

# Lecture 1: Block codes

Invited lecturer: Grigory Kabatiansky

`g.kabatyansky@skoltech.ru`

Teaching Assistant: Stanislav Kruglik

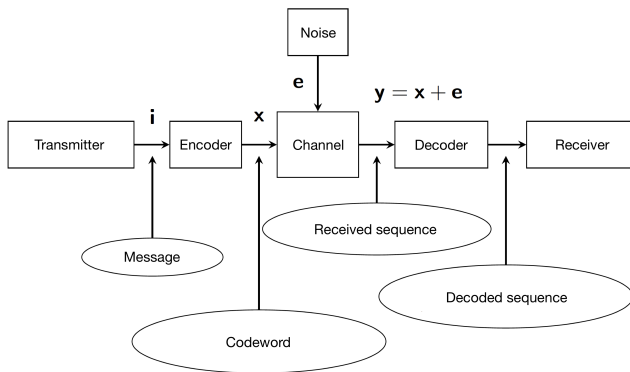
`stanislav.kruglik@skolkovotech.ru`

January 30, 2018

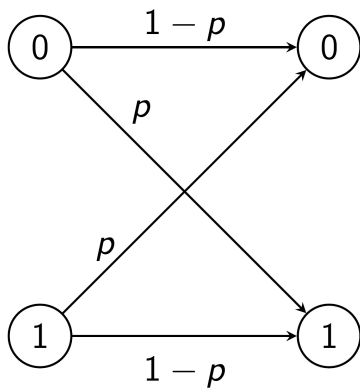
- 1 Definitions and geometric interpretation
- 2 Bounds on code parameters
- 3 Problems

- 1 Definitions and geometric interpretation
- 2 Bounds on code parameters
- 3 Problems

# Noisy transmission



# Binary symmetric channel



101101  $\rightsquigarrow$  100101

# Why do we need encoder and decoder?

## Example

Let  $p = 10^{-3}$ .

The probability of correct reception of  $n$  bits is equal to

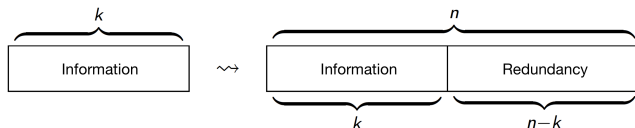
$$P_0(n) = (1 - p)^n = 0.999^n.$$

Note, that

- $P_0$  decreases exponentially;
- $P_0(10^3) < 0.37$ ;
- $P_0(10^5) < 5 \cdot 10^{-5}$ ;

# Block and convolutional coding

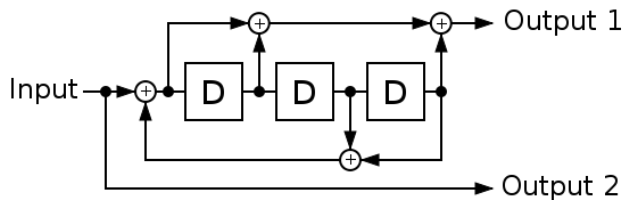
**Main idea:** add redundancy and use it to deal with errors.



Coding methods:

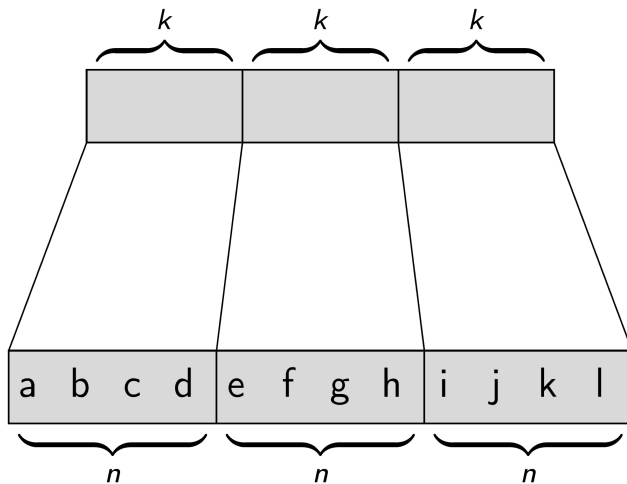
- 1 **Block codes.** Information is split in blocks of  $k$  bits. Each block is encoded independently. As a result we obtain blocks of length  $n$ .
- 2 **Convolutional codes.** The output of a convolutional encoder (potentially) depends on all the previous input bits.

# Convolutional coding



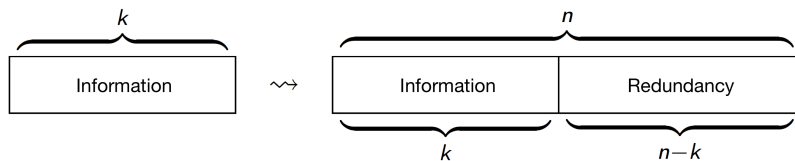


# Block coding



- $\{1, 2, \dots, M\}$  – message set;
- $Q = \{0, \dots, q - 1\}$ ;
- $\mathbf{x} = \Psi(i) \in Q^n$  – codeword;
- $\mathcal{C} = \{\mathbf{x} = \Psi(i), i = 1, \dots, M\}$  – code;
- codebook – a table with all codewords listed;
- $\mathbf{y} \sim P(y^n|x^n)$  – received sequence;
- $\hat{i} = \Psi^{-1}(\mathbf{y})$  – decoding rule.
- $R = \frac{\log_q M}{n} = \frac{k}{n}$ .

# Systematic encoding



$k$  information symbols,  $n - k$  check symbols.

# How to decode?

$$\mathbf{y} = 10101$$

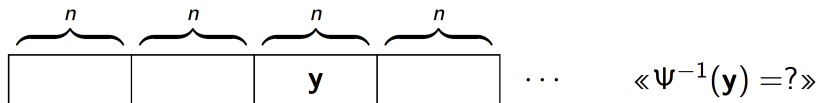
$$\psi : \begin{cases} 00 \rightarrow 00001 \\ 01 \rightarrow 01010 \\ 10 \rightarrow 10111 \\ 11 \rightarrow 11100 \end{cases}$$

$\mathbf{x}$	$P(\mathbf{y} \mathbf{x})$
00001	$p^2(1-p)^3$
01010	$p^5$
10111	$p(1-p)^4$
11100	$p^2(1-p)^3$

$$p^5 < p^2(1-p)^3 < p(1-p)^4$$

$$\Rightarrow \mathbf{x} = 10111, \mathbf{i} = 10$$

# Maximum likelihood decoding



ML decoding:

- ①  $\mathbf{x} = \arg \max_{\mathbf{x} \in \mathcal{C}} P(\mathbf{y}|\mathbf{x});$
- ②  $i = \Psi^{-1}(\mathbf{x}).$

## Lemma

Let  $\mathcal{C} = \{\mathbf{x}_i\}$ ,  $p < 0.5$  and  $P(\mathbf{y}|\mathbf{x}) = \max_i P(\mathbf{y}|\mathbf{x}_i)$ , then

$$d(\mathbf{y}, \mathbf{x}) = \min_i d(\mathbf{y}, \mathbf{x}_i),$$

where  $d(\mathbf{y}, \mathbf{x})$  denotes the number of elements in which  $\mathbf{y}$  and  $\mathbf{x}$  differ.

# Hamming distance

## Definition

Let  $\alpha, \beta \in Q^n$ .

$$d(\alpha, \beta) = |\{i : \alpha(i) \neq \beta(i)\}|.$$

## Example

$$\alpha = 01101$$

$$\beta = 00111$$

$$d(\alpha, \beta) = 2.$$

## Definition

- $||\alpha|| = d(\alpha, \mathbf{0})$  – weight of  $\alpha$ ;
- $|\alpha| = \sum_{i=1}^n \alpha_i q^{n-i}$  – number (lexicographic order) of  $\alpha$ ;

## Definition

Let us consider a metric space  $(Q^n, d)$ , then a ball and sphere are defined as follows

$$B_r(\alpha) = \{\beta \in Q^n : d(\alpha, \beta) \leq r\}$$

and

$$S_r(\alpha) = \{\beta \in Q^n : d(\alpha, \beta) = r\}$$



$$|S_r(\alpha)| = \binom{n}{r} (q-1)^r$$

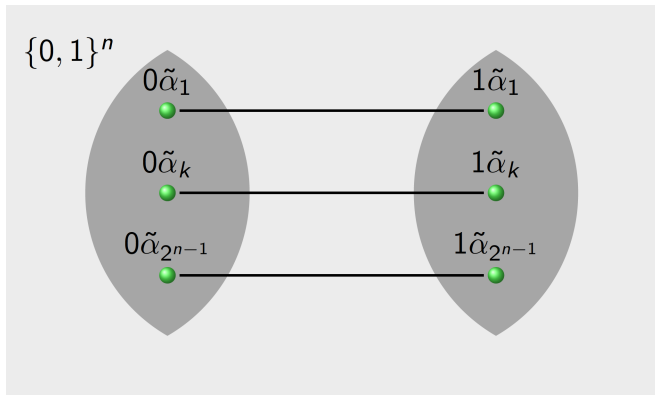
and

$$|B_r(\alpha)| = \sum_{i=0}^r |S_i(\alpha)| = \sum_{i=0}^r \binom{n}{i} (q-1)^i$$

- $\{0, 1\}^n$  – Boolean cube;
- $\{0, 1\}_k^n = \{\alpha \in \{0, 1\}^n : \|\alpha\| = k\}$  – Boolean cube layer;
- The set of points of  $\{0, 1\}^n$  with fixed  $n - k$  coordinates is called  $k$ -dimensional facet.

$$*0*10 = \left\{ \begin{array}{l} 00010 \\ 00110 \\ 10010 \\ 10110 \end{array} \right\}$$

$$\{0, 1\}^{n-1} \rightarrow \{0, 1\}^n$$

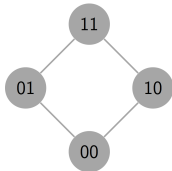


# Small dimensions

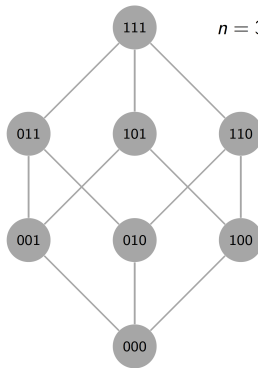
$n = 1$

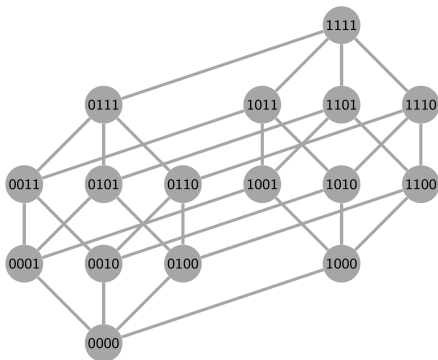


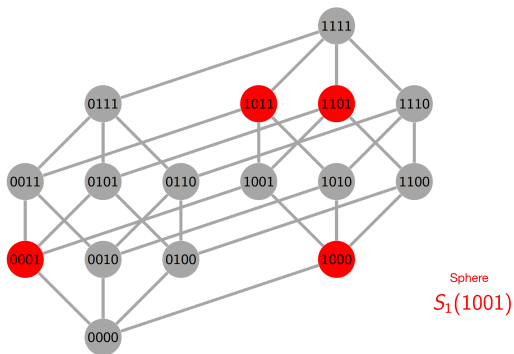
$n = 2$

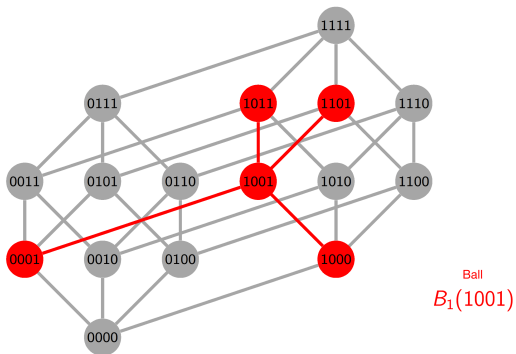


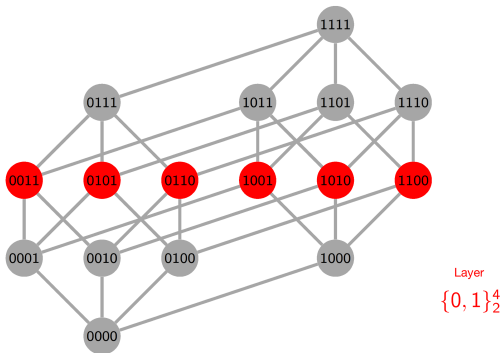
$n = 3$



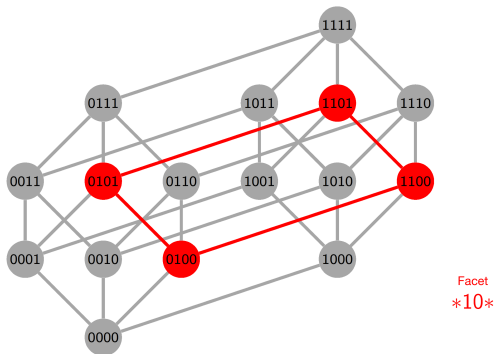












## Definition

- Code  $\mathcal{C} \subseteq Q^n$ ;
- Minimum code distance

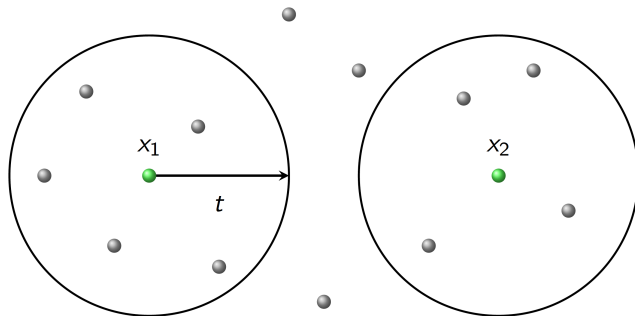
$$d(\mathcal{C}) = \min_{a, b \in \mathcal{C}; a \neq b} d(a, b).$$

## Theorem

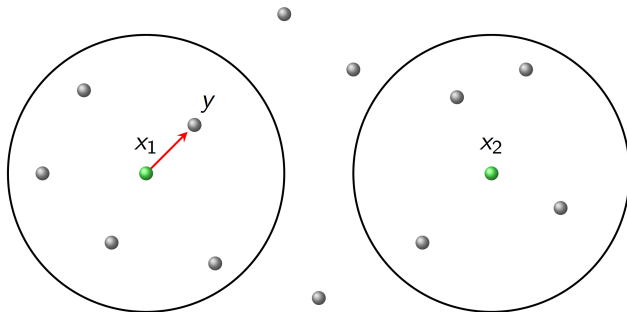
*Assume the code  $\mathcal{C}$  can correct  $t$  errors, then*

$$d(\mathcal{C}) \geq 2t + 1.$$

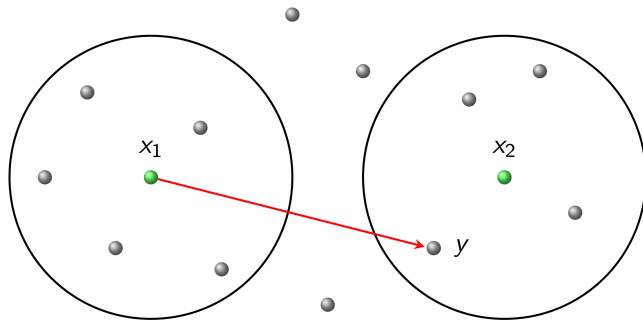
# Geometric interpretation



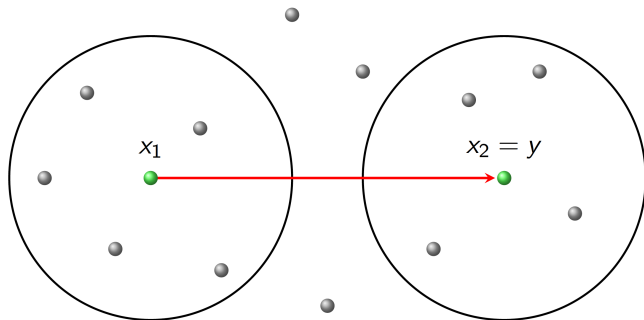
# Error corrected



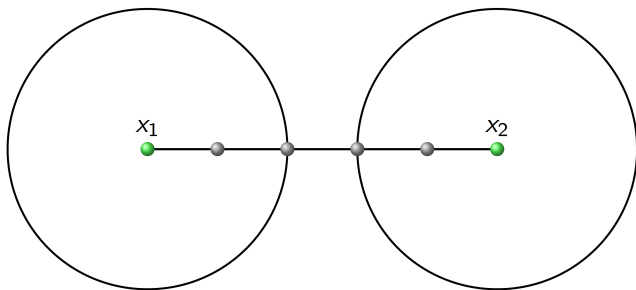
# Error detected



# Error undetected

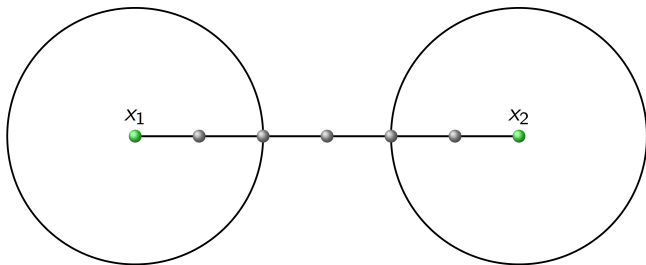


# Odd distance



$$d = 5 \Rightarrow t = 2, s = 4, s' = 2$$





$$d = 6 \Rightarrow t = 2, s = 5, s' = 3$$

## Theorem

*Assume  $d(C) = d$ , then*

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

*and*

$$s = d - 1.$$

- 1 Definitions and geometric interpretation
- 2 Bounds on code parameters
- 3 Problems

# Definition of $A_q(n, d)$

## Definition

$$A_q(n, d) = \max_{\mathcal{C} \subseteq Q^n, d(\mathcal{C})=d} |\mathcal{C}|.$$

Note, that size and rate maximization are equal tasks.

In what follows we omit the index  $q$  in case of  $q = 2$ .

# Hamming bound

Let  $\alpha \in Q^n$ . Let us introduce a notation

$$V_t = V_q(t) = |B_t(\alpha)| = \sum_{i=0}^n \binom{n}{i} (q-1)^i.$$

## Theorem (Hamming bound)

$$A_q(n, d) \leq \frac{q^n}{V_t}.$$

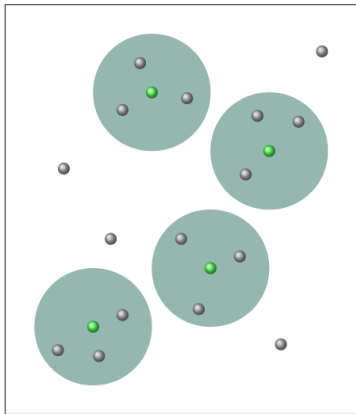
## Definition

The code is called a *perfect* code if  $|\mathcal{C}| = \frac{q^n}{V_t}$ .

## Example

A code  $\mathcal{C} = \{000, 111\} \subset \{0, 1\}^3$  is a perfect code.

# Proof of Hamming bound

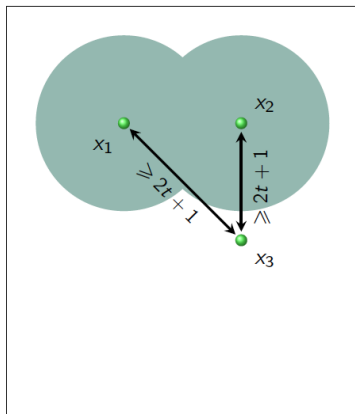


Balls of radius  $t$  do not intersect!

$$A_q(n, d)V_q(t) \leq q^n.$$

Theorem (Varshamov–Gilbert bound)

$$A_q(n, d) \geq \frac{q^n}{V_{2t}}.$$



$$\mathbf{x}_3 \notin B_{2t}(\mathbf{x}_1) \cup B_{2t}(\mathbf{x}_2)$$

$\mathcal{C}_3 = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$  corrects  $t$  errors.

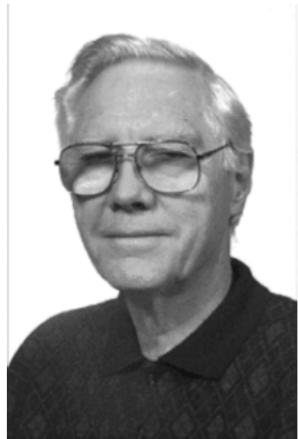
Assume we constructed  $m$  codewords and can not add more

$$q^n = \left| \bigcup_{i=1}^m B_{2t}(\mathbf{x}_i) \right| \leq mV_{2t}.$$





Richard Wesley  
Hamming



Edgar Nelson  
Gilbert

# Singleton bound

## Theorem (Singleton bound)

$$A_q(n, d) \leq q^{n-d(C)+1}.$$

## Proof.

Consider the codebook and delete  $d - 1$  columns from it. All the words are different in the resulting table. □

Theorem (Plotkin bound)

$$d(\mathcal{C}) \leq \frac{q-1}{q} \frac{M}{M-1} n.$$

$$S = \sum_{u,v \in \mathcal{C}} d(u,v).$$

Note, that

$$S \geq M(M-1)d$$

Consider the first column of the codebook. Let  $t_i$  be the number of times  $i$  appears in the first column.

$$\sum_{i=0}^{q-1} t_i(M - t_i) = \ell.$$

Finally,

$$\ell = M^2 - \sum_{i=0}^{q-1} t_i^2 \leq M^2 - q \left( \frac{M}{q} \right)^2 = M^2 \frac{q-1}{q}.$$

$$\frac{d}{n} \rightarrow \delta, \frac{\log_q M}{n} = \frac{k}{n} \rightarrow R$$

## Definition

A code family  $\{\mathcal{C}_n\}$  is said to be *asymptotically good* if there exist constants  $R, \delta > 0$ :

- $\frac{\log_q M_n}{n} = \frac{k_n}{n} \geq R > 0$ ;
- $\frac{d_n}{n} \geq \delta > 0$ ;

# Asymptotic regime, $n \rightarrow \infty$ , $q = 2$

Hamming bound

$$R \leq 1 - h(\delta/2).$$

Varshamov–Gilbert bound

$$R \geq 1 - h(\delta).$$

Singleton bound

$$R \leq 1 - \delta.$$

Plotkin bound

$$R \leq \frac{1}{2}(1 - \delta).$$

To derive asymptotic form of Hamming and Varshamov–Gilbert bounds use the following inequality

$$\sum_{i=0}^W \binom{n}{i} \leq 2^{nh\left(\frac{W}{n}\right)} \quad \text{for } W \leq n/2.$$

# Proof hints

To derive asymptotic form of Plotkin bound use the shortening method

## Lemma

$$A_q(n, d) \leq qA_q(n-1, d).$$

## Proof.

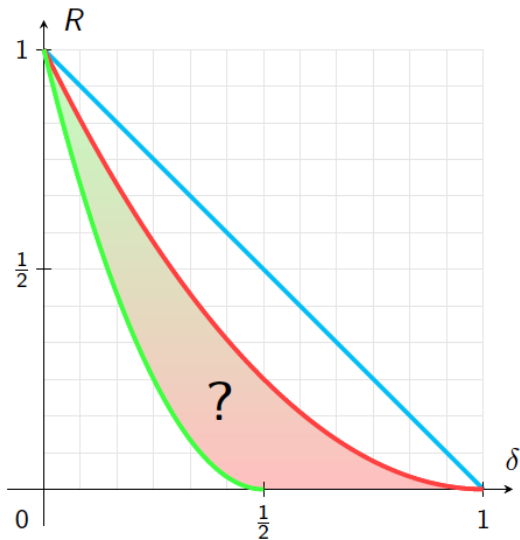
Consider the codebook and split it into  $q$  parts in dependence on the first symbol, i.e.

$$\mathcal{C} = \begin{bmatrix} 0 & \mathcal{C}'_0 \\ 1 & \mathcal{C}'_1 \\ \vdots & \\ q-1 & \mathcal{C}'_{q-1} \end{bmatrix}$$

At least one of the codes  $\mathcal{C}'_i$  contains  $|\mathcal{C}|/q$  codewords. At the same time  $d(\mathcal{C}'_i) \geq d(\mathcal{C})$  for all  $i$ . □



# Asymptotic regime, $n \rightarrow \infty$



- 1 Definitions and geometric interpretation
- 2 Bounds on code parameters
- 3 Problems

# Problem 1

Let us have binary symmetric channel (BSC) with bit error rate  $10^{-5}$ . To transmit data over this channel we use some code of length 1000.

- a. Find the probability of occurring  $k$  errors in a codeword for  $k=0,1,2$
- b. Suppose that the bit error rate after decoding must be LESS than  $10^{-9}$ . What should be the minimal required error correcting capability of an employed code in order to guaranty this probability by correcting errors up to the half of the minimal code distance?

## Problem 2

Let us have binary repetition code of length 4

- a. List codewords which will be uniquely decoded as 1111 using maximal likelihood technique.
- b. Find the probability of wrong decoding if probability of error in one symbol is equal to  $p$

## Problem 3

Proof that the over-all parity check code is optimal, i.e., has the maximal cardinality among all codes with the minimal distance  $d=2$  and the same length.

## Problem 4

Do the codes  $[16, 11, 9]_2$  and  $[16, 10, 9]_2$  exist?

Thank you for your attention!