cf. [Stallings])

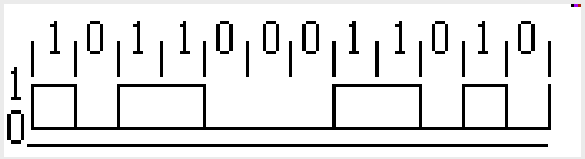
Digital Data – Digital Signal (Digital Encoding)

Digital signal encoding	Characteristics
Nonreturn to Zero-Level (NRZ-L)	0 – high, 1 – low
Nonreturn to Zero Inverted (NRZI)	0 – no transition at the beginning of interval, 1 – transition at the beginning o interval
Bipolar-AMI	0 – no line signal, 1 – positive or negative level (alternating for successive 1)
Pseudoternary	0 – positive or negative level (alternating for successive 0), 1 – no line signal
Manchester	0 – transition from high to low in the middle of interval, 1 – transition from low to high in the middle of interval
Differential Manchester	Always a transition in middle of interval. 0 – transition at the beginning of interval, 1 – no transition at the beginning of interval
B8ZS	Same as bipolar AMI, except that any string of eight zeros is replaced by a string with two code violations
HDB3	Same as bipolar AMI, except that any string of four zeros is replaced by a string with one code violation

Non-return to zero encodings

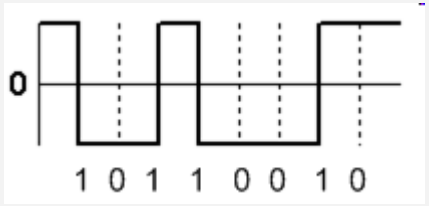
Non-return-to-Zero-Level (NRZL)

- “0” is represented as one physical level
- “1” is represented as another physical level



Non-return-to-Zero-Inverted (NRZI)

- “0” is represented as no transition
- “1” is represented as a transition



Remark: NRZI is a case of **differential encoding** (the signal is decoded by comparing two consecutive signal elements)

For more details and variants see *http://en.wikipedia.org/wiki/Non-return-to-zero*

Main limitations: lack of synchronization, presence of a dc component

Multilevel binary encodings

Bipolar AMI

- “0” is represented as no signal
- “1” is represented as positive ore negative pulse (consecutive 1’s alternate)

Pseudoternary (opposite to Bipolar AMI)

- “0” is represented as positive ore negative pulse (consecutive 0’s alternate)
- “1” is represented as no signal

Advantage: Absence of a dc component

Disadvantage: In both cases one bit always produces lack of synchronization

Fix: Introduce additional bits to force transitions (used in ISDN)

Remark: Multilevel binary is not efficient from information representation point of view as it requires 3 states to represent 2 distinct values.

How many bits of information could represents each signal element ? This leads to the need for an additional 3 db signal power

Binary encodings (continued)

Universitatea Politehnica Timişoara

Bipolar with 8 zeros substitution (B8ZS)

Intended to overcome the lack of synchronization when 0's are transmitted:

- An octet of 0's is represented as 000+-0-+ if the last voltage pulse was positive
- An octet of 0's is represented as 000-+0+- if the last voltage pulse was negative

High-density bipolar 3 zeros (HDB3)

Used in Japan, Europe, Australia

A nibble (4 consecutive bits) of 0's is represented as 0001 or 1001 according to the table

Polarity of preceding pulse	Odd number of ones since previous substitution	Even number of ones since previous substitution
-	000-	+00+
+	000+	-00-

Remark: In order to distinguish real sequences from scrambled sequences, code violations are forced.

Show what are the code violations for B8ZS and HDB3

The Big Picture, cf. [Stallings]

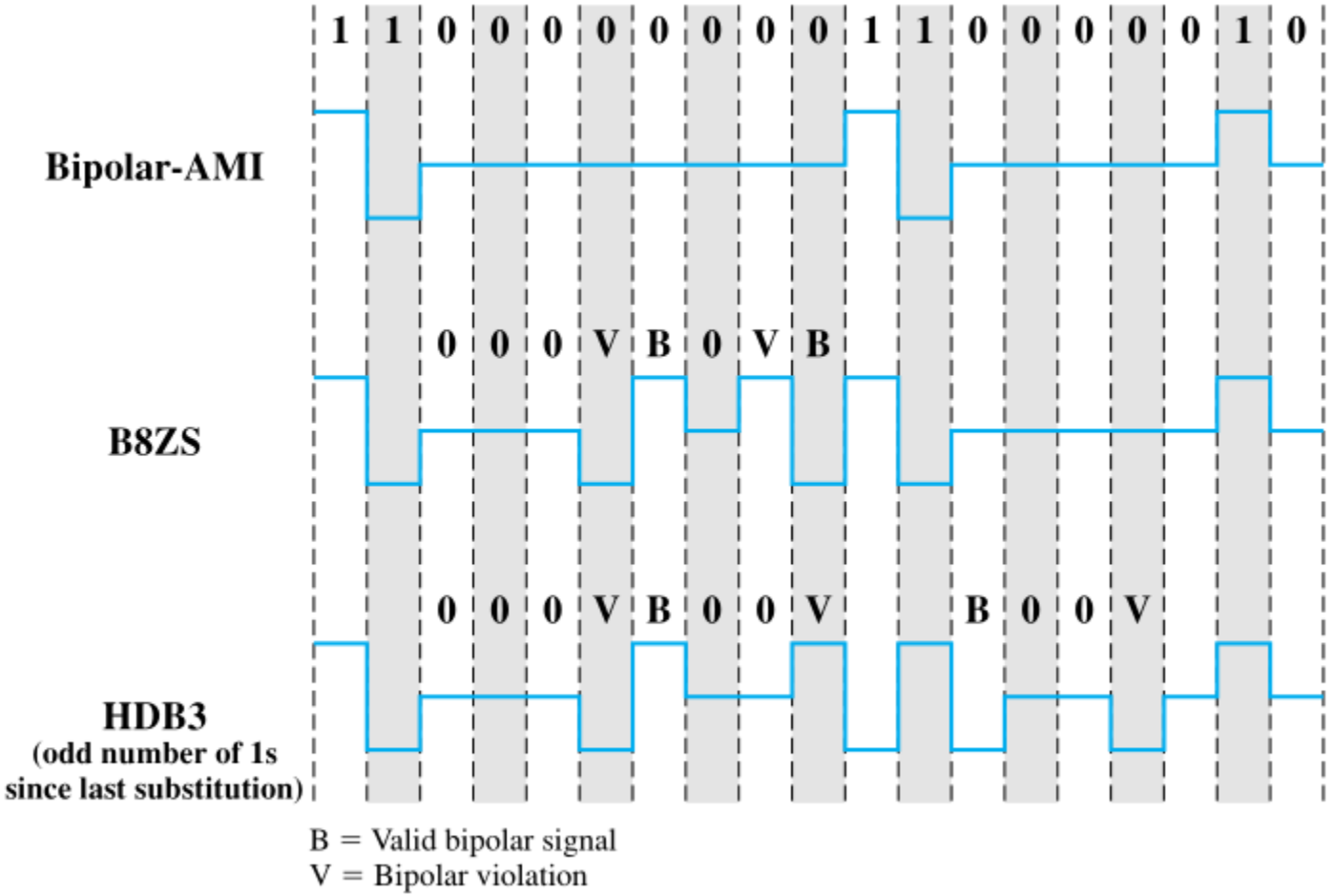


Figure 5.6 Encoding Rules for B8ZS and HDB3

Biphase encodings

Manchester

- “0” is represented as a high to low transition at the middle of a bit period
- “1” is represented as a low to high transition at the middle of a bit period

Differential Manchester

- “0” is represented as the presence of a transition at the beginning of a bit period
- “1” is represented as the absence of a transition at the beginning of a bit period

Advantages:

- Receiver can always synchronize (also called self-clocking codes)
- No dc component
- Error detection: absence of transitions can be used to detect errors

Disadvantage:

- As there may be two transitions per bit time, bandwidth is higher

The Big Picture, cf. [Stallings]

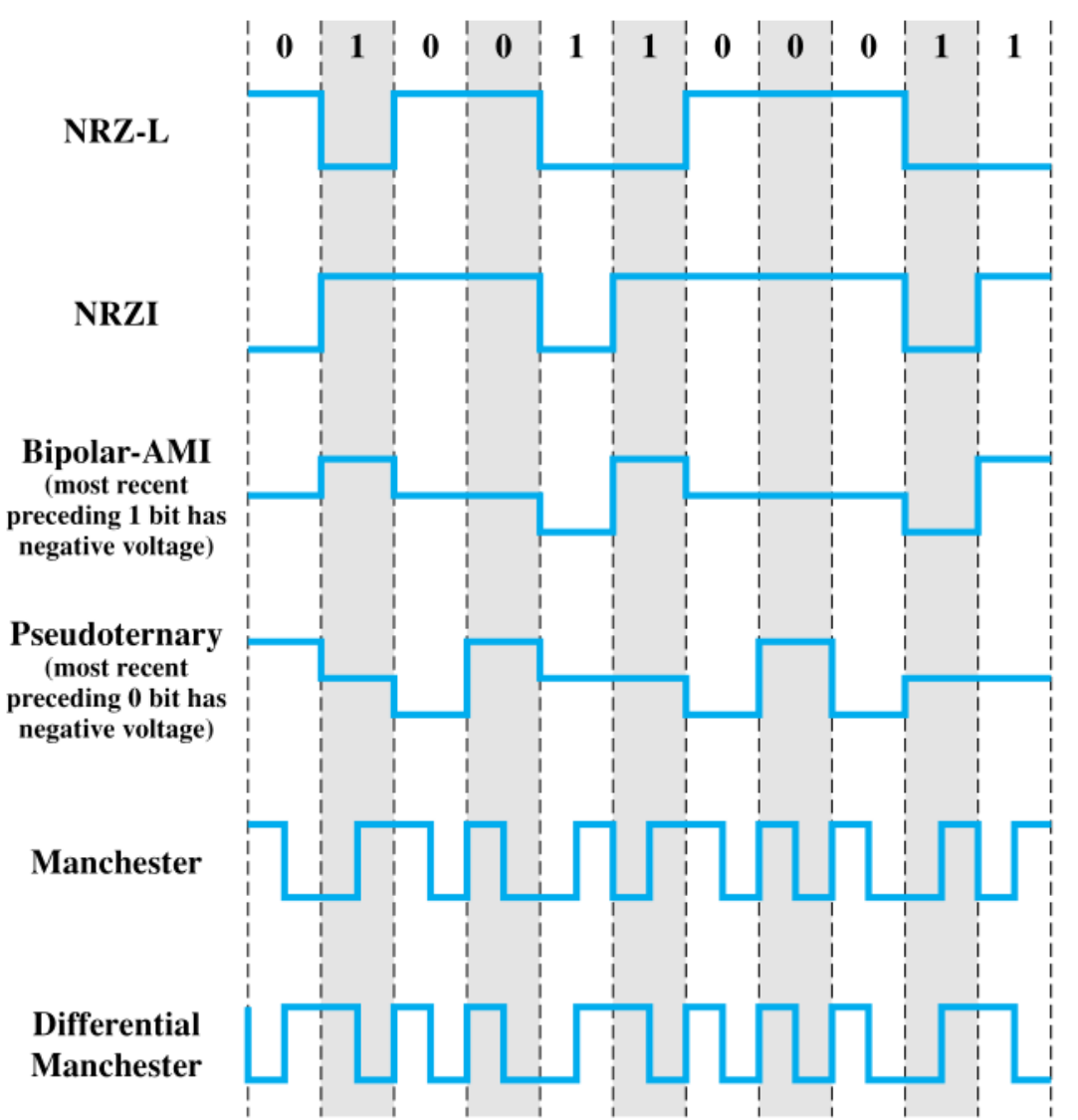


Figure 5.2 Digital Signal Encoding Formats

Modulation rate (Baud rate)

Universitatea Politehnica Timişoara

Baud - the number of distinct signal changes per second (measured in bauds)

Not to be confused with data rate (bit rate measured in bps)

The symbol duration time T_s can be computed based on the symbol rate f_s as:

$$T_s = \frac{1}{f_s}$$

For a gross bit rate of R bits per second and N bits for each symbol we have:

$$f_s = \frac{R}{N}$$

For a symbol rate f_s and M distinct signals we have:

$$R = f_s \log_2 M$$

Modulation rates for various encodings (cf. [Stallings])

	Minimum	101010…	Maximum
NRZ-L	0 (all 0s or 1s)	1.0	1.0
NRZI	0 (all 0s)	0.5	1.0 (all 1s)
Bipolar-AMI	0 (all 0s)	1.0	1.0
Pseudoternary	0 (all 1s)	1.0	1.0
Manchester	1.0 (1010…)	1.0	2.0 (all 0s or 1s)
Differential Manchester	1.0 (all 1s)	1.5	2.0 (all 0s)

Digital Data – Analog Signals (Digital Modulation)

The continuous constant-frequency analog signal that “carries” the data is known as the **carrier signal**.
Modulation is the process of encoding source data onto a carrier signal.

To transmit digital data using analog signals, an analog carrier signal is modulated by a digital stream.

Main modulation methods, based on the three characteristics (amplitude, frequency, phase):

- Amplitude-Shift Keying (ASK)
- Frequency-Shift Keying (FSK)
- Phase-Shift Keying (PSK)

Amplitude-Shift Keying (ASK)

Universitatea Politehnica Timişoara

Binary values are represented by two different amplitudes of the carrier

For example:

- "0" is represented by 0 amplitude
- "1" is represented by some constant non-zero amplitude

$$s(t) = \begin{cases} A\cos(2\pi f t), b = 1 \\ 0, b = 0 \end{cases}$$

Kind of "ON/OFF keying"

Lower error rates at higher amplitudes, but error rate also increases at higher noise

Frequency-Shift Keying (FSK)

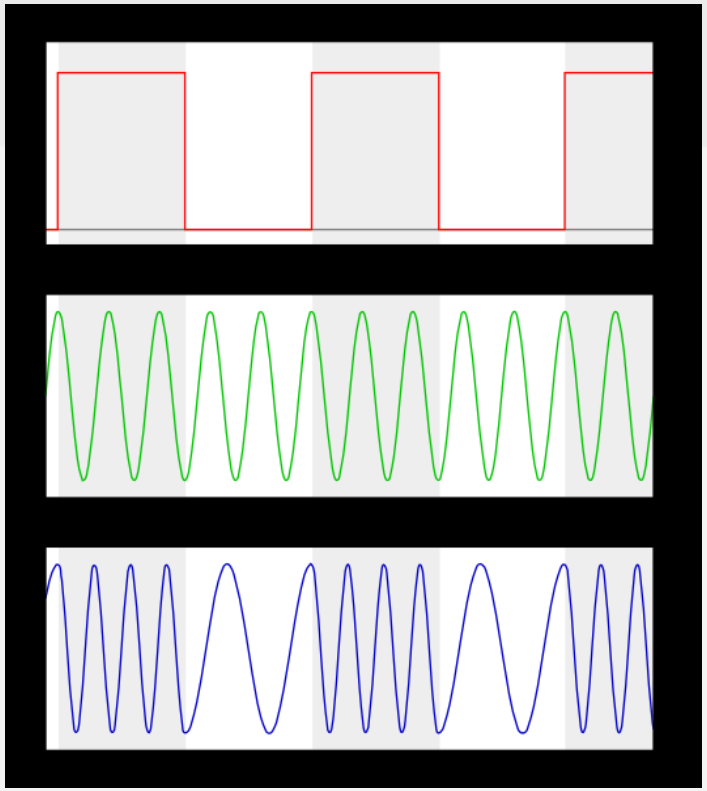
Universitatea Politehnica Timişoara

Binary values are represented by two different frequencies near the carrier frequency

For example:

- "0" is represented by *f1*
- "1" is represented by *f2*

$$s(t) = \begin{cases} A\cos(2\pi f_1 t), b = 1 \\ A\cos(2\pi f_2 t), b = 0 \end{cases}$$

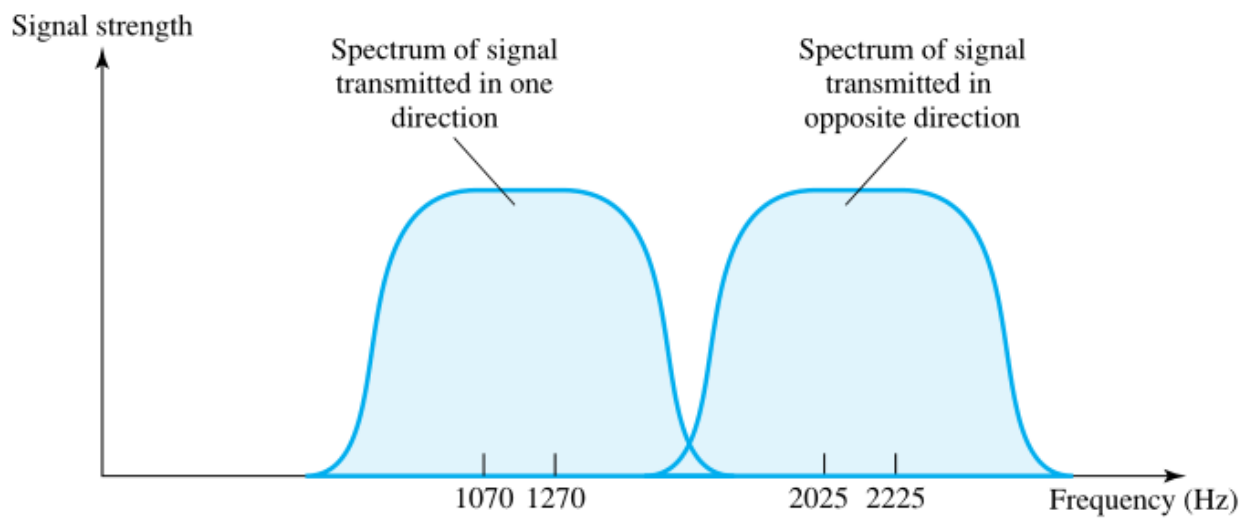


Cf. http://en.wikipedia.org/wiki/Frequency-shift_keying

FSK Example

- Voice grade lines pass frequencies in the range between 300 to 3400 HZ
- Remarks (non-related to FSK):
  - The bandwidth allocated for a single voice-frequency transmission channel is usually 4 kHz
  - The voiced speech of a typical adult male will have a fundamental frequency of from 85 to 155 Hz, and that of a typical adult female from 165 to 255 Hz
  - The generally accepted frequencies for human hearing are 20Hz – 20 kHz
  - Normal voice range is about 500 Hz to 2 kHz

- To achieve full-duplex the bandwidth can be split
- For example, Bell System 108 Series, in one direction centered around 1170 Hz and in another direction centered around 2125 Hz



Cf. [Stallings]

The V.21 Modem at 0.3 kb/s has 300 bauds and uses FSK

It is a variant of Bell 103, from AT&T, which can achieve full-duplex by splitting the frequency as follows:

- The originating station used a mark tone of 1,270 Hz and a space tone of 1,070 Hz
- The answering station used a mark tone of 2,225 Hz and a space tone of 2,025 Hz

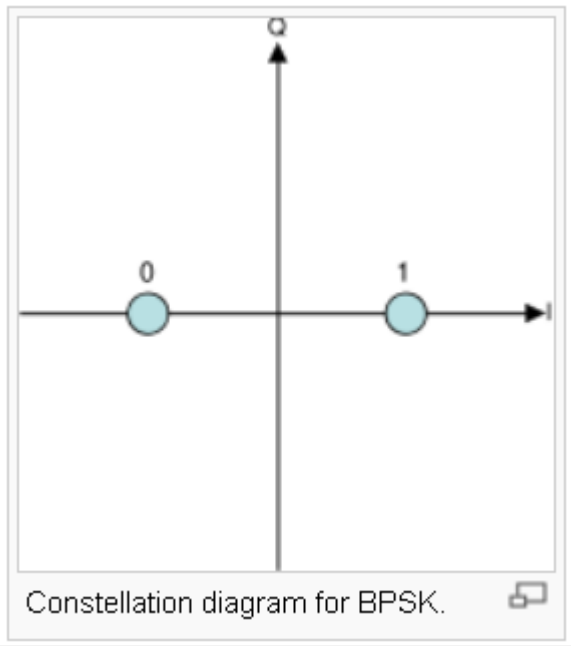
Phase-Shift Keying (PSK)

The phase of the carrier signal is shifted to represent data:

- Binary phase-shift keying (**BPSK**) – two phases separated by 180 degrees are used to represent 0's and 1's

$$s(t) = \begin{cases} A\cos(2\pi f t + \pi), b = 1 \\ A\cos(2\pi f t), b = 0 \end{cases}$$

http://en.wikipedia.org/wiki/Phase-shift_keying



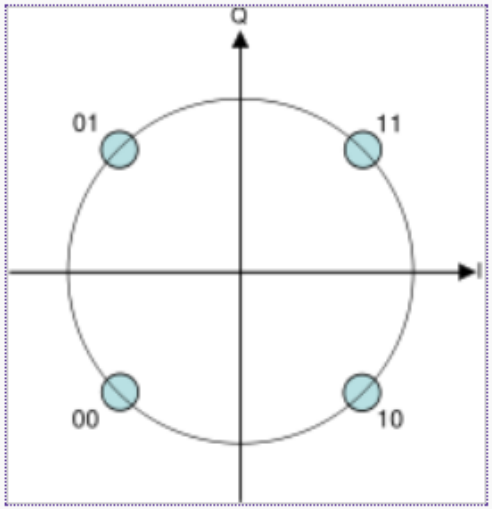
Constellation diagram for BPSK.

- Quadrature phase-shift keying (QPSK) (quaternary or quadriphase PSK) uses 4 points

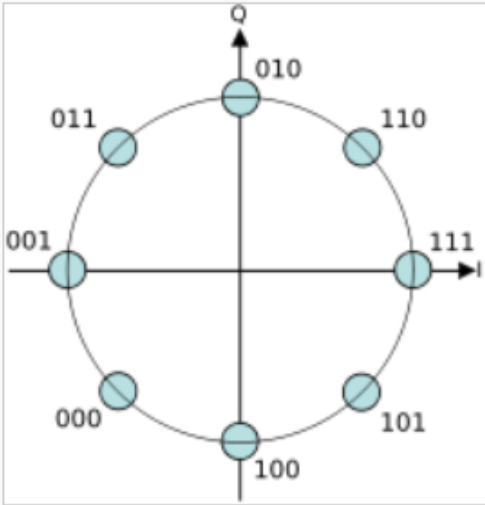
$$s(t)=\begin{cases} A\cos\left(2\pi ft+\frac{\pi}{4}\right), b=11 \\ A\cos\left(2\pi ft+3\frac{\pi}{4}\right), b=10 \\ A\cos\left(2\pi ft+5\frac{\pi}{4}\right), b=00 \\ A\cos\left(2\pi ft+7\frac{\pi}{4}\right), b=01 \end{cases}$$

- Higher-order PSK: 8-PSK is usually the highest order PSK as higher orders introduce to high error rates

http://en.wikipedia.org/wiki/Phase-shift_keying



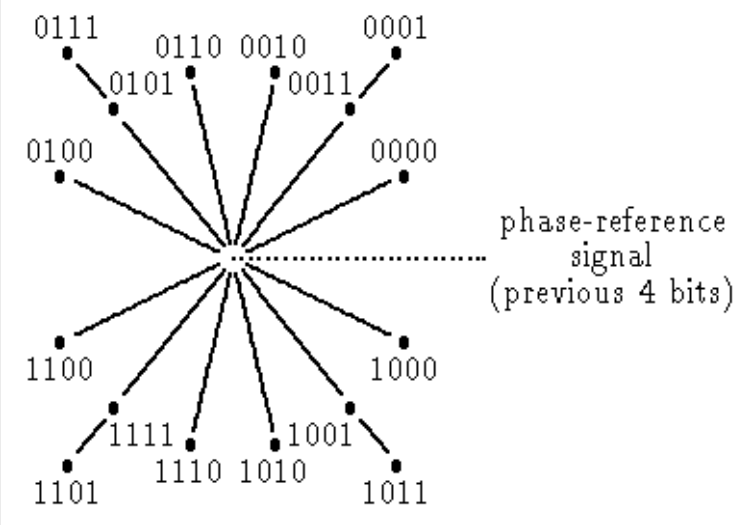
Constellation diagram for QPSK with Gray coding. Each adjacent symbol only differs by one bit.



Constellation diagram for 8-PSK with Gray coding.

Example

- A standard V.32 Modem at 9.6 kb/s has 2400 bauds
- This is because it uses 12 phase angles, 4 of which can have 2 amplitude values (mixed ASK and PSK)
- Explain why at 9.6 kb/s the baud rate is 2400 bauds



Analog Data – Digital Signals

- Digitalization: converting analog data to digital data
- Methods:
  - Pulse-code modulation (PCM)
  - Delta modulation (DM or Δ-modulation)
- For other variants see wiki: http://en.wikipedia.org/wiki/Modulation

Pulse-code modulation (PCM)

Based on the sampling theorem:

An analog signal that has been sampled can be perfectly reconstructed from the samples if the sampling rate was 1/(2B) seconds, where B is the highest frequency in the original signal

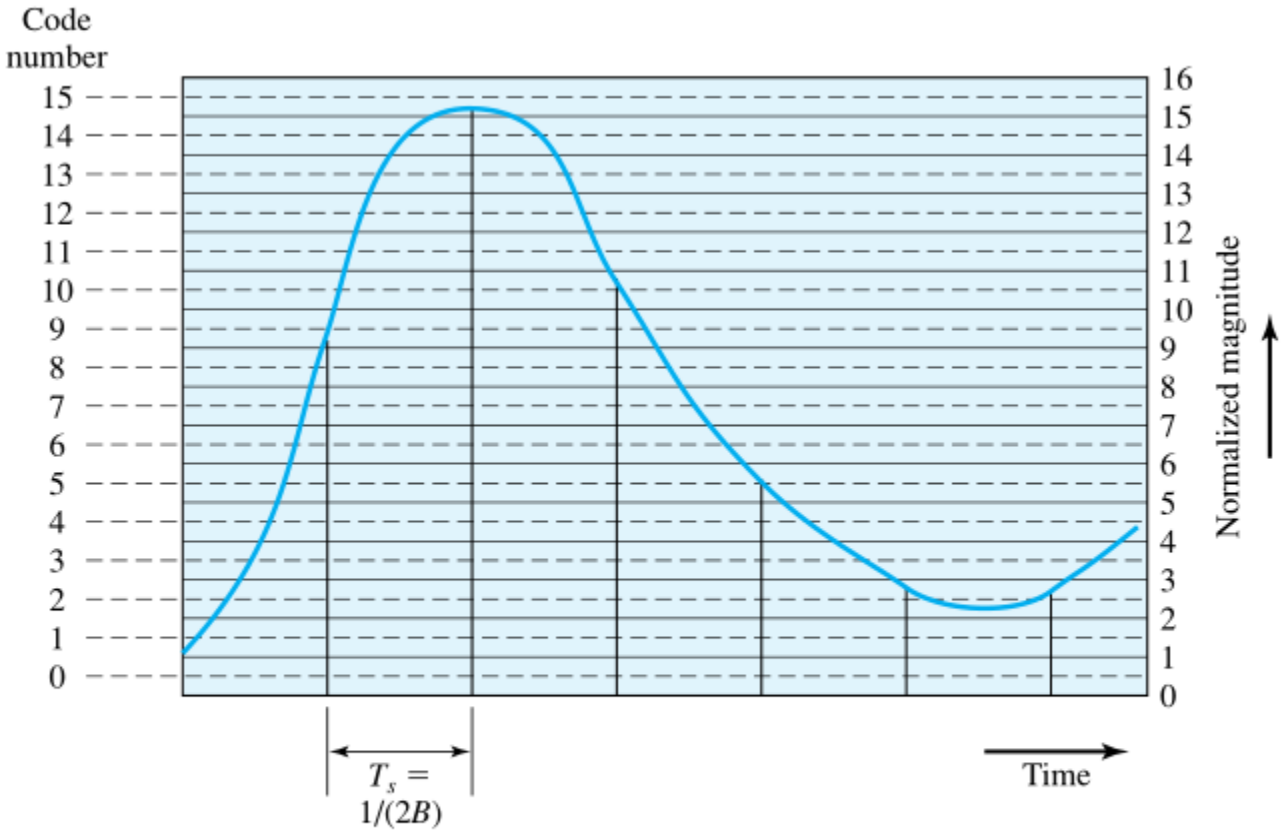
Example: for a voice grade line at 4khz for a complete reconstruction 8000 samples per second are needed

Pulse Amplitude Modulation (PAM) – samples are represented as pulses with amplitude proportional to the values of the signal

Pulse Code Modulation (PCM) – PAM samples are quantized on bits (approximated as n-bit integers)

Remark: This violates the sampling theorem, therefore the reconstructed signal is only an approximation of the original one

Example, cf. [Stallings]



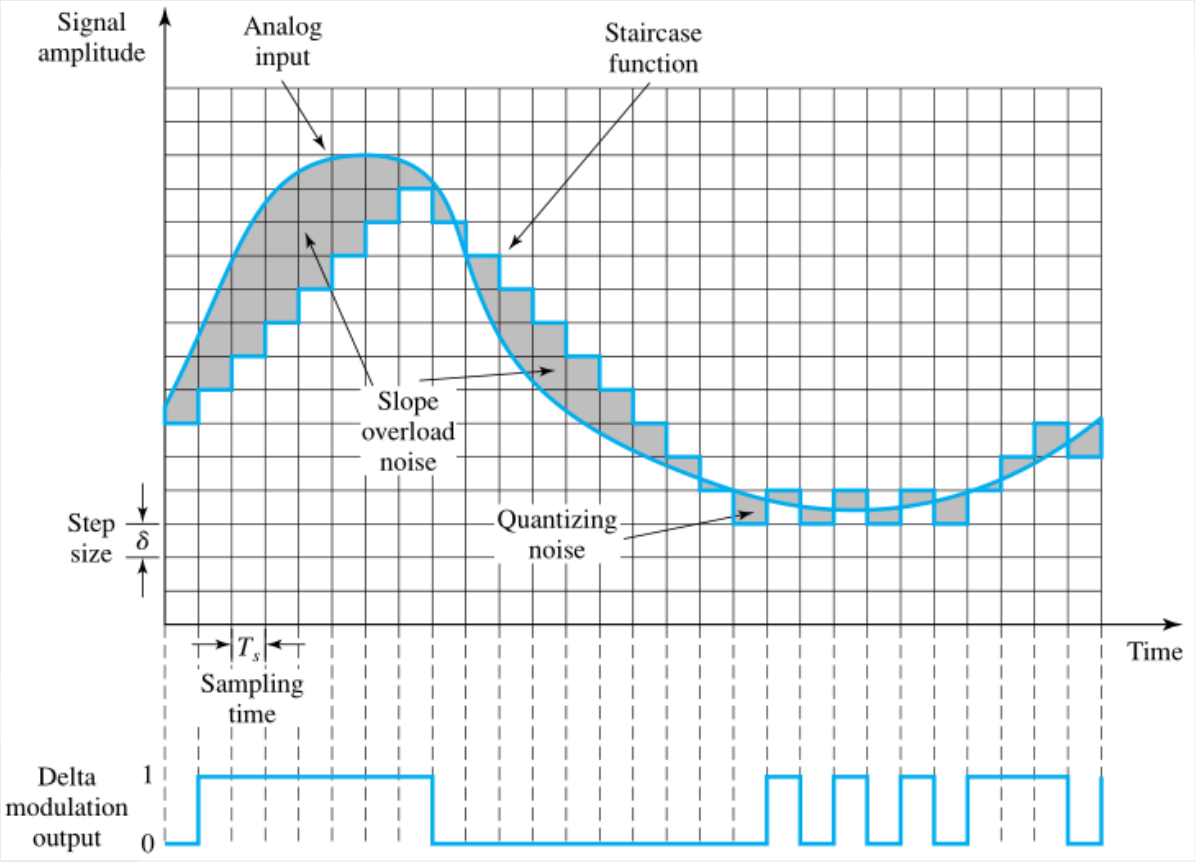
PAM value	1.1	9.2	15.2	10.8	5.6	2.8	2.7
Quantized code number	1	9	15	10	5	2	2
PCM code	0001	1001	1111	1010	0101	0010	0010

Example

- Remember that a voice grade line has 4KHz
  - What is the sampling rate according to the Sampling Theorem?
  - If for PCM 7 bits are used to encode each sample, what is the data rate of the communication line?
  - For the previous data rate, what is the minimal bandwidth that the channel require? What is the recommended bandwidth?
- Proof for sampling theorem:
  - See [Stallings]
  - For the original proof from Shannon see http://en.wikipedia.org/wiki/Sampling_theorem#Shannon.27s_original_proof

Delta Modulation

- Intended to reduce PCM complexity
- The input signal is approximated by a staircase that moves up or down by one quantization level
- Can be encoded as one binary digit for each sample



Cf. [Stallings]

Analog Data – Analog Signals (Analog Modulation)

Universitatea Politehnica Timişoara

Analog-over-analog methods:

- Amplitude Modulation (AM)
- Angle Modulation: Frequency Modulation or Phase Modulation (FM, PM)

The idea is to encode the frequency spectrum of a baseband signal on the carrier signal which is high frequency and can travel over longer distances (also known as Passband Modulation)

Motivation

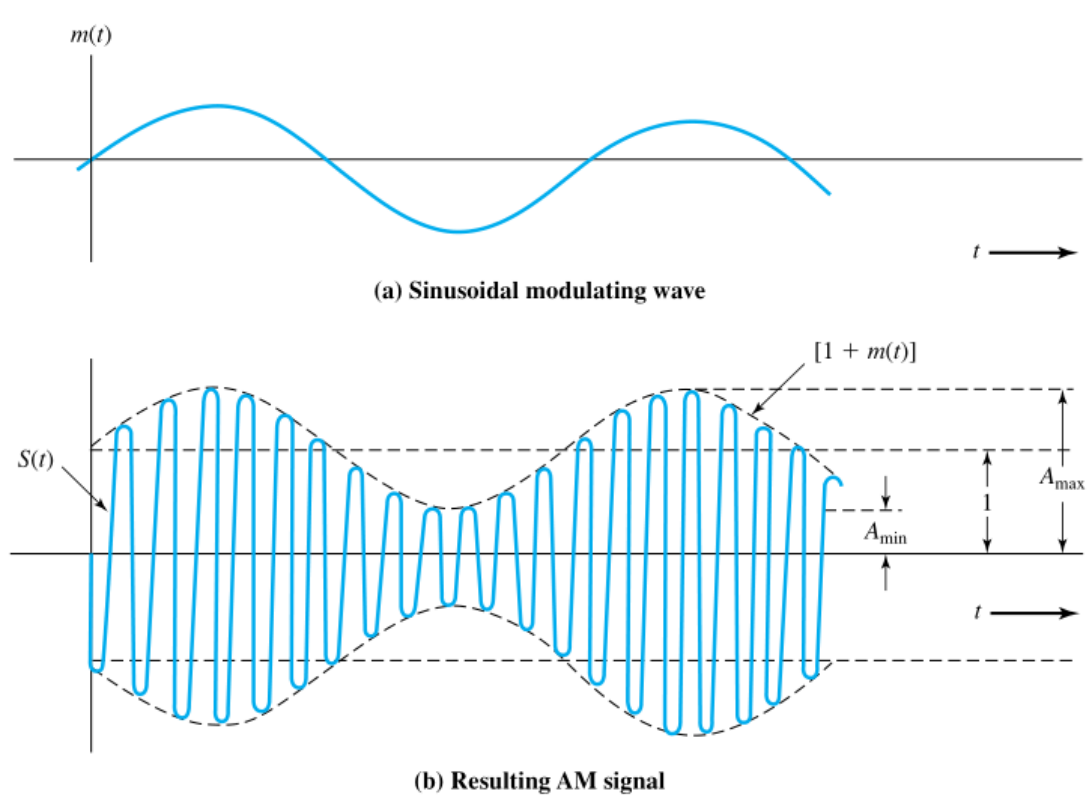
- You may ask yourself why do we need to encode analog onto analog
- This is needed for communication efficiency
- In wireless transmission the antenna must be at least a substantial fraction of the size of the wavelength
- Consider a 1 kHz which travels at the speed of light, i.e. 299,792,458 m/s
- The wavelength is 299,792 meters, i.e. 299 km
- Obviously … a too large antenna is needed
- Suppose this signal is modulated on a 30 Ghz carrier
- The wavelength is only 0.1 meter, i.e. 10 centimeters … obviously a smaller antenna

AM

The modulated signal is: $s(t) = [1 + n_A x(t)] \cos 2\pi f_c t$

- $x(t)$ input signal (modulating signal)
- f_c carrier frequency
- n_A modulation index (ratio of the amplitude of the original signal on the carrier)

$$m(t) = n_A\, x(t)$$



Cf. [Stallings]

Example

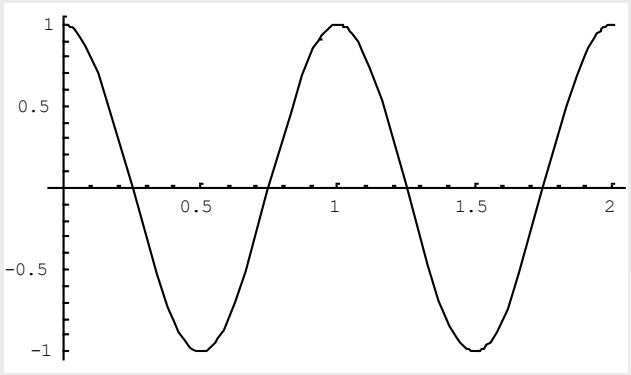
- For $x(t) = \cos 2\pi f_m t$
- We have $s(t) = [1 + n_A \cos 2\pi f_m t] \cos 2\pi f_c t$

$$\Rightarrow s(t) = \cos 2\pi f_c t + \frac{n_a}{2} \cos 2\pi (f_c - f_m)t + \frac{n_a}{2} \cos 2\pi (f_c + f_m)t$$

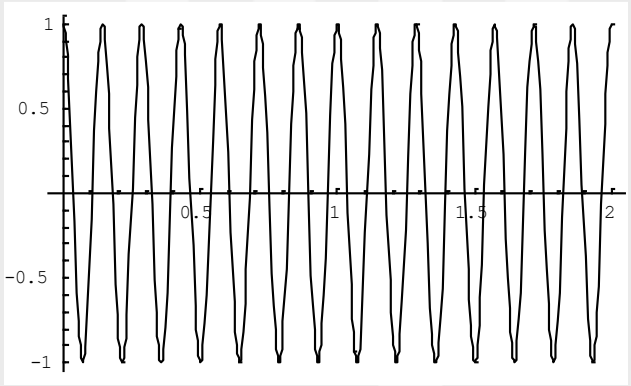
- The resulting signal has a component at the original frequency of the carrier and a pair of components deviated by the frequency of the modulating signal
- The value $1+n_A\ x(t)$ is called the envelope of the signal
- The envelope is an exact reproduction of the signal if and only if $n_A < 1$

Modulated signals

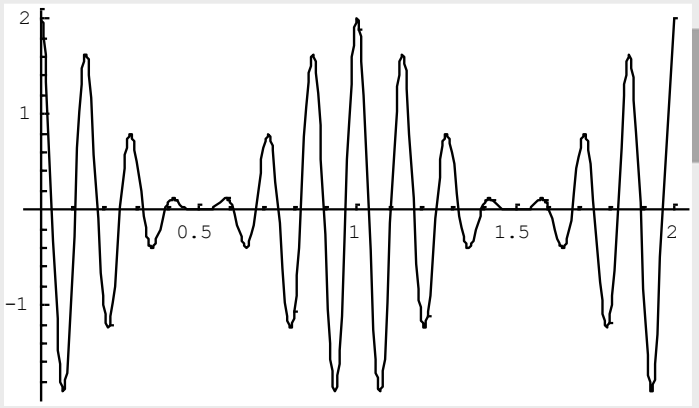
Modulating signal



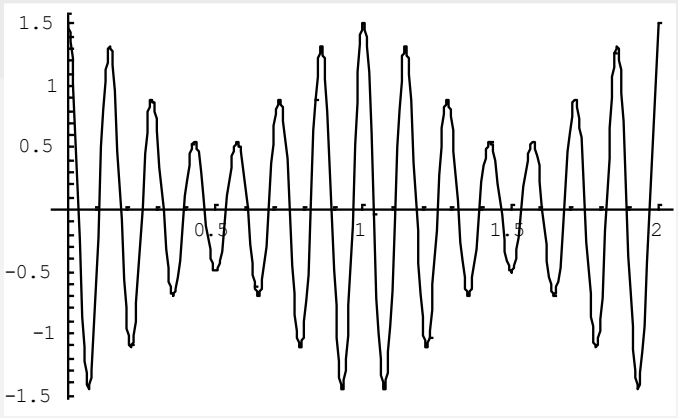
Carrier



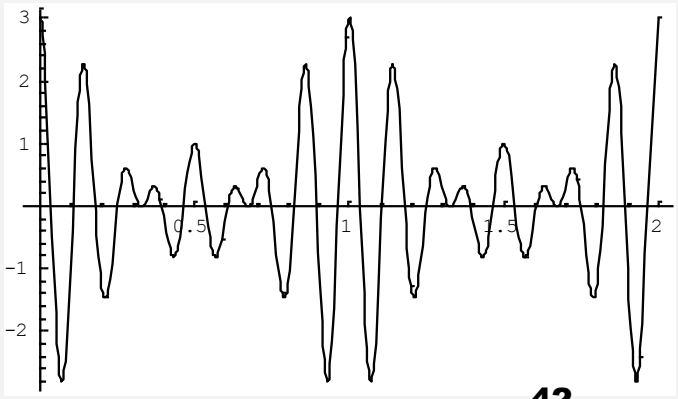
$n_A = 1$



$n_A = 0.5$



$n_A = 2$

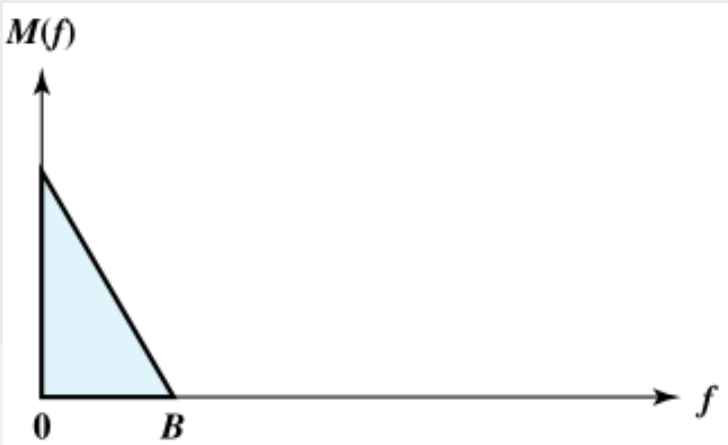


Spectrum of an AM signal

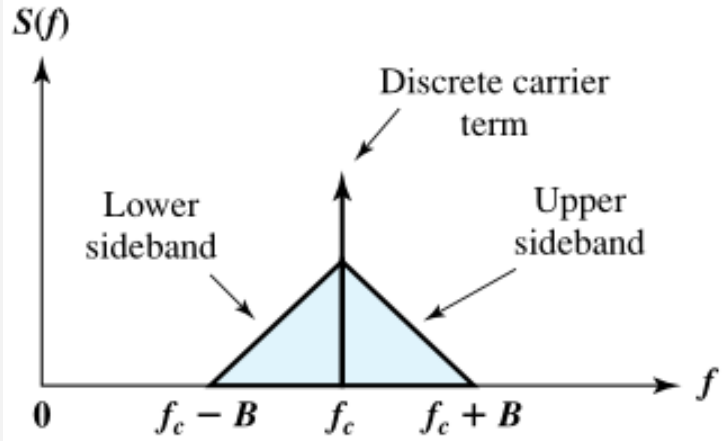
Consider the spectrum of the modulating signal as in the following figure

From the relation that defines the AM signal we get the spectrum of s

$$s(t) = \cos 2\pi f_c t + \frac{n_a}{2}\cos 2\pi (f_c - f_m)t + \frac{n_a}{2}\cos 2\pi (f_c + f_m)t$$



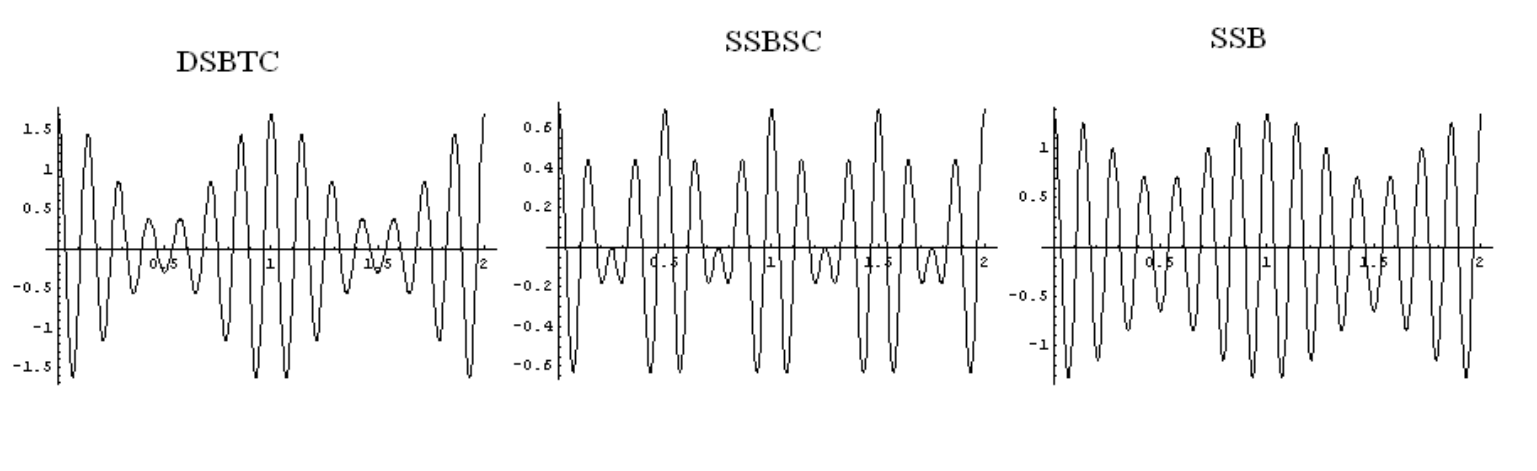
(a) Spectrum of modulating signal

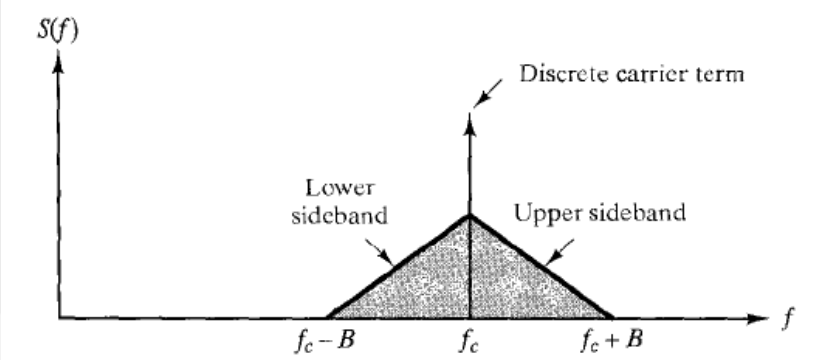


(b) Spectrum of AM signal with carrier at f_c

Cf. [Stallings]

- Note that the lower sideband and the upper sideband are identical, this is called Double Sideband Transmitted Carrier (DSBTC)
- Variant: Single sideband (SSB) send only one of the two sidebands: only half bandwidth is used, less power is required
- Variant: Double-sideband suppressed carrier (DSBSC) send both sidebands, suppress carrier: saves power but not bandwidth





Example: consider a voice signal from 300 to 3000 Hz and an 60 kHz carrier. What is the range of the upper and lower sideband?

FM & PM

Special cases of angle modulation

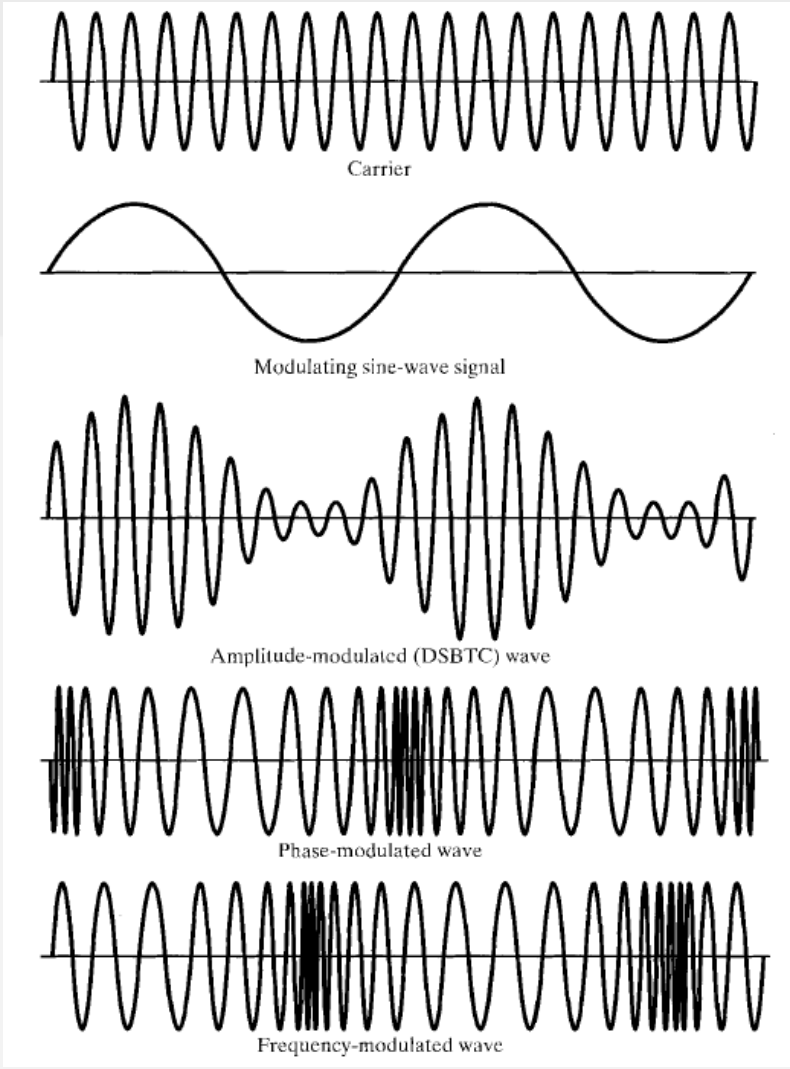
$$s(t) = A_c \cos\left[2\pi f_c t + \phi(t)\right]$$

For frequency modulation

$$\phi(t) = n_f m(t)$$

For phase modulation

$$\phi(t) = n_p m(t)$$



Cf. [Stallings]

Transmission errors: causes

Attenuation – the reduction of the signal strength caused by signal spreading and resistance of the medium

- Resistance increases with length
- Attenuation is more pronounced over wireless networks and increases in proportion to the square of the distance or worse
- **Amplifiers** can be used to boost the energy in the signals for analog transmissions, main deficiency is that they also increase noise
- **Repeaters** can be used to retransmit digital signals

Propagation loss is the ratio between the received and transmitted powers, usually measured in decibels

Transmission errors: causes

Delay Distortion – each sinusoidal component of the signal arrives with a different phase, this difference can make the sum of the sinusoidal components differ from the transmitted signal

- **Equalizers** - are used to restore delay distortion

Noise – added by the channel, equipment etc.

- **Thermal noise** – arise from the agitation of electrons in electronic devices, it exists at all frequencies (also called white noise)
- **Crosstalk** – a signal transmitted over a channel creates effects over the signal from another channel (originally observed in phone conversations when pieces of spech leaks from another conversation)

Probability Theory (theoretical foundation for handling errors)

Universitatea Politehnica Timişoara

An event E is the result of an experiment S

The probability that the event occurs will be denoted as P(E)

Two events can be:

- Independent – not related in any way: $P(E_1 \cap E_2) = P(E_1) \cdot P(E_2)$
- Mutually Exclusive – can not happen at the same time: $P(E_1 \cap E_2) = 0$
- Complementary – if one does not occur the other occurs: $P(E_1) + P(E_2) = 1$

Bit error rate and Frame error rate

- Bit error rate (probability) will be denoted by BER
  - The probability that a bit is in error BER
  - The probability that a bit is intact is $1\text{-}BER$
  - The probability that k bits are in error $BER\text{^}k$
  - The probability that k bits are correct $(1\text{-}BER)\text{^}k$
- A n bit frame has a frame error rate denoted by FER
- Giving BER, FER can be computed as:

$$FER = \sum_{k=1}^{n} C_n^k (BER)^k (1-BER)^{n-k} \qquad FER = 1-(1-BER)^k$$

Exercise: explain the previous two relations

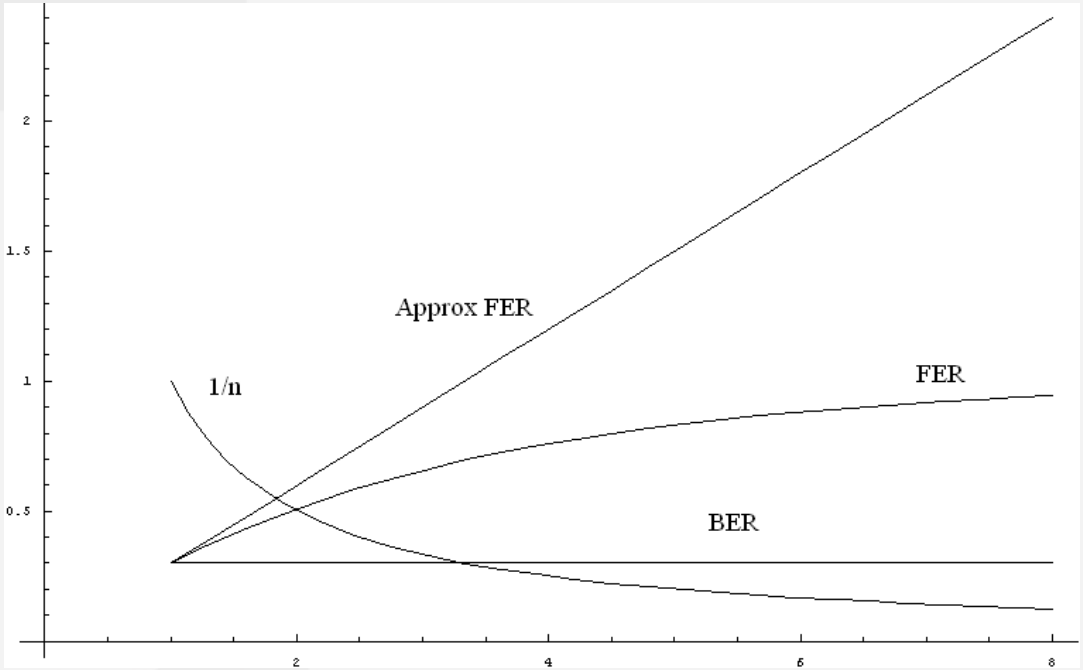
Binomial distributions

- If an experiment has two possible outcomes $E1$ and $E2$ which are complementary events, than the probability that event $E1$ is the outcome k times out of n trials is

$$C_n^k P(E_1)^k \cdot P(E_2)^{n-k}$$

- This is also called binomial distribution
- This also explains previous computation of FER

May be useful to know for very short frames: if $1/n >> k$ then we can approximate FER by $FER \approx n \cdot BER$



Probability of Undetected Error

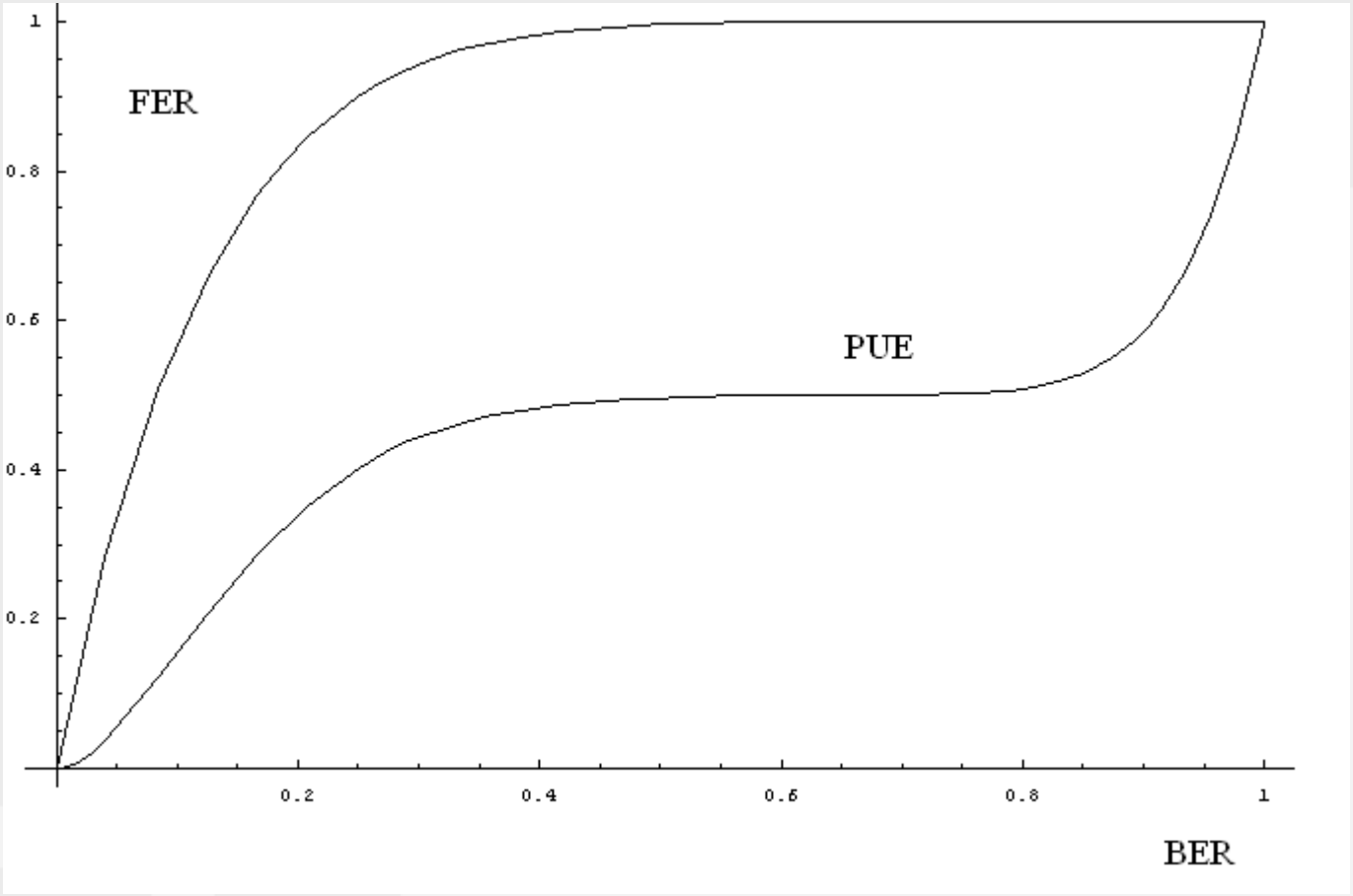
- Let PUE denote the probability of an undetected error
- If there is no error detection mechanism $PUE=FER$

Introducing Parity Bits

- A bit is added to the end of each frame such that the total number of 1's is always even (or odd, actually doesn't matter)
- A receiver checks the number of 1's and if it is not even (odd) it knows there was an error
- Very useful in dome situation, e.g. ASCII characters are 7-bit, 1-bit can be used for parity
- The error goes undetected if an even number of bits are altered, i.e.

$$PUE = \sum_{k=even}^{n} C_n^k \left(BER\right)^k \left(1 - BER\right)^{n-k}$$

- FER and PUE based on BER for 8 bits



CRC (Cyclic Redundancy Check)

- Can detect some accidental alteration
- Particularly good at detecting errors caused by noise
- Easy to understand and implement on hardware
- Cannot detect intentionally alteration (in contrast to hash functions and message authentication codes)
- Cannot prove authenticity or integrity
- Most of them used 32 bits
- Unlikely to ever use more than 128 bits as cryptographic hash functions are a stronger alternative at such bit-lenght

CRC - Main principle

Consider bits inside a frame binary as coefficients of a polynomial, e.g. $01001001 \Leftrightarrow x^6 + x^3 + 1$

- All algebraic operations (+,-,x,/) are done modulo 2 (binary addition without carry)
- Chose some polynomial P (usually named pattern) to test if received message are divisible with P
- Transform each sent message into a message that is divisible by P
- If any received message is not divisible by P then it has an error, otherwise it is correct with a high probability

Computing the CRC of a message

Let $T=M||CRC$, M – message, CRC – check code, be the transmitted frame, i.e.

$$|M| = k$$

$$|CRC| = n$$

$$|T| = n + k$$

$$T = 2^k M + CRC$$

By dividing the message shifted with n bits to the left we get

$$2^n M = PQ + R$$

This also means that: $P \mid 2^n M + R$

Therefore CRC value can be R

And the transmitted frame is: $T = M \,||\, CRC$

Example CRC calculation

Compute the CRC for the message that consists of the following sequence of bits **110101**, considering the CRC polynomial to be **101 (x^2+1)**

Solution:

- The CRC size in this case is n=2.
- The message is first left shifted by 2, then the result is divided by the polynomial to get the remainder (CRC)

Exercise:

The obtained CRC is concatenated to the message. Verify the message consistency via CRC

11010100 / 101 = 111011

101
111
101
100
101
110
101
110
101
11 = CRC

Parity bit revisited

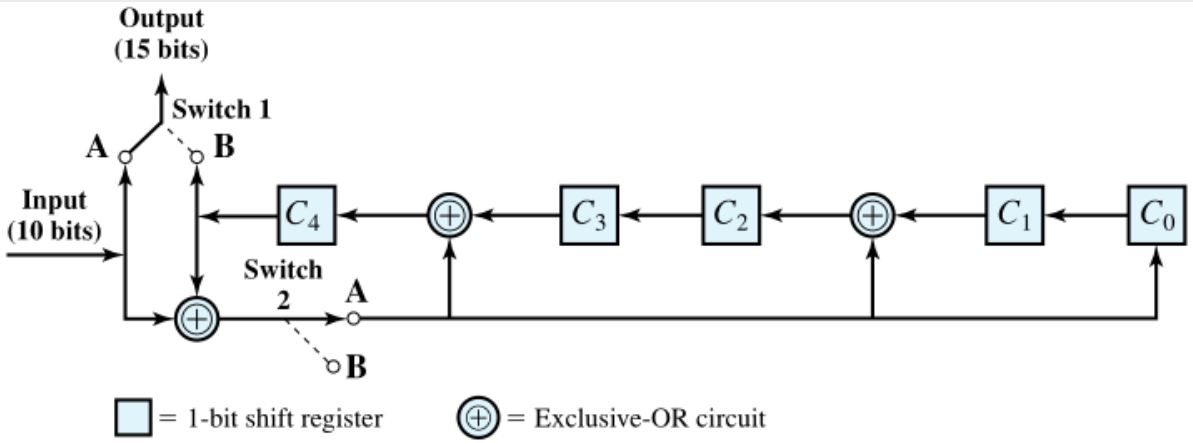
Exercise.

The polynomial x+1 is also known as CRC-1 and is in fact the parity bit. Prove it !

For other frequently used polynomials see
http://en.wikipedia.org/wiki/Cyclic_redundancy_check

Hardware Implementations

A big advantage of CRC is that it can be easily implemented on hardware



(a) Shift-register implementation

	C_4	C_3	C_2	C_1	C_0	$C_4 \oplus C_3 \oplus I$	$C_4 \oplus C_1 \oplus I$	$C_4 \oplus I$	I = input	
Initial	0	0	0	0	0	1	1	1	1	
Step 1	1	0	1	0	1	1	1	1	0	
Step 2	1	1	1	1	1	1	1	0	1	
Step 3	1	1	1	1	0	0	0	1	0	
Step 4	0	1	0	0	1	1	0	0	0	Message to be sent
Step 5	1	0	0	1	0	1	0	1	0	
Step 6	1	0	0	0	1	0	0	0	1	
Step 7	0	0	0	1	0	1	0	1	1	
Step 8	1	0	0	0	1	1	1	1	0	
Step 9	1	0	1	1	1	0	1	0	1	
Step 10	0	1	1	1	0					

(b) Example with input of 1010001101

[Stallings, pp. 195]

Power of CRC codes

Universitatea Politehnica Timişoara

Several requirements are usually imposed for CRC codes:

- All single bit errors can be detected
- All double errors can be detected if the CRC polynomial has at least 3 terms
- Any odd number of errors can be detected if the CRC polynomial contains a factor (x+1)
- Any burst error can be detected if the length of the burst is less than the remainder (burst means consecutive bits are affected)
- Most of the larger burst errors can be detected
- A large number of error patterns can be detected, depending on the CRC polynomial

Error recovery

Two main practices:

- On channels with high reliability (e.g. optical fiber), it is more convenient to detect errors and request retransmission of faulty messages (**error detection codes**, e.g. CRC)
- On unreliable channels (e.g. wireless) retransmission is not so efficient (as the channel itself is faulty) and it is better to add redundant bits such that the receiver can figure out what bits were affected (**error correcting codes**, e.g. Hamming Codes)