Communication in Electronic Systems

Lecture 11: Coding and Digital Modulation

Lecturer: Petar Popovski

TA: Junya Shiraishi, João H. Inacio de Souza

email: petarp@.es.aau.dk

AALBORG UNIVERSITY
DENMARK

Connectivity

Course Overview: Part 2. Communication and Networking

- MM5: Introduction to Communication Systems
- MM6: Simple Multiuser Systems and Layered System Design
- MM7: Network Topology and Architecture
- MM8: Networking and Transport Layers
- MM9: Introduction to Security
- Guest lecture
- **MM11: Coding and Digital Modulation**
- MM12: Communication Waveforms
- MM13: Workshop on Modulation and Link Operation

outline

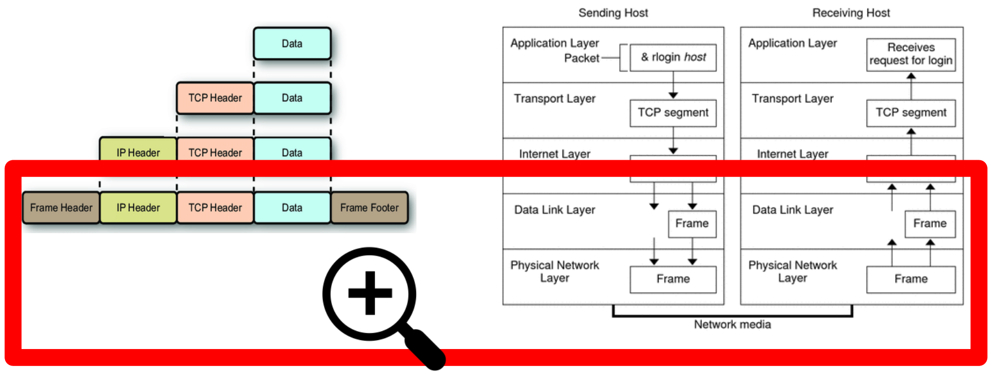
- coding for reliable communication
- digital modulation
  - amplitude-shift keying (ASK)
  - phase-shift keying (PSK)
  - frequency-shift keying (FSK)
  - quadrature amplitude modulation (QAM)
- elements of modulation and detection theory

today

- focus on the data-link and physical layer communication

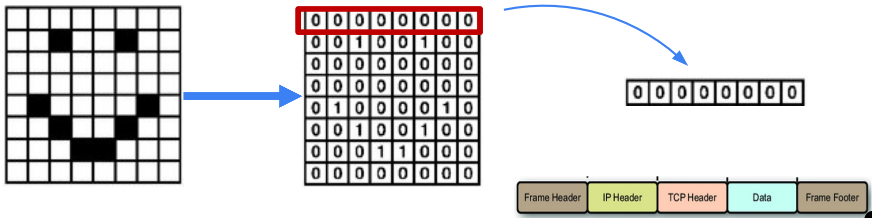
we abstract this away, and

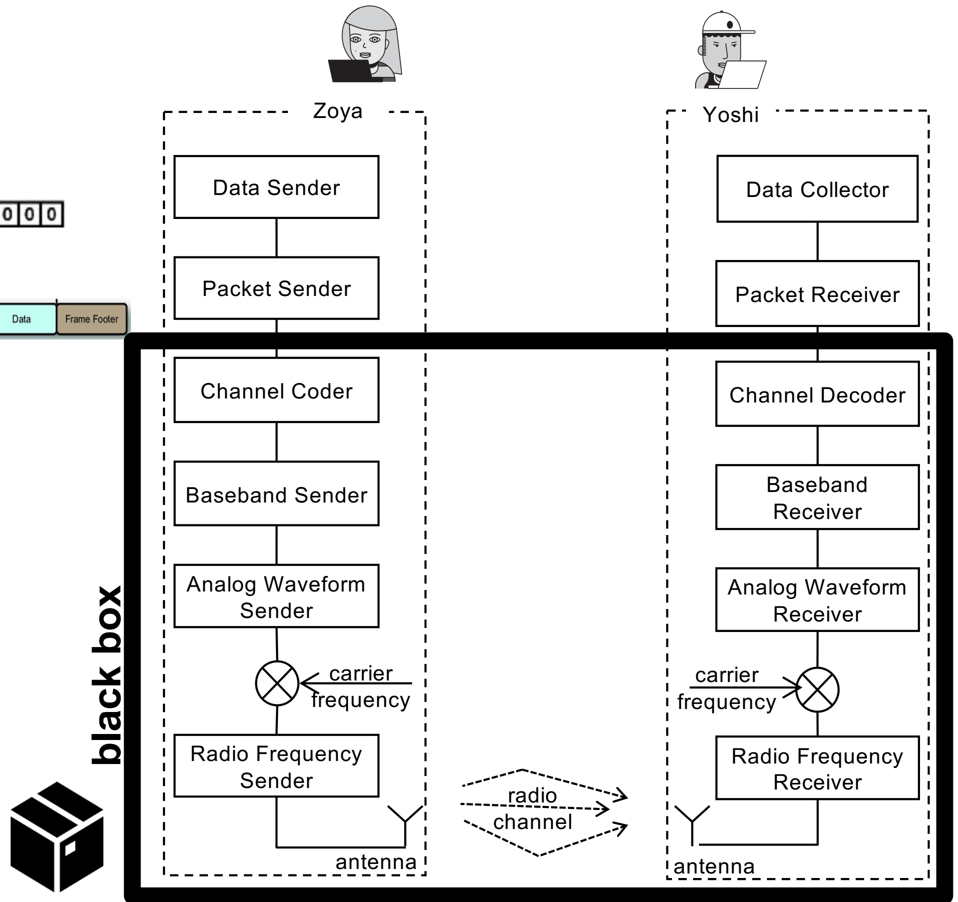
consider it as our packet



- better define the strategies to provide a reliable communication
  - we have seen a bit of error detection and error correction in the first lecture
  - our goal is to recap and go a little bit further

reliable communication



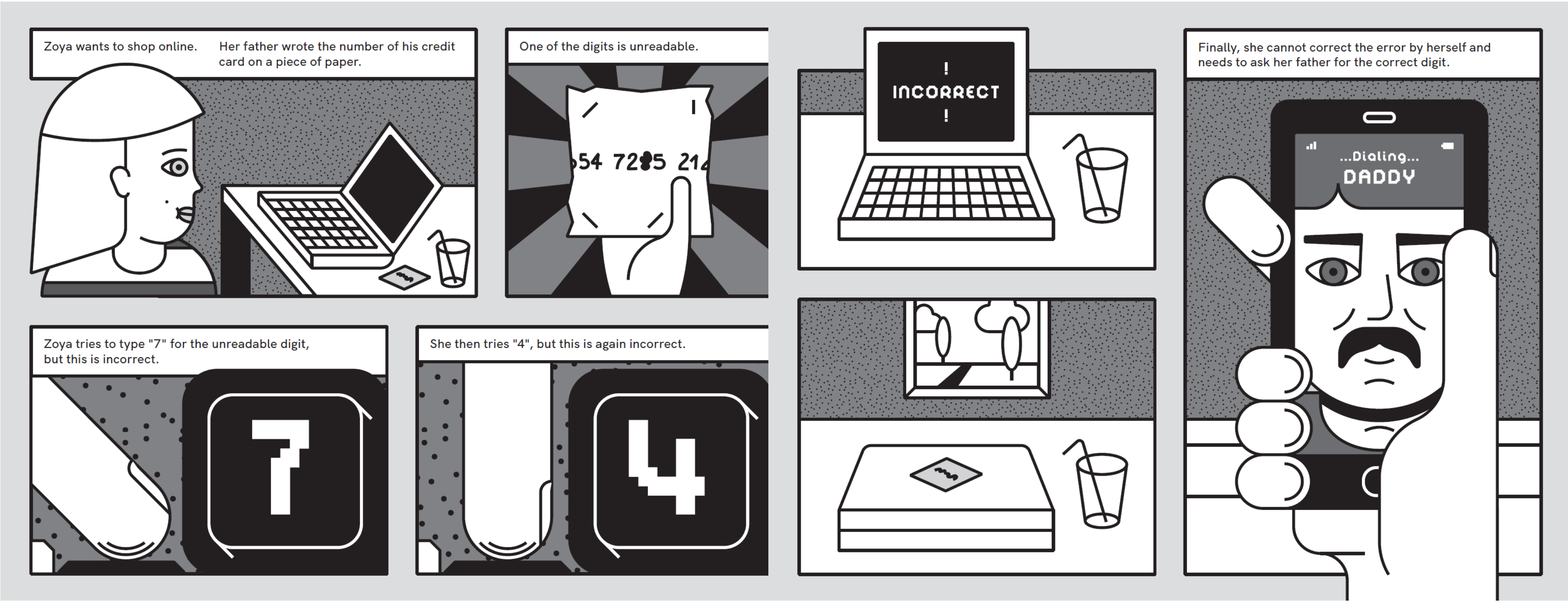


main question for today:

how do we guarantee a

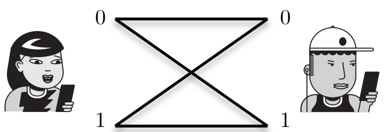
reliable communication?

coding for reliable communication

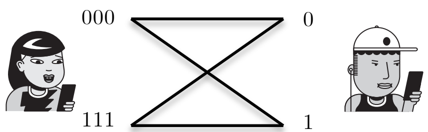

Zoya wants to shop online.
Her father wrote the number of his credit card on a piece of paper.
One of the digits is unreadable.
!
INCORRECT
!
Finally, she cannot correct the error by herself and needs to ask her father for the correct digit.
...Dialing...
DADDY
Zoya tries to type "7" for the unreadable digit, but this is incorrect.
7
She then tries "4", but this is again incorrect.
4

communication over unreliable channels

- binary symmetric channel (BSC): an unreliable bit pipe
- simple idea: repeat each bit three times and do a majority voting
  - sender: send 000 for data bit 0 and 111 for data bit 1
  - receiver: decide 0 if receiving 000, 001, 010, 100



BSC



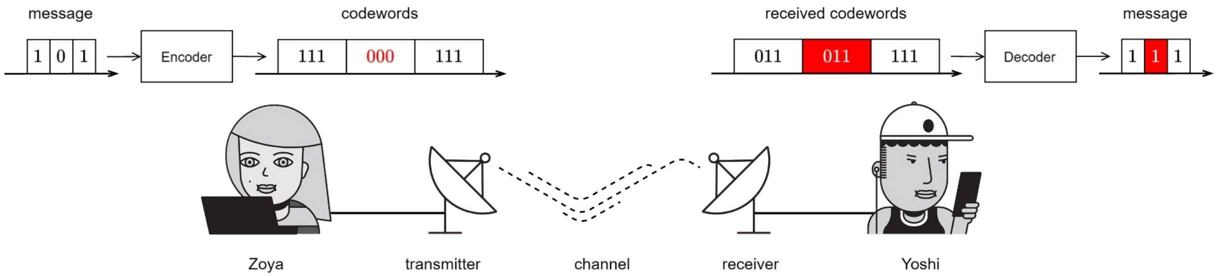
repetition code

- tradeoff
  - the probability of error is decreased
  - but the goodput is decreased to 1/3 since the channel is used to send redundancy bits

definition of a code rate

- we use the binary channel n times to send $b < n$ bits
- the code rate is then $R = \frac{b}{n}$ [bits/channel use]
- number of redundant bits is $n - b$
- both error detection and error correction require redundancy
- in general, we can send M possible messages by using the channel n times
  - here $M < 2^n$
  - code rate $R = \frac{\log_2 M}{n}$

repetition code and majority voting (1)

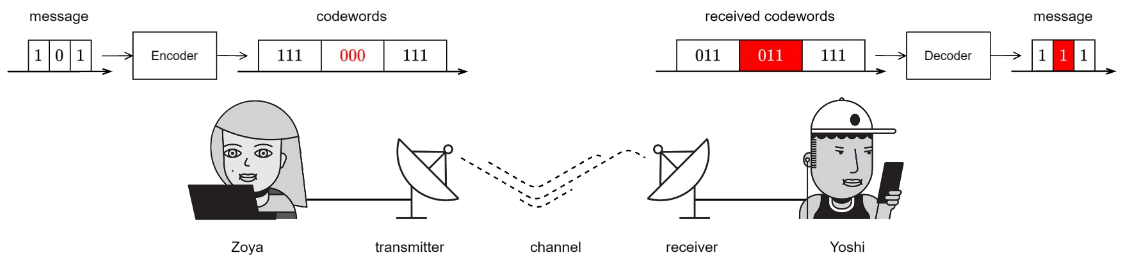


- encoder
  - bit 0 → codeword 000
  - bit 1 → codeword 111
- decoder
  - majority voting
  - most frequent bit in the received codeword
  - lookup table
- bit error rate analysis
  - BER uncoded communication (BSC): p_U
  - tx codeword: 111
  - prob. rx 000: p_U^3
  - prob. rx 001: $p_U^2(1-p_U)$
  - prob. rx 010: $p_U^2(1-p_U)$
  - prob. rx 100: $p_U^2(1-p_U)$
  - BER coded communication: $p_C = 3p_U^2(1-p_U) + p_U^3 < p_U$

Received codeword	Decoded bit
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

repetition code and majority voting (2)

- throughput analysis
  - b information bits + c check bits
- uncoded communication
  - $T_U = \frac{b}{b+c}(1-p_U)^{b+c}$
- coded communication
  - $T_C = \frac{b}{3(b+c)}(1-p_C)^{b+c}$
  - $T_C = T_U \frac{1}{3}\left(\frac{1-p_C}{1-p_U}\right)^{b+c}$
- throughput degrades significantly when the BSC BER is low

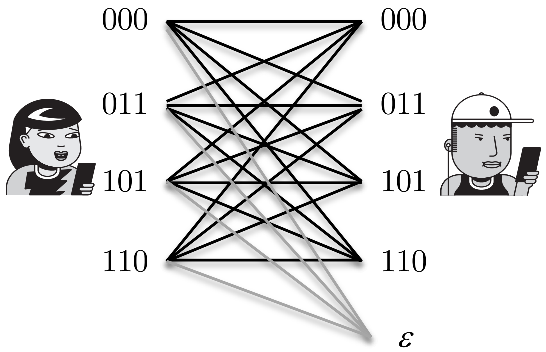


BSC BER (p_U)	Number of bits ($b+c$)	Throughput
0.495	100	$T_C = 0.549T_U$
0.495	200	$T_C = 0.895T_U$
0.495	300	$T_C = 1.47T_U$
10^{-6}	100	$T_C = 0.333T_U$

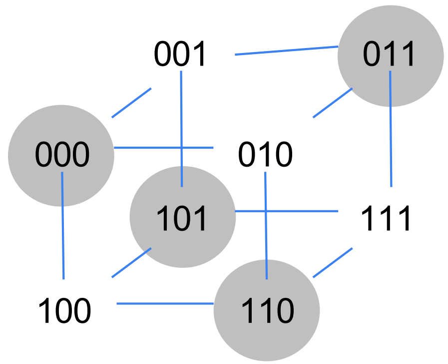
forward error correction (FEC): a simple code

- block code: b bits supplied as a **message** $\mathbf{d} = (d_1, \dots, d_b)$
- each **message** is associated a **codeword** $\mathbf{x} = (x_1, \dots, x_n)$
- $n > b$ and both d_i and x_j assumed binary
- we call this an $(\boldsymbol{n}, \boldsymbol{b})$**-code** with rate $R = \frac{b}{n}$ [bit/c.u.] and corresponds to *c*-channel with 2^b inputs and 2^n outputs
- Hamming distance of 2

message $\mathbf{d}$	codeword $\mathbf{x}$
00	000
01	011
10	101
11	110



(d)



FEC: linear block code

the code provided as example belongs to the class of *linear block codes*, where linearity is wrt. addition and multiplication of binary numbers, i.e., within the *GF*(2)

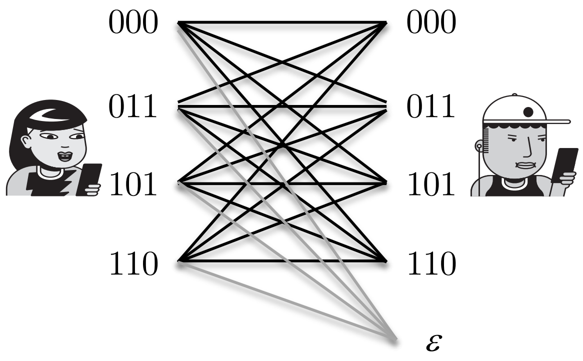
encoding has particularly simple interpretation

$$\mathbf{x} = \mathbf{d} \cdot \mathbf{G}$$

where $\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ is the Generator matrix

the additional bits are called **parity bits**

- in a good code **one bit** should influence **several symbols**, and **one symbol** should be influenced by **several bits**



(d)

message $\mathbf{d}$	codeword $\mathbf{x}$
00	000
01	011
10	101
11	110

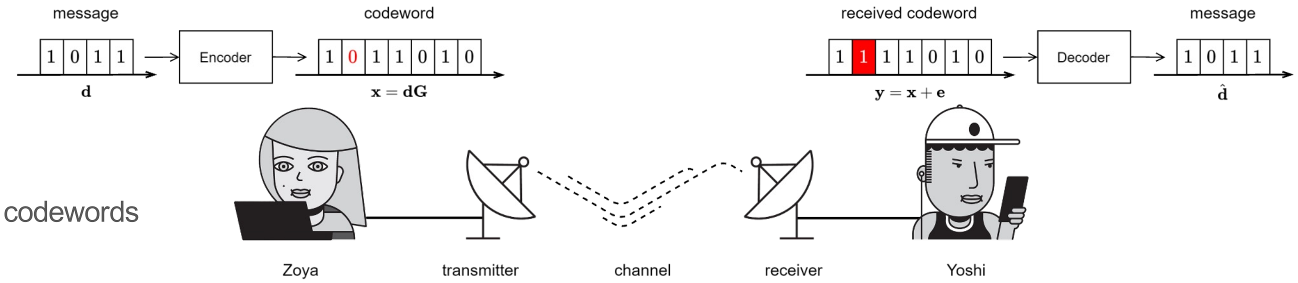
Hamming code (1)

- linear block code
- detect 1- and 2-bit errors
- correct 1-bit errors

- (l, b) code
  - b-bits blocks mapped into l-bits codewords
  - code rate: $R = \frac{b}{l}$ bit/c. u.

- encoder
  - $d \in \{0,1\}^{1\times b}$: message
  - $x \in \{0,1\}^{1\times l}$: codeword
  - tx codeword: $\boldsymbol{x} = \boldsymbol{dG}$ (binary addition!)
- receiver
  - rx codeword: $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$
  - syndrome vector: $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^T$
  - $s = 0 \Rightarrow$ no error in the received codeword
  - $s \neq 0 \Rightarrow$ error in the received codeword

- $(7,4)$ Hamming code
  - higher rate than the repetition code $\left(\frac{4}{7} > \frac{1}{3}\right)$

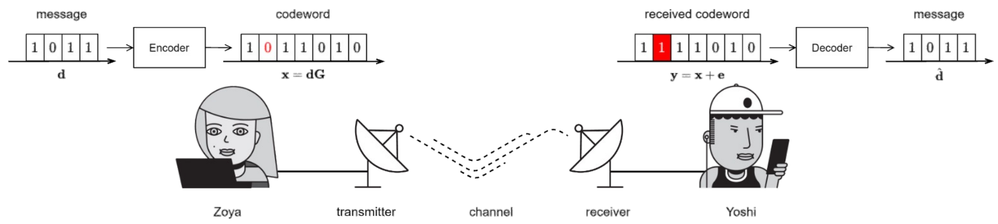


generator and parity-check matrices:

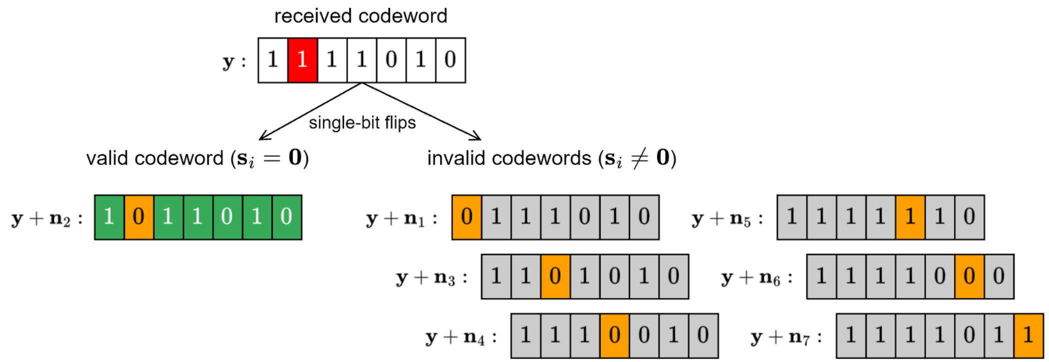
$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad \boldsymbol{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Hamming code (2)

- syndrome decoding
  - compute syndrome vector for each bit flip
  - $\boldsymbol{s}_i = (\boldsymbol{y} + \boldsymbol{n}_i)\boldsymbol{H}^T$
  - the message is the valid codeword
  - no valid codeword ⇒ 2-bit error detected
  - the message is in the 4 initial bits of the corrected codeword



- codewords
  - in the Hamming code the minimum distance between valid codewords is always 3
  - this is why we can detect up to 2-bit errors and correct 1-bit errors



- other Hamming codes
  - m parity bits, with $m \geq 3$
  - we can create $(m, 2^m - 1)$ codes
  - if we choose a large m, the code rate approaches 1
  - rate improves with large m, but we cannot correct more erroneous bits

error detection: Cyclic Redundancy Check (CRC)

- cyclic redundancy check (CRC) is an error detection technique to detect changes to raw data and is used widely in today's computer networks.
- recall the credit card number error

Dataword	Codeword	Dataword	Codeword
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

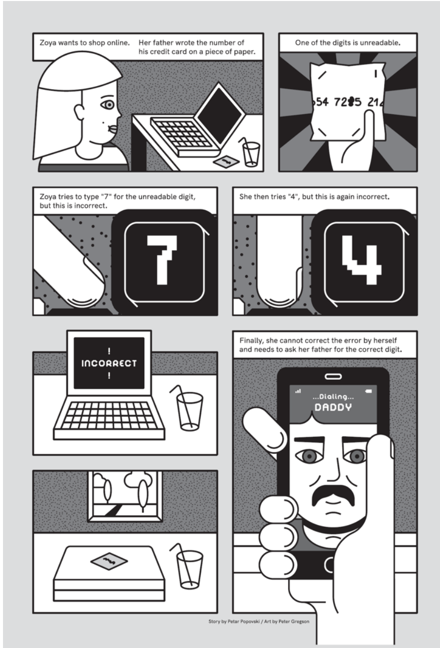
A CRC code with C(7,4)

retransmission in addition to coding

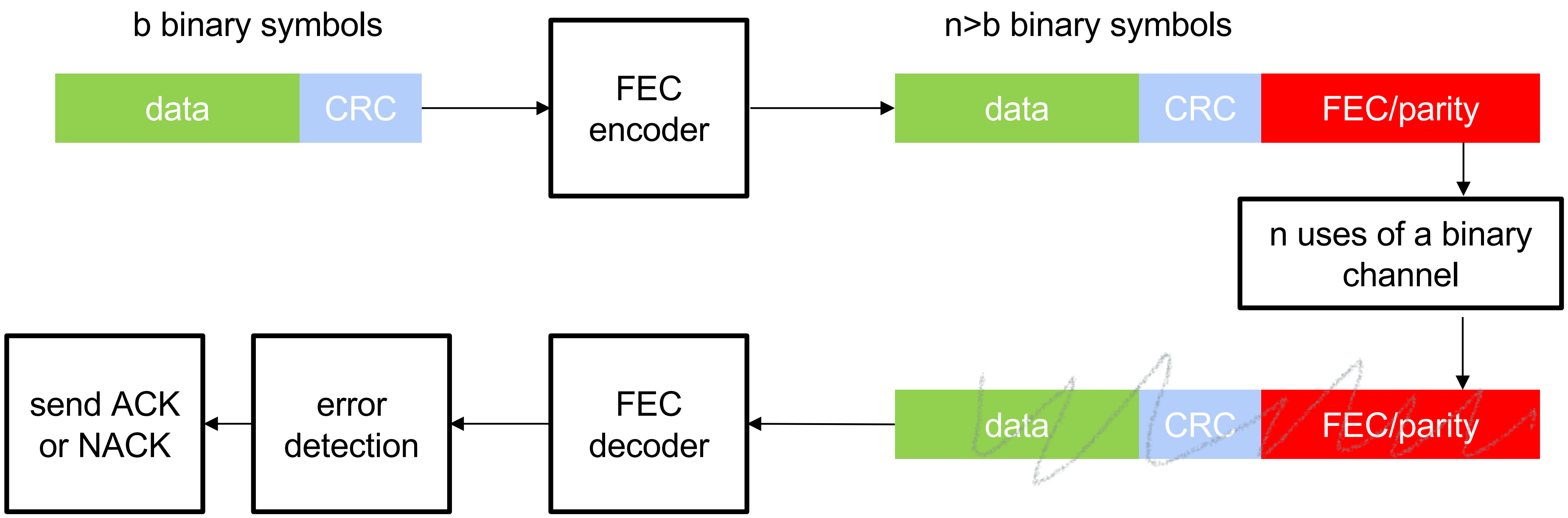
- what if FEC fails?

- decoded packet $\mathbf{d}_2 = \mathbf{d}_1 \oplus \mathbf{e}$
  - accidentally $\mathbf{d}_2$ satisfies the CRC
  - a simple 1-bit ACK does not help; Base station would have to send whole $\mathbf{d}_2$ back as very rich ACK

- what if the error process produces $\mathbf{e}$ again?
  - received ACK is $\mathbf{d}_2 \oplus \mathbf{e} = \mathbf{d}_1 \oplus \mathbf{e} \oplus \mathbf{e} = \mathbf{d}_1$ satisfying error check
- **impossible perfectly reliable** transmission within **limited time**

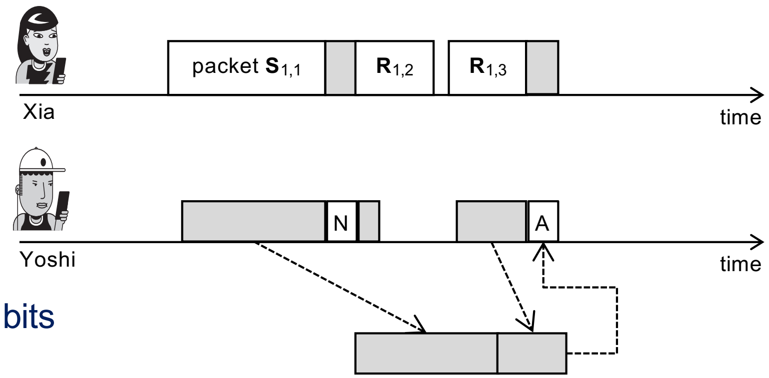


generalize ARQ to hybrid ARQ



- **incremental redundancy:** send additional parity bits instead of the whole thing

partial retransmission & incremental redundancy



- retransmitting **smaller set of symbols**
- how much redundancy is **further** required?
  - challenging how to signal this back
- simpler: retransmit data (systematic) bits
  - Yoshi may use the new ones, or use MRC on the retransmitted bits
  - however, Xia needs to signal which bits were retransmitted
- more practical: using linear codes and puncturing
  - $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ sending one fragment at a time in case no ACK
  - Could be coupled with adaptation of power

digital modulation

digital modulation

an **analog carrier** is modulated by a **discrete signal**

advantages vs. analog modulation:

- higher data rate (bits per second) given a fixed bandwidth
- more robust to channel impairments
  - advanced coding and decoding to combat fading and noise
  - spread spectrum techniques to deal with multipath and to resist interference
- allows for multiple access
  - signals from multiple users in the same bandwidth can be decoded simultaneously
- security and privacy: encryption

going from bits to symbols

three steps

Baseband

1. map bits to complex-valued baseband symbols (2 dimensions)

example: with two complex values, the symbols can be $1-j$ to represent 0 and $1+j$ for 1

The system transmits one symbol each T seconds: symbol period

$$0110101\ldots \longrightarrow X_0, X_1, X_2, \ldots$$

2. assign a pulse waveform (pulse shape) to each symbol

$$X_0, X_1, X_2, \ldots \longrightarrow \sum_k X_k p(t-kT)$$

3. modulate to a high frequency carrier

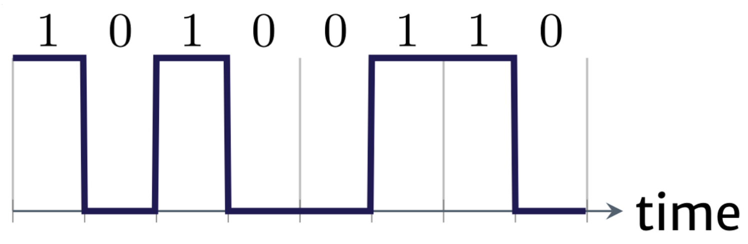
higher data rate?

a complex symbol can carry more than one bit

example:

1 bit per symbol: $0 \rightarrow -A$ and $1 \rightarrow A$

vector $[1,0,1,0,0,1,1,0] \rightarrow [A,-A,A,-A,-A,A,A,-A]$



2 bits per symbol
$$00 \rightarrow A$$
$$01 \rightarrow Aj$$
$$10 \rightarrow -A$$
$$11 \rightarrow -Aj$$

pulse shape examples

sampling function

$$p(t) = \frac{1}{\sqrt{T}} \operatorname{sinc}\left(\frac{\pi t}{T}\right) = \begin{cases} \frac{1}{\sqrt{T}}, & \text{for } t = 0 \\ \frac{1}{\sqrt{T}} \frac{T \sin\left(\frac{\pi t}{T}\right)}{\pi t}, & \text{otherwise} \end{cases}$$

rectangular function

$$p(t) = \begin{cases} \frac{1}{\sqrt{T}}, & \text{for } t \in (0, T] \\ 0, & \text{otherwise} \end{cases}$$

IQ representation of a signal

a bandpass signal can be represented as

$$s(t) = s_I(t)\cos(2\pi f_c t) + js_Q(t)\sin(2\pi f_c t)$$

$$= I(t) + jQ(t)$$

I : in-phase component $s_I(t)$

Q : quadrature component $s_Q(t)$

canonical form of a bandpass signal

the carrier is normally thought as the cosine term, so, the I term is “in-phase” with the carrier

amplitude: $A(t) = \sqrt{s_I^2(t) + s_Q^2(t)}$

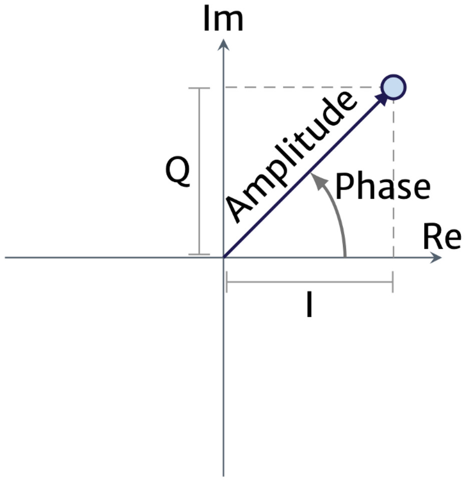
Phase: $\phi(t) = \tan^{-1}\left(\frac{s_Q(t)}{s_I(t)}\right)$

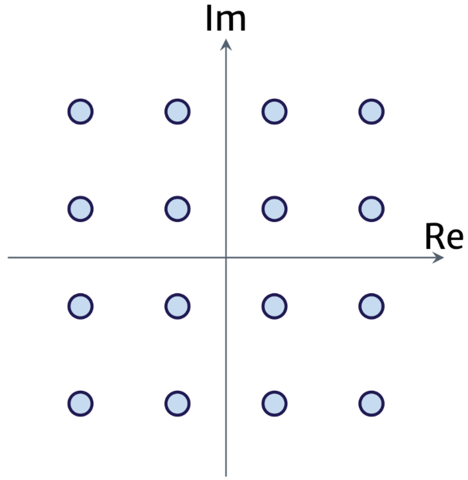
constellation diagram

representation of a digitally modulated signal
uses a collection of points to represent all the different symbols that can be transmitted

the **angle** represents the shift of the carrier wave from a reference phase

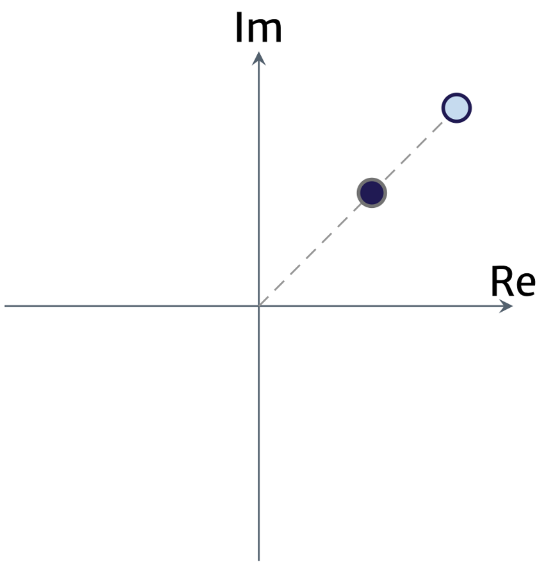
the **distance** of a point from the origin represents the amplitude or power of the signal



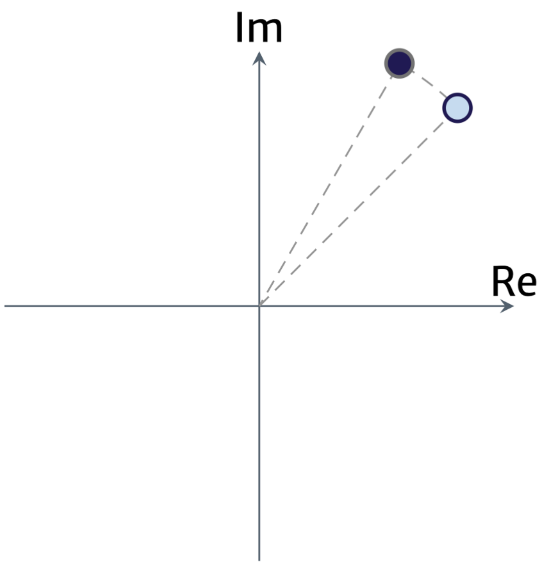


effects of the channel on the symbols

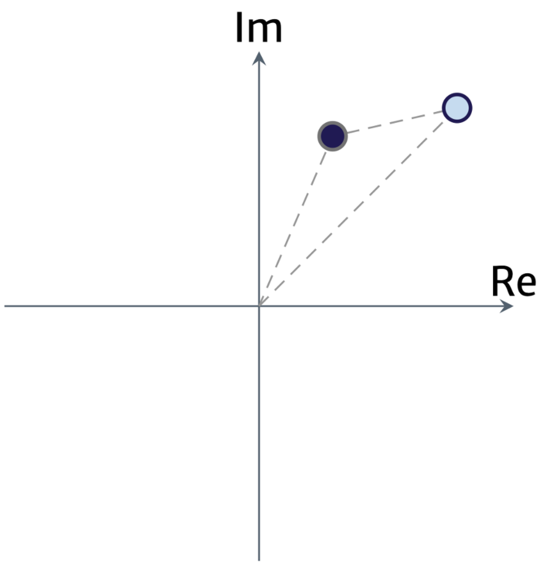
amplitude change



phase change



amplitude and phase change



bit rate and symbol rate

in a constellation with M symbols, each symbol represents $N = \log_2 M$ bits

symbol period: T_{sym}

a new symbol is represented once every T_{sym} seconds by shifting the pulse

symbol rate: $R_{sym} = \dfrac{1}{T_{sym}}$ symbols/second (bauds)

the bit rate is $R_b = NR_{sym} = R_{sym} \log_2 M$ bits per second (bps)

digital modulations

amplitude-shift keying (ASK)

phase-shift keying (PSK)

frequency-shift keying (FSK)

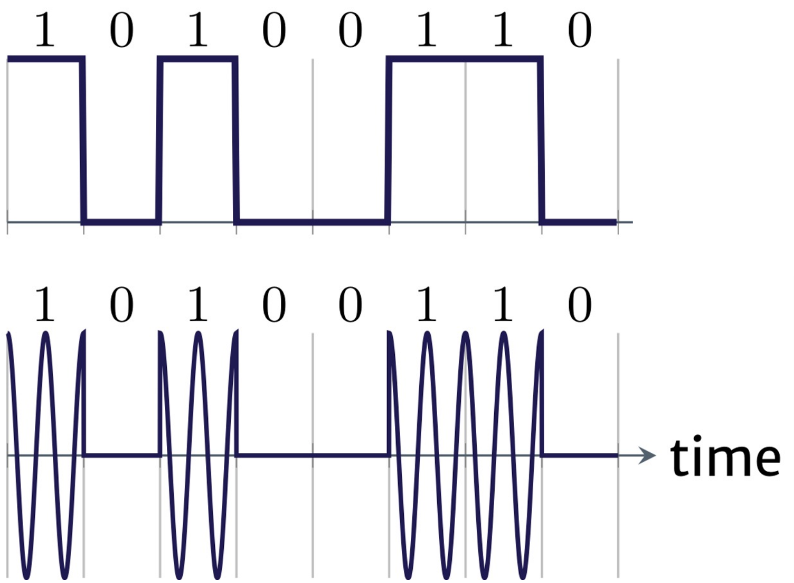
quadrature amplitude modulation (QAM)

amplitude-shift keying (ASK)

bit stream is encoded with the amplitude of the transmitted signal

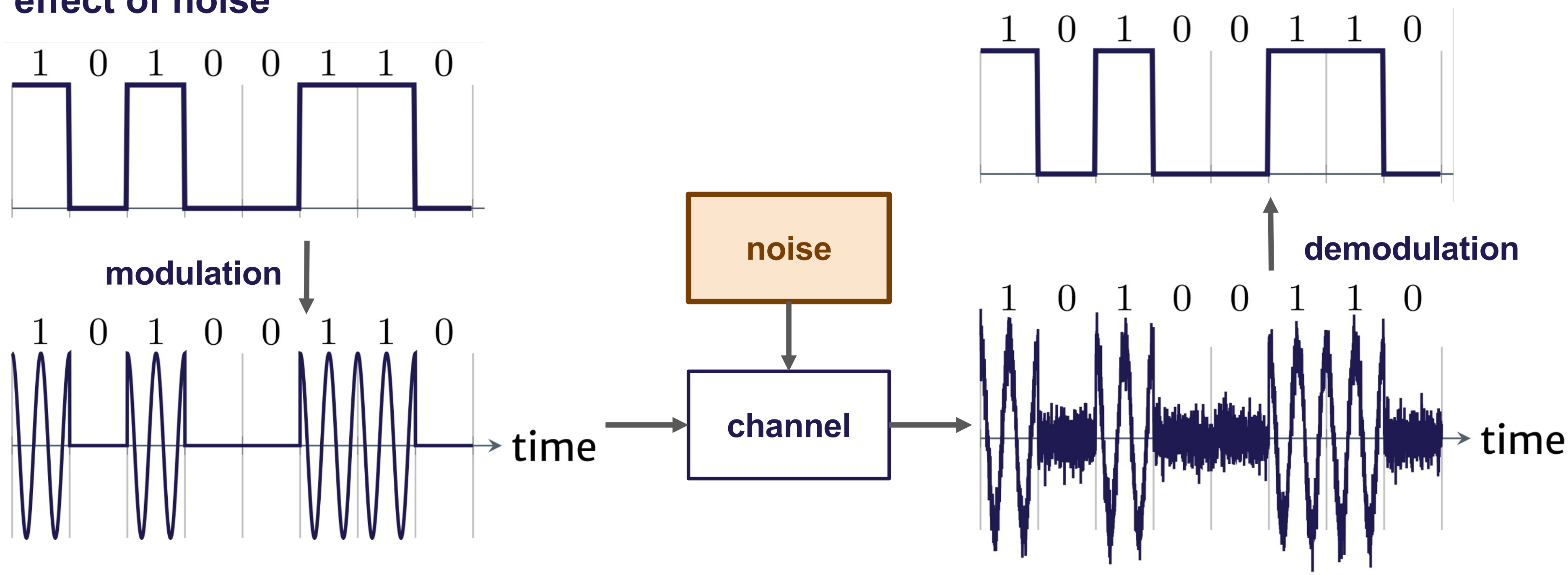
simplest form: on-off keying (OOK)

$$\begin{cases} s_0(t) = 0 \\ s_1(t) = A\cos(2\pi f_c t) \end{cases}$$



on-off keying (OOK)

effect of noise

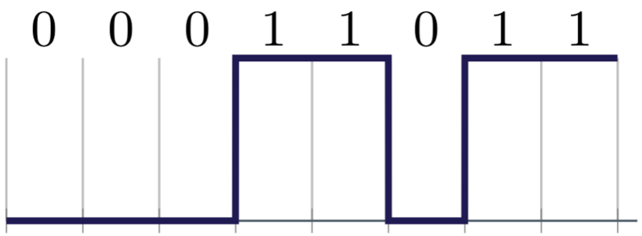


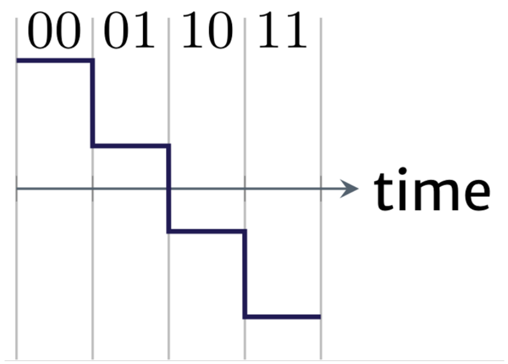
M-ary amplitude-shift keying (M-ASK)

there is an amplitude for each symbol (bit pattern)

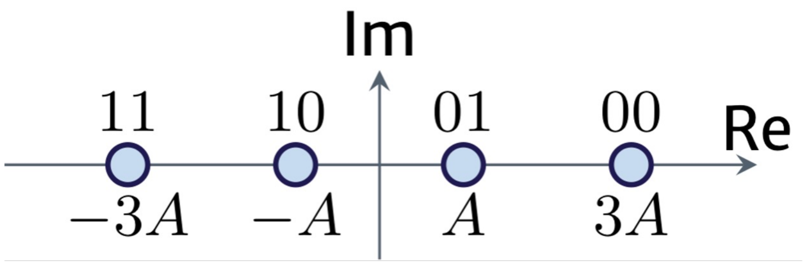
$m \in \{1, 2, \ldots, M\}$

$s_m(t) = A_m \cos(2\pi f_c t) \quad t \in [0, T_{sym})$





example: 4-ASK

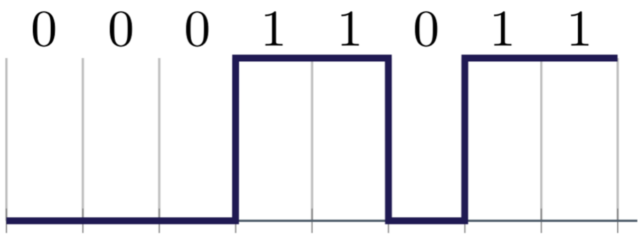


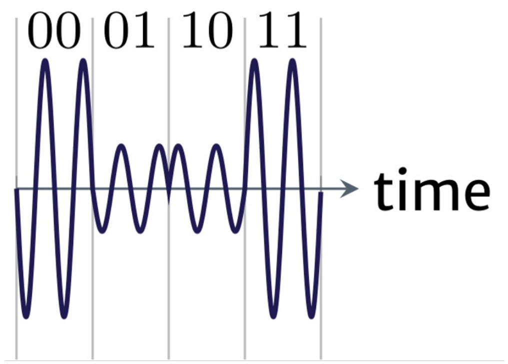
M-ary amplitude-shift keying (M-ASK)

there is an amplitude for each symbol (bit pattern)

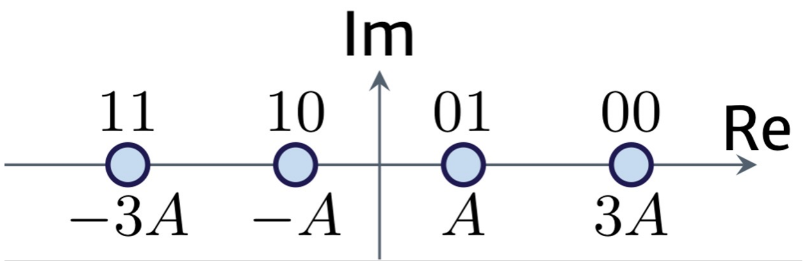
$$m \in \{1, 2, \ldots, M\}$$

$$s_m(t) = A_m \cos(2\pi f_c t) \quad t \in [0, T_{sym})$$





example: 4-ASK



phase-shift keying (PSK)

bit streams are encoded in the phase of the transmitted signal

simplest: Binary Phase-Shift Keying (BPSK)

$$\begin{cases} s_0(t) = A\cos(2\pi f_c t + 0) \\ s_1(t) = A\cos(2\pi f_c t + \pi) \end{cases} \qquad f_c = \frac{n_c}{T_{sym}}$$

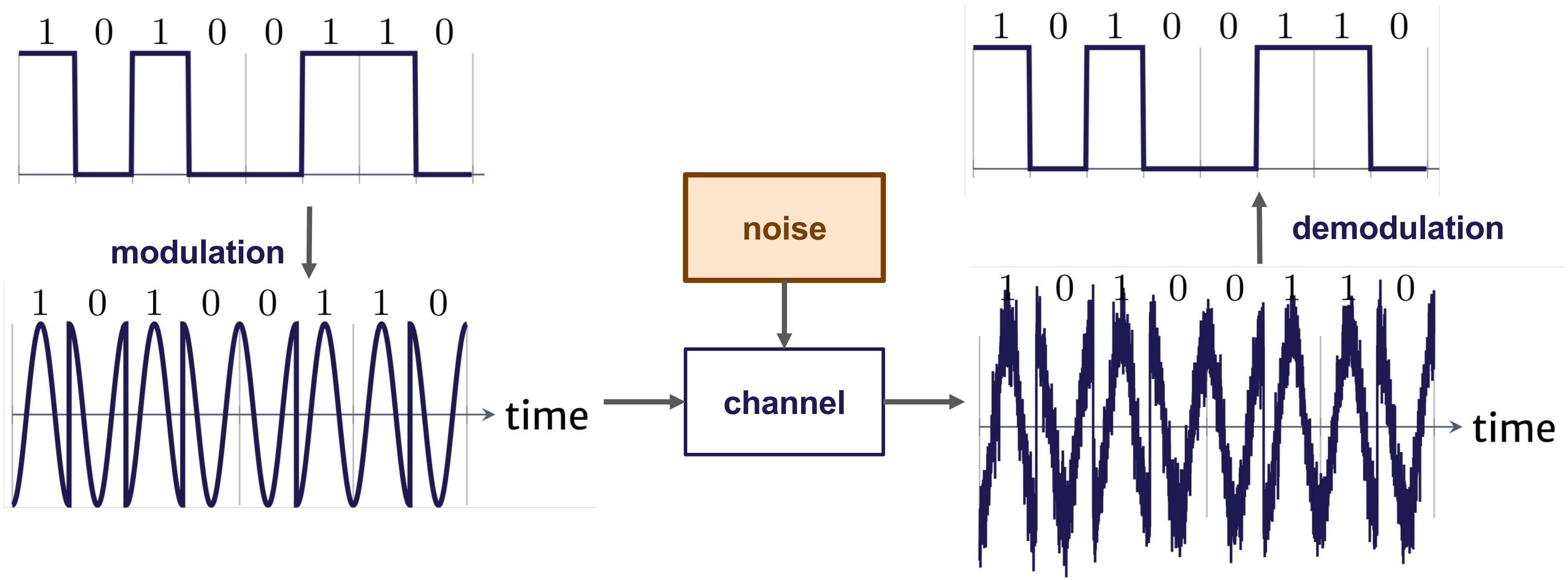
bandwidth $\mathrm{BW} \approx 2R_{sym}\ \mathrm{Hz}$

modulated signal with rectangular pulse: bandwidth approximated by

m-ary Phase-Shift Keying (M-PSK)

$$s_m(t) = A\cos(2\pi f_c t + \theta_m) \qquad \theta_m = \frac{2\pi(m-1)}{M} \qquad m \in \{1, 2, \ldots, M\} \qquad t \in [0, T_{sym})$$

binary phase-shift keying (BPSK)

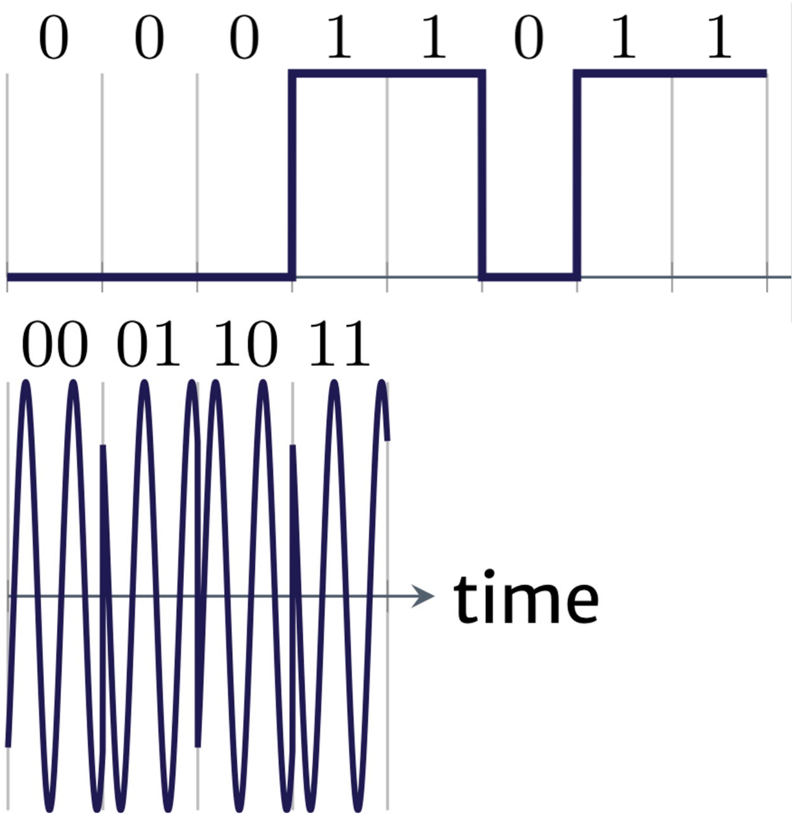


quaternary phase-shift keying (QPSK)

phases

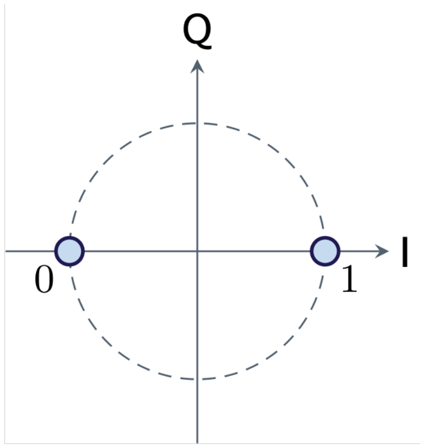
$$\theta_m = \frac{2\pi(m-1)}{M} + \frac{\pi}{4}$$

like 4-PSK but rotated $\frac{\pi}{4}$

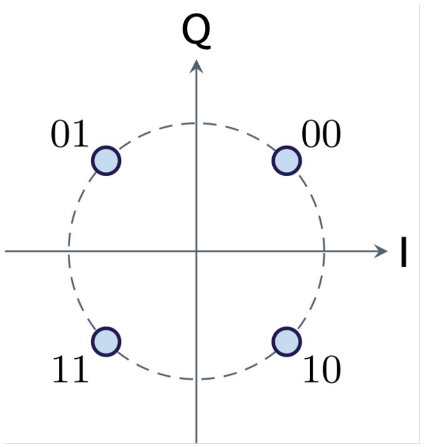


M-PSK

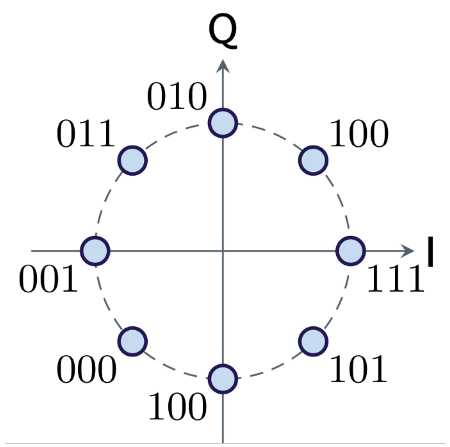
BPSK



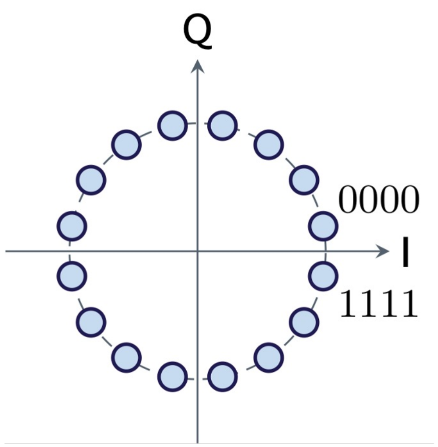
QPSK



8-PSK



16-PSK



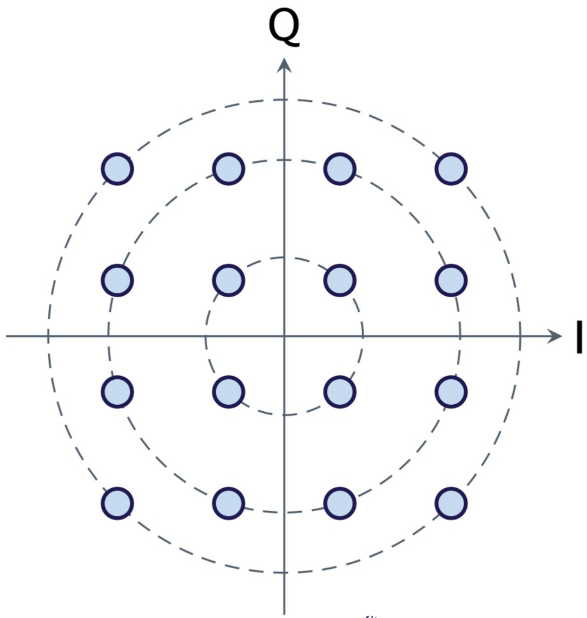
Gray coding

quadrature amplitude modulation (QAM)

QAM has two carriers, each having the same frequency but differing in phase by 90 degrees

the information symbol modulates both the amplitude and phase of the carrier

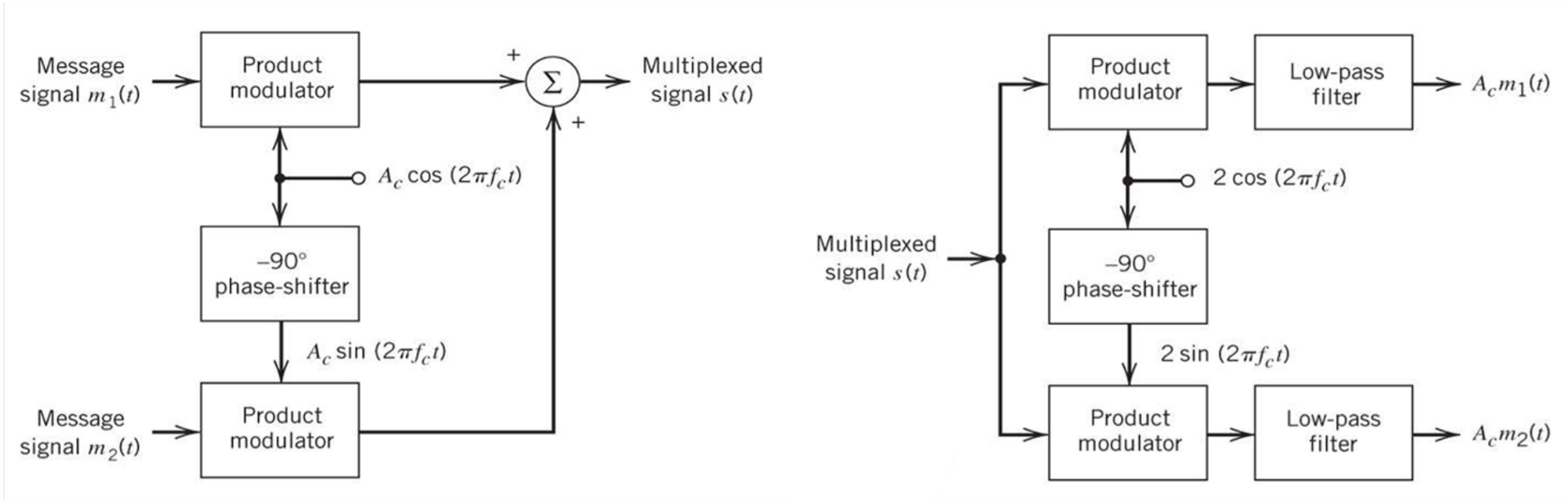
combination of PSK and ASK



receiver:
the two waves can be coherently separated (demodulated) because of their orthogonality property

widely used
- IEEE 802.11
- optical fiber
- cellular systems

QAM modulation and demodulation



frequency-shift keying (FSK)

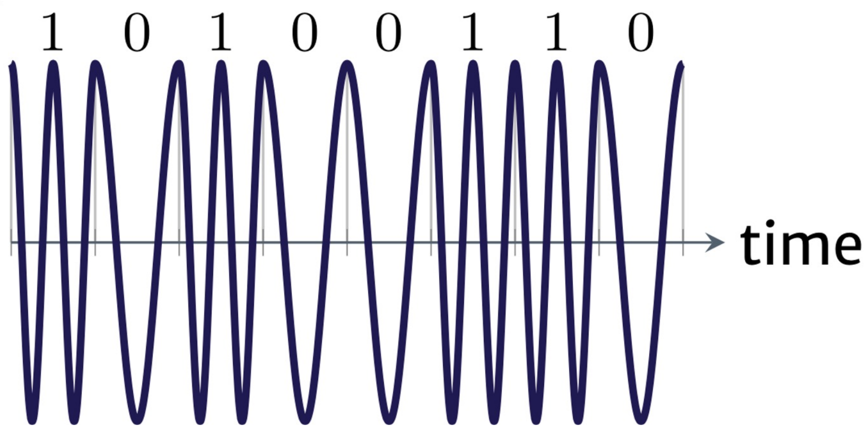
the digital message is carried in the discrete frequency changes of the carrier

simplest: Binary FSK (BFSK)

two frequencies:

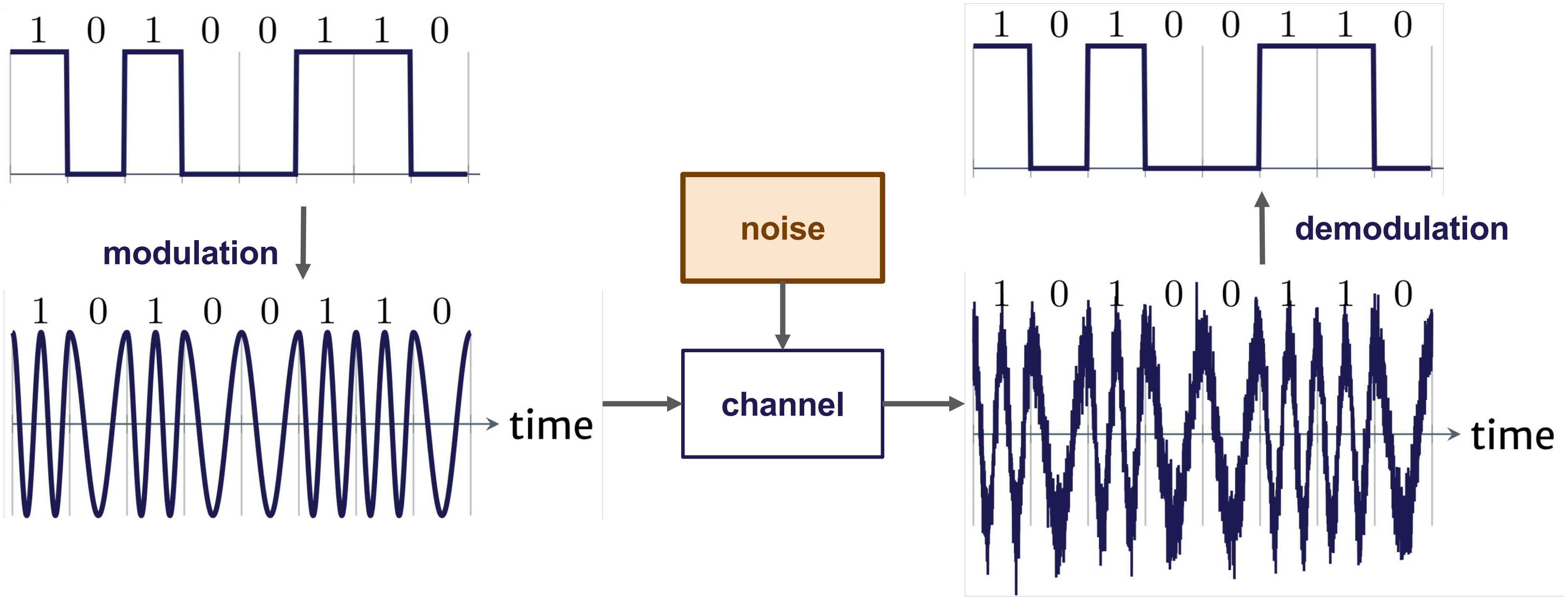
- 1: “mark frequency”
- 0: “space frequency”

$$\begin{cases} s_0(t) = A\cos(2\pi f_{space}\, t) \\ s_1(t) = A\cos(2\pi f_{mark}\, t) \end{cases}$$



Gaussian FSK (GFSK)

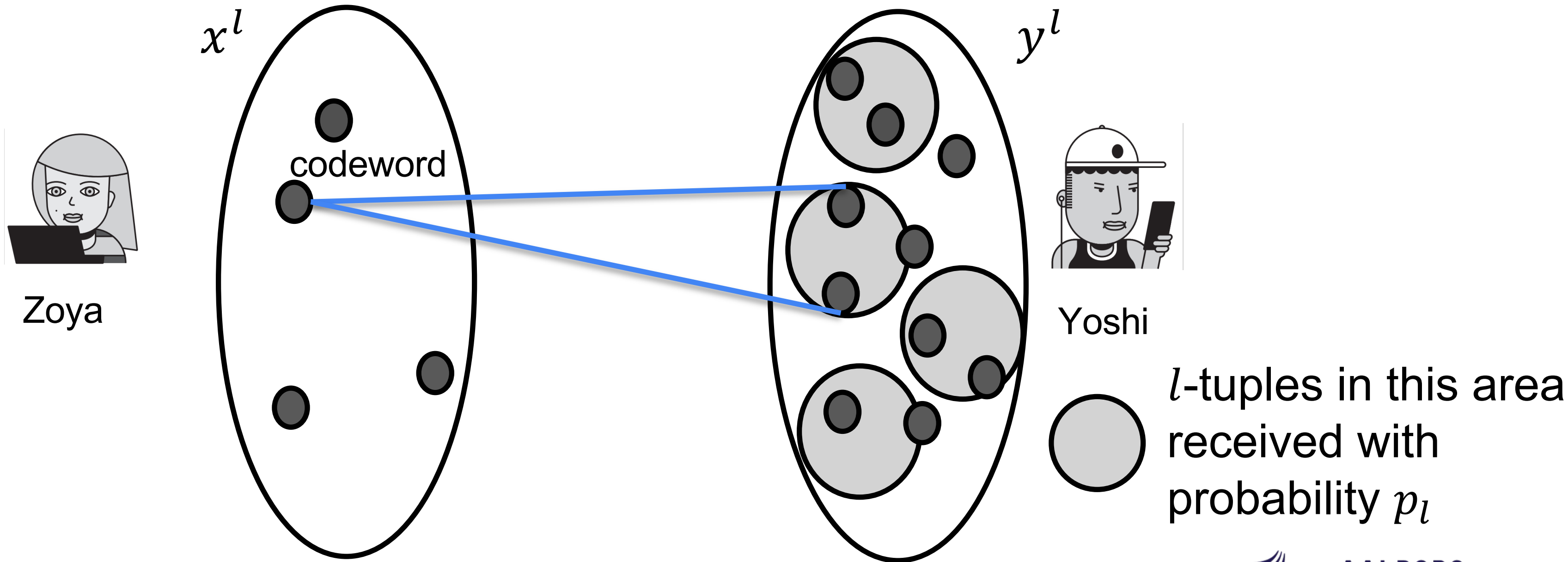
binary frequency-shift keying (BPSK)



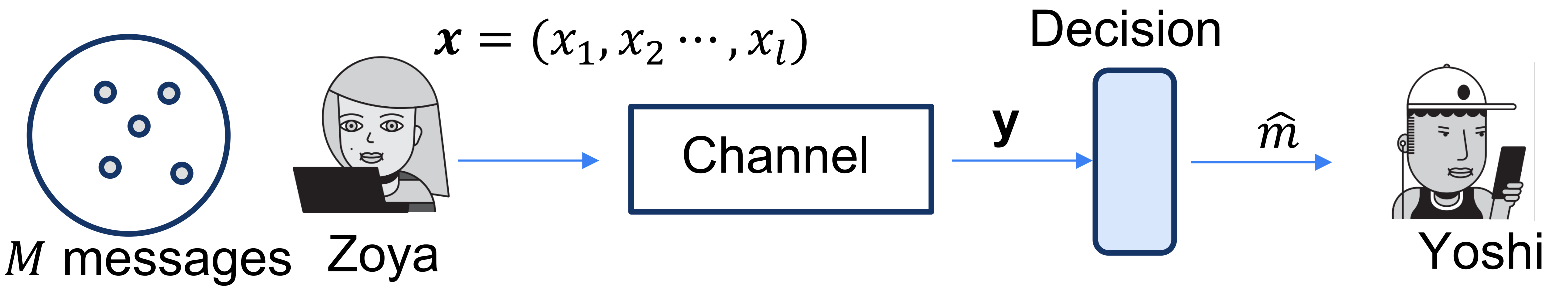
elements of modulation and detection theory

Generalization of coding idea

- How to select as many as possible inputs for the expanded channel
- Guarantee high reliability for the transmission of a single input in the expanded channel.



Maximum likelihood detector



Likelihood

e.g., memoryless channel

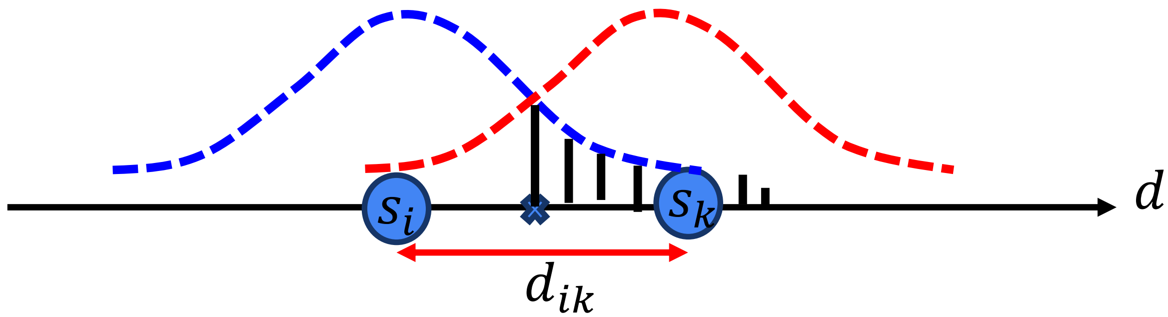
$$\Pr(\boldsymbol{x}_i|\boldsymbol{y}) = \frac{\boxed{\Pr(\boldsymbol{y}|\boldsymbol{x}_i)}\,P(\boldsymbol{x}_i)}{p(\boldsymbol{y})} \qquad \Pr(\boldsymbol{y}|\boldsymbol{x}_i) = \prod_{j=1}^{l} \Pr(y_j|x_{i\ j})$$

Maximum log likelihood: $$\hat{m} = \underset{i\,\in\{1,2,\cdots,M\}}{\operatorname{argmax}} \log \Pr(\boldsymbol{y}|\boldsymbol{x}_i)$$

basics of error probability

$$Q(z) = \int_z^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) dx$$

- $\boldsymbol{y = x + n}$
  - ***x:*** input symbol
  - ***y:* received signal**
  - ***n:*** zero mean Gaussian random variable with variance $\boldsymbol{\sigma^2}$

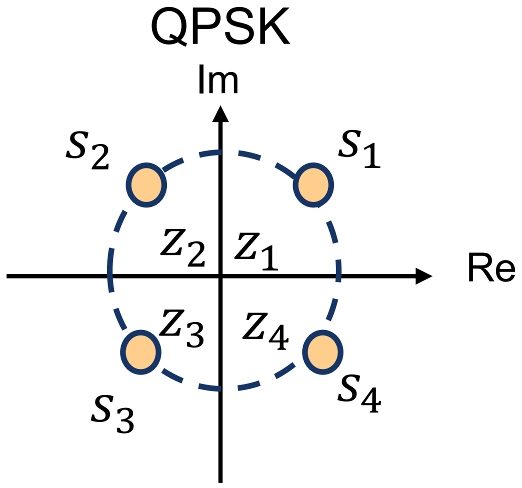


$$\Pr(A_{ik}) = \Pr\left(n > \frac{d_{ik}}{2}\right) = \int_{\frac{d_{ik}}{2}}^{\infty} \frac{1}{\sqrt{\pi N_0}} \exp\left(-\frac{v^2}{N_0}\right) dv = Q\left(\frac{d_{ik}}{\sqrt{2N_0}}\right)$$

decision regions and error probability

- decision region

$$z_i = (x{:}\, \|x - s_i\| < \|x - s_j\|, j = 1, \cdots M, j \neq i)$$



- probability of symbol error

$$P_e = \sum_{i=1}^{M} \Pr(\boldsymbol{x} \neq \boldsymbol{Z_i} | \boldsymbol{m}_i\ sent) \Pr(\boldsymbol{m}_i\ sent)$$

lower bound of error analysis

- union Bound of probability

$$P_e(m_i) = Pr\left(\bigcup_{k=1,k\neq i}^{M} A_{i,k}\right) \leq \sum_{k=1,k\neq i}^{M} \Pr(A_{i,k}) = \sum_{k=1,k\neq i}^{M} Q\left(\frac{d_{i\,,k}}{\sqrt{2N_0}}\right)$$

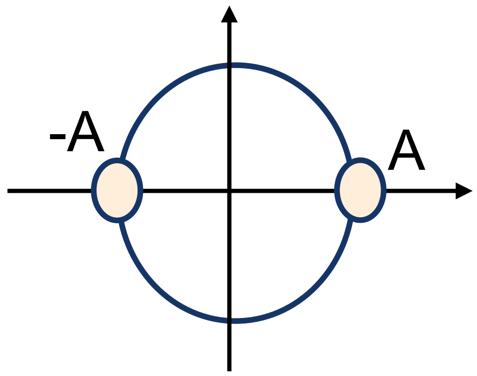
- expectation of error probability

$$P_e = \sum_{i=1}^{M} \Pr(m_i) P_e(m_i) \leq \frac{1}{M} \sum_{i=1}^{M} \sum_{k=1,k\neq i}^{M} Q\left(\frac{d_{i\,,k}}{\sqrt{2N_0}}\right)$$

- looser bound
  - $d_{min} = \min_{i,k} d_{ik}$

$$P_e \leq (M-1) Q\left(\frac{d_{min}}{\sqrt{2N_0}}\right)$$

error probability for BPSK



- Bit 1: $s_1(t) = Ag(t)\cos(2\pi f_c t)$
- Bit 0: $s_2(t) = -Ag(t)\cos(2\pi f_c t)$
- Minimum distance: $A - (-A) = 2A$
- Energy per bit:

$$E_b = \int_0^{T_b} s_1(t)^2\,dt = \int_0^{T_b} s_2(t)^2\,dt = \int_0^{T_b} A^2 g(t)^2 cos^2(2\pi f_c t)\,dt = A^2$$

- Bit Error Probability

$$P_b = Q\left(\frac{d_{min}}{\sqrt{2N_0}}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) = Q\left(\sqrt{2\gamma_b}\right)$$

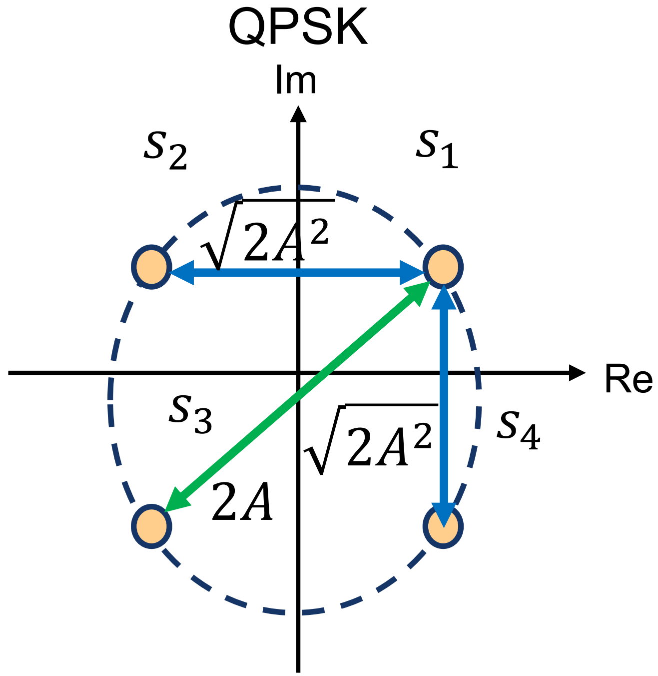
error probability of QPSK

- union bound of error probability

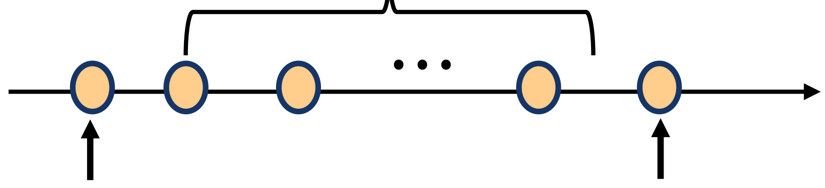
$$P_e \leq 2Q\left(\frac{A}{\sqrt{N_0}}\right) + Q\left(\frac{A\sqrt{2}}{N_0}\right)$$

- $\gamma_s = 2\gamma_b = 2\frac{A^2}{N_0}$

$$P_e \leq 2Q\left(\sqrt{\frac{\gamma_s}{2}}\right) + Q(\sqrt{\gamma_s})$$



error Probability for ASK/PAM



- two types of symbols
  - $M-2$ inner points
  - 2 Outer points

Error probability for inner point

$$p_{e,i} = Pr\left[|n| > \frac{d_{min}}{2}\right] = 2Q(\frac{d_{min}}{\sqrt{2N_0}})$$

Error probability for outer point

$$p_{e,o} = \frac{1}{2}p_{e,i} = 2Q(\frac{d_{min}}{\sqrt{2N_0}})$$

- Expected error probability

$$P_e = \frac{1}{M}\left[(M-2)p_{e,i} + 2p_{e,o}\right] = \frac{2(M-1)}{M}Q(\frac{d_{min}}{\sqrt{2N_0}})$$

summary and outlook

- coding for reliable communication

- digital modulation
    - Amplitude-Shift Keying (ASK)
    - Phase-Shift Keying (PSK)
    - Quadrature Amplitude Modulation (QAM)
    - Frequency-Shift Keying (FSK)

- detection theory and Maximum Likelihood decoding