Channel Coding I

Exercises

– SS 2019 –

Lecturer: Dirk Wübben
Tutor: Shayan Hassanpour
SPT, Room C 3220, Tel.: 0421/218-62387
E-mail: {wuebben, hassanpour}@ant.uni-bremen.de

Universität Bremen, FB1
Institut für Telekommunikation und Hochfrequenztechnik
Arbeitsbereich Nachrichtentechnik
Prof. Dr.-Ing. A. Dekorsy
Postfach 33 04 40
D–28334 Bremen

WWW-Server: http://www.ant.uni-bremen.de

Version from July 12, 2019

General Information

- The dates for the exercises are arranged in the lectures. Tutorials take place in room N 1250. The exercises cover the contents of past lectures and contain a theoretical part and a programming part, in general. The students are advised to repeat the corresponding chapters and to prepare the exercises for presenting them at the board.
- All references to passages in the text (chapter- and equation numbers) refer to the script: V. Kühn, **"Kanalcodierung I+II"** in german language. References of equations in the form of (1.1) refer to the script, too, whereas equations in the form (1) refer to solutions of the exercises.
- Although MATLAB is used in the exercises, no tutorial introduction can be given due to the limited time. A tutorial and further information can be found in
  - MATLAB Primer, 3rd edition, Kermit Sigmon
  - Practical Introduction to Matlab, Mark S. Gockenbach
  - NT Tips und Tricks für MATLAB, Arbeitsbereich Nachrichtentechnik, Universität Bremen
  - Einführung in MATLAB von Peter Arbenz, ETH Zürich

  available on `http://www.ant.uni-bremen.de/teaching/kc/exercises/`.
- PDF-files of the tasks, solutions and MATLAB codes are available on
  `http://www.ant.uni-bremen.de/de/courses/cc1/`.

  Within the university net the additional page
  `http://www.ant.uni-bremen.de/de/courses/cc1/`
  is available. Beside the tasks and solutions you will find additional information on this page, e.g the matlab primer, the original paper of C. E. Shannon **A mathematical theory of communication**, some scripts and a preliminary version of the book "Error-Control Coding" of B. Friedrichs!

1 Introduction

Exercise 1.1 **Design of a discrete channel**

a) Given is a transmitting alphabet consisting of the symbols -3, -1, $+1$, $+3$. They shall be transmitted over an AWGN channel, which is real-valued and has the noise variance $\sigma_n^2 = 1$. At the output of the channel a hard-decision takes place, i.e. the noisy values are again mapped to the 4 symbols ($\mathcal{A}_{\text{out}} = \mathcal{A}_{\text{in}}$), where the decision threshold in each case lies in the middle of two adjacent symbols. Calculate the transition probabilities $\Pr\{Y_\mu | X_\nu\}$ of the channel and represent them in a matrix.

b) Check the correctness of the resulting matrix by checking the sums of probabilities to one.

c) Determine the joint probabilities $\Pr\{X_\nu, Y_\mu\}$ for equiprobable transmitting symbols.

d) Calculate the occurrence probabilities for the channel output symbols Y_μ.

e) Calculate the error probability $P_{\text{e}}\{X_\nu\}$ for the transmitting symbols X_ν and the mean overall error probability P_{e}.

Exercise 1.2 **Statistics of the discrete channel**

Given are the channels in **figure 1**. Complete the missing probabilities.

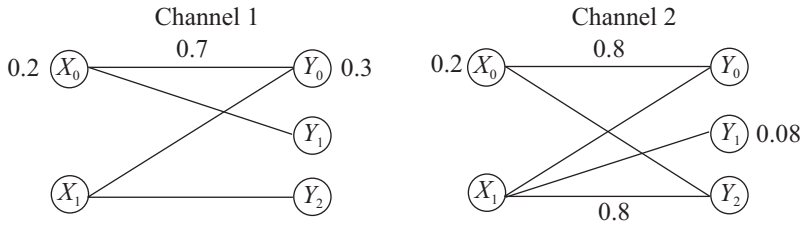


Fig. 1: Discrete channel models

Exercise 1.3 **Binary symmetric channel (BSC)**

a) The word 0110100 is transmitted by a BSC with the error probability $P_{\text{e}} = 0.01$. Specify the probability of receiving the word 0010101, wrongly.

b) Determine the probability of m incorrectly received bits at the transmission of n bits.

c) For a BSC with the error probability $P_{\text{e}} = 0.01$, the probability of more than 2 errors at words of length 31 shall be determined.

Exercise 1.4 **Serial concatenation of two BSCs**

Two BSCs with $P_{\text{e},1}$ and $P_{\text{e},2}$ shall be connected in series. Determine the error probability of the new channel.

Exercise 1.5 **Transmission of coded data over a BSC**

Use Matlab to simulate the transmission of coded data over a Binary Symmetric Channel (BSC) with error probability $P_{\text{e}} = 0.1$. Apply repetition coding of rate $R_{\text{c}} = 1/5$ for error protection.

2 Survey of Information Theory

Exercise 2.1 **Entropy**

a) The average information content $\mathcal{H}(X_\nu)$ of the signal X_ν (also called partial entropy) shall be maximized. Determine the value $\Pr\{X_\nu\}$, for which the partial entropy reaches its maximum value and specify $\mathcal{H}(X_\nu)_{max}$. Check the result with MATLAB by determining the partial entropy for $\Pr\{X_\nu\} = 0 : 0.01 : 1$ and plotting $\mathcal{H}(X_\nu)$ over $\Pr\{X_\nu\}$.

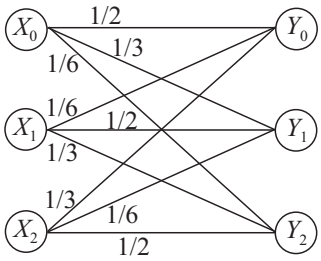
b) The random vector $(X_1X_2X_3)$ can exclusively carry the values (000), (001), (011), (101) and (111) each with the probability of $1/5$.

Determine the entropies:

1. $\mathcal{H}(X_1)$
2. $\mathcal{H}(X_2)$
3. $\mathcal{H}(X_3)$
4. $\mathcal{H}(X_1, X_2)$
5. $\mathcal{H}(X_1, X_2, X_3)$
6. $\mathcal{H}(X_2|X_1)$
7. $\mathcal{H}(X_2|X_1 = 0)$
8. $\mathcal{H}(X_2|X_1 = 1)$
9. $\mathcal{H}(X_3|X_1, X_2)$

Exercise 2.2 **Channel capacity of a discrete memoryless channel**

Determine the channel capacity for the following discrete memoryless channel on condition that $\Pr\{X_\nu\} = 1/3$ is valid.



Exercise 2.3 **Channel capacity of the BSC**

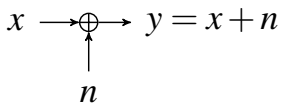
a) Derive the capacity for equiprobable input symbols $\Pr\{X_0\} = \Pr\{X_1\} = 0.5$ in dependence on the error probability for a binary symmetric channel (BSC).

b) Prepare a MATLAB program, which calculates the (input-output)mutual information of an asymmetric binary channel for the input probabilities $\Pr\{X_0\} = 0 : 0.01 : 1$. It shall be possible to set the error probabilities P_{e,X_0} and P_{e,X_1} at the program start. (Attention: $\Pr\{Y\}$ must be calculated!)

c) For a BSC determine the (input-output)mutual information for several error probabilities P_e at a fixed input probability $\Pr\{X\}$ within MATLAB. Plot the corresponding curves of $\mathcal{I}(X;Y)$.

Exercise 2.4 **Channel capacity of the AWGNC**

Derive the channel capacity for a Gaussian channel ($\sigma_n^2 = N_0/2$) with normal distribution at input ($\sigma_x^2 = E_s$).



3 Linear Block Codes

3.1 Finite Field Algebra

Exercise 3.1 **Polynomials in the GF(2)**

a) Given is the polynomial $p(D) = 1 + D^3 + D^4 + D^5 + D^6$ in the GF(2). Check if $p(D)$ is irreducible with respect to GF(2) or primitive in the GF(2^6) using the routine `gfprimck`.

b) Determine the partial polynomials of $p(D)$ using the routine `gfdeconv`. (Hint: polynomials can be represented clearly visible in MATLAB with the command `gfpretty`.)

c) State a list of all primitive polynomials of the GF(2^6) using the MATLAB command `gfprimfd`.

d) Determine all irreducible polynomials of rank $m = 7$ that are not primitive polynomials with a MATLAB routine.

Exercise 3.2 **Fields**

Given is the set $\mathcal{S}_q := \{0, 1, \ldots, q-1\}$ and two connections

- Addition modulo q
- Multiplication modulo q

a) Calculate the connection tables for $q = 2, 3, 4, 5, 6$.

b) Specify from which q results a field.

c) Specify a primitive element for each field.

Exercise 3.3 **Extension of a non-binary field, GF(3^2)**

Compute the *log table* (i.e., a table of all elements of the field in exponential representation) for GF(3^2). Use $p(D) = D^2 + D + 2$ as a primitive polynomial over GF(3).

Exercise 3.4 **Extension of a binary field, GF(2^4)**

Compute the *log table* for GF(2^4). Use $p(D) = D^4 + D + 1$ as a primitive polynomial over GF(2). Then

a) Use the table to calculate $p_1(D) = (D - \alpha)(D - \alpha^2)(D - \alpha^4)(D - \alpha^8)$.

b) Use the table to calculate $p_2(D) = (D - \alpha)(D - \alpha^2)(D - \alpha^3)(D - \alpha^4)$.

c) Comment on the difference between $p_1(D)$ and $p_2(D)$ (BCH-Code introduction).

Exercise 3.5 **2-out-of-5-code**

a) Given is a simple 2-out-of-5-code of length $n = 5$ that is composed of any possible words with the weight $w_{\mathrm{H}}(\mathbf{c}) = 2$. Specify the code Γ. Is it a linear code?

b) Determine the distance properties of the code. What is to be considered?

c) Calculate the probability P_{ue} of the occurrence of an undetectable error for the considered code at a binary symmetric channel. The bit-flip probability of the BSC shall be in the range $10^{-3} \leq P_e \leq 0.5$. Represent P_{ue} in dependence on P_e graphically and depict also the error rate of the BSC in the chart.

3.2 Distance Properties of Block Codes

Exercise 3.6 **Error correction**

Given is a $(n, k)_q$ block code with the minimum distance $d_{\min} = 8$.

a) Determine the maximum number of correctable errors and the number of detectable errors at pure error detection.

b) The code shall be used for the correction of 2 errors and for the simultaneous detection of 5 further errors. Demonstrate by illustration in the field of code words (like in Fig 2), that this is possible.

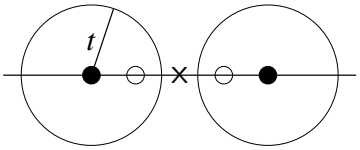


Fig. 2: Example of a code with $d_{\min} = 4$

c) Demonstrate by illustration in the field of code words, how many possibilities of variation of a code word have to be taken into consideration for the transmission over a disturbed channel.

Exercise 3.7 **Sphere-Packing bound (Hamming bound)**

a) A linear $(n, 2)_2$-block code has the minimum Hamming distance $d_{\min} = 5$. Determine the minimum block length.

$$q^{n-k} \geq \sum_{r=0}^{t} \binom{n}{r} \cdot (q-1)^r$$

b) A binary code Γ has the parameters $n = 15, k = 7, d_{\min} = 5$. Is the sphere-packing bound fulfilled? What does the right side minus the left side of the sphere-packing bound (cp. eq. (3.7)) state?

c) Can a binary code with the parameters $n = 15, k = 7, d_{\min} = 7$ exist?

d) Check whether a binary code with the parameters $n = 23, k = 12, d_{\min} = 7$ can exist.

e) A source-coder generates 16 different symbols with equal probability, that shall be binary coded with a correction capacity of $t = 4$ in the channel-coder. How large does the code rate have to be in any case?

3.3 Matrix Description of Block Codes

Exercise 3.8 **Generator and parity check matrices**

a) State the generator as well as the parity check matrix for a $(n, 1, n)$ repetition code with $n = 4$. What parameters and properties does the dual code have?

b) The columns of the parity check matrix of a Hamming code of rank r represent all dual numbers from 1 to $2^r - 1$. State a parity check matrix for $r = 3$ and calculate the corresponding generator matrix. Determine the parameters of the code and state the code rate.

c) Analyze the connection between the minimum distance of a code and the number of linearly independent columns of the parity check matrix $\mathbf{H}$ by means of this example.

Exercise 3.9 **Expansion, shortening and puncturing**

a) Given is the systematic $(7, 4, 3)$-Hamming code from exercise 3.8. Expand the code by an additional test digit such that it gets a minimum distance of $d_{\min} = 4$. State the generator matrix $\mathbf{G}_E$ and the parity check matrix $\mathbf{H}_E$ of the expanded (8,4,4)-code.
Hint: Conduct the construction with the help of the systematic parity check matrix $\mathbf{H}_{sys}$ and note the result from 3.8c.

b) Shortening means decreasing the cardinality of the field of code words, i.e., information bits are canceled. Shorten the Hamming code from above to the half of the code words and state the generator matrix $\mathbf{G}_S$ and the parity check matrix $\mathbf{H}_S$ for the systematic case. What is the minimum distance of the shortened code?

c) Puncturing a code means removing some of the test bits (parity bits) which serves for increasing the code rate. Puncture the Hamming code from above to the rate $R_c = 2/3$. What is the minimum distance of the new code?

Exercise 3.10 **Coset decomposition and syndrome decoding**

a) State the number of syndromes of the $(7, 4, 3)$-Hamming code and compare it with the number of correctable error patterns.

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

b) Make up a table for the systematic $(7, 4, 3)$-Hamming coder which contains all syndromes and the corresponding coset leaders.

c) The word $\mathbf{y} = (1\,1\,0\,1\,0\,0\,1)$ is found at the receiver. Which information word $\mathbf{u}$ was sent with the highest probability?

d) The search for the position of the syndrome $\mathbf{s}$ in $\mathbf{H}$ can be dropped by resorting the columns of $\mathbf{H}$. The decimal representation of $\mathbf{s}$ then can directly be used for the addressing of the coset leader. Give the corresponding parity check matrix $\tilde{\mathbf{H}}$.

Exercise 3.11 **Coding program**

Write a MATLAB program which codes and decodes a certain number of input data bits. The transmission is assumed through a BSC with $P_e = 0.15$. The $(7, 4, 3)$-Hamming code with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and the parity check matrix

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

shall be used.

3.4 Cyclic Codes

Exercise 3.12 **Polynomial multiplication**

Given are two polynomials $f(D) = D^3 + D + 1$ and $g(D) = D + 1$.

a) Calculate $f(D) \cdot g(D)$. Check the result with MATLAB.

b) Give the block diagram of a non-recursive system for a sequential multiplication of both polynomials.

c) Illustrate the stepwise calculation of the polynomial $f(D) \cdot g(D)$ in dependence on the symbol clock by means of a table.

Exercise 3.13 **Polynomial division**

Given are two polynomials $f(D) = D^3 + D + 1$ and $g(D) = D^2 + D + 1$.

a) Calculate the division of $f(D)$ by $g(D)$. Check the result with MATLAB.

b) Give the block diagram of a recursive system for a sequential division of the polynomial $f(D)$ by the polynomial $g(D)$.

c) Illustrate the stepwise calculation of the polynomial $f(D) : g(D)$ in dependence on the symbol clock by means of a table.

Exercise 3.14 **Generator polynomial**

Given is a cyclic $(15, 7)$ block code with the generator polynomial $g(D) = D^8 + D^7 + D^6 + D^4 + 1$.

a) Indicate that $g(D)$ can be a generator polynomial of the code.

b) Determine the code polynomial (code word) in systematic form for the message $u(D) = D^4 + D + 1$.

c) Is the polynomial $y(D) = D^{14} + D^5 + D + 1$ a code word?

Exercise 3.15 **Syndrome**

The syndromes s_1 to s_8 of a 1-error-correcting cyclic code are given.

$$
\begin{array}{lcccccc}
s_1 & = & 1 & 0 & 1 & 0 & 0 \\
s_2 & = & 0 & 1 & 0 & 1 & 0 \\
s_3 & = & 0 & 0 & 1 & 0 & 1 \\
s_4 & = & 1 & 0 & 0 & 0 & 0 \\
s_5 & = & 0 & 1 & 0 & 0 & 0 \\
s_6 & = & 0 & 0 & 1 & 0 & 0 \\
s_7 & = & 0 & 0 & 0 & 1 & 0 \\
s_8 & = & 0 & 0 & 0 & 0 & 1
\end{array}
$$

a) Determine the parity check matrix $\mathbf{H}$ and the generator matrix $\mathbf{G}$.

b) State the number of test digits $n - k$ and the number of information digits k.

c) What is the generator polynomial $g(D)$?

d) How many different code words can be built with the generator polynomial $g(D)$?

e) The code word $\mathbf{y}_1 = (0\,1\,1\,0\,1\,0\,1\,1)$ is received. Has this code word been falsified on the channel? Can the right code word be determined? If yes, name the right code word.

f) Now the code word $\mathbf{y}_2 = (10110111)$ has been received. Has this code word been falsified on the channel? Can the right code word be determined? If yes, name the right code word.

Exercise 3.16 **Primitive polynomials**

Given are two irreducible polynomials $g_1(D) = D^4 + D + 1$ and $g_2(D) = D^4 + D^3 + D^2 + D + 1$. Which of these two polynomials is primitive?

Exercise 3.17 **CRC codes**

a) State the generator polynomial for a CRC code of length $n = 15$.

b) Determine the generator matrix $\mathbf{G}$ and the parity check matrix $\mathbf{H}$ using command `cyclgen`.

c) Now the efficiency of the CRC code shall be examined by considering the perceptibility of all burst errors of length $4 \leq l_e \leq n$. Only error patterns with l_e errors directly succeeding one another shall be taken into consideration. Give the relative frequency of the detectable errors.

Exercise 3.18 **Reed-Solomon codes**

a) A RS-code in the GF(2^3) that can correct $t = 1$ error is considered. Determine the parameters k, n and R_c.

b) Give the generator polynomial $g(D)$ of the RS-code. Use the command `rsgenpoly` cf. eq. (3.85).

c) The message $\mathbf{u} = (110\ 010\ 111\ 000\ 001)$ shall be coded. At the subsequent transmission 3 bits shall be falsified. How do the error positions affect the decoding result?

d) Now a $t = 2$ errors correcting code in the GF(8) shall be designed. Determine the parameters k and R_c and give $g(D)$.

e) The word $\mathbf{y} = (110\ 010\ 111\ 011\ 010\ 110\ 110)$ is received. Determine the number of errors, corrected code word and the transmitted message using command `rsdec`.

Exercise 3.19 **BCH codes**

a) We want to design a BCH code in the GF(2^4) that can correct $t = 3$ errors. Form the cyclotomic cosets $\mathcal{K}_i$ with the command `gfcosets`. Which sets can be combined to fulfill the requirement of $t = 3$. Which parameters does the resulting BCH code have?

b) By declaration of the parameters n and k, the command `bchgenpoly` supplies a valid generator polynomial $g(D)$. Choose suitable code parameters and determine $g(D)$.

c) Code the information word $\mathbf{u} = (1\,1\,0\,1\,1)$ with the command `bchenc` and determine the roots of the code word $c(D)$ with the help of the command `gfroots`.

d) Transform the code word with the function `gf_dft` into the spectral domain. What is noticeable?

4 Convolutional Codes

4.1 Fundamental Principles

Exercise 4.1 **Convolutional codes**

Given is a convolutional code with the code rate $R_c = 1/3$, memory $m = 2$ and the generator polynomials $g_1(D) = 1 + D + D^2$ and $g_2(D) = 1 + D^2$ and $g_3(D) = 1 + D + D^2$.

a) Determine the output sequence for the input sequence $u = (0\ 1\ 1\ 0\ 1\ 0)$.

b) Sketch the corresponding Trellis diagram for the given input sequence in a).

c) Sketch the state diagram of the encoder.

d) Determine the corresponding free distance d_f.

4.2 Characterization of Convolutional Encoders

Exercise 4.2 **Catastrophic encoders**

Given is a convolutional code with the generator polynomials $g_1(D) = 1 + D^2$ and $g_2(D) = 1 + D$. Show that this corresponds to a catastrophic encoder and explain the consequences.

4.3 Optimal Decoding with Viterbi Algorithm

Exercise 4.3 **Viterbi decoding**

Given is a convolutional code with $g_1(D) = 1 + D + D^2$ and $g_2(D) = 1 + D^2$, where termination shall be considered.

a) Generate the corresponding Trellis diagram and encode the information sequence $u(\ell) = (1\ 1\ 0\ 1)$.

b) Conduct the Viterbi decoding for the transmitted code sequence $x = (11\ 01\ 01\ 00\ 10\ 11)$ and for the two disturbed receiving sequences $y_1 = (11\ 11\ 01\ 01\ 10\ 11)$ and $y_2 = (11\ 11\ 10\ 01\ 10\ 11)$ respectively and describe the differences.

c) Check the results with the help of a MATLAB program:

Define the convolutional code with `G=[7;5]`, `r_flag=0` and `term=1`, generate the Trellis diagram with `trellis = make_trellis(G,r_flag)` and sketch it with `show_trellis(trellis)`. Encode the information sequence `u` with `c = conv_encoder(u,G,r_flag,term)` and decode this sequence with `viterbi_omnip(c,trellis,r_flag,term,6,1)`. Then decode the sequences `y_1` and `y_2`.

Exercise 4.4 **Viterbi decoding with puncturing**

Given is a convolutional code with $g_1(D) = 1 + D + D^2$ and $g_2(D) = 1 + D^2$, out of which a punctured code shall be generated by the puncturing matrix

$$\mathbf{P} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

a) Determine the code rate of the punctured code.

b) Conduct the Viterbi decoding for the case of undisturbed receiving sequence $y = (1\,1\,0\,0\,0\,1\,0\,1)$. Pay attention to the puncturing!

Exercise 4.5 **RSC encoders**

a) We consider a recursive systematic convolutional encoder with the generator polynomials $\tilde{g}_1(D) = 1$ and $\tilde{g}_2(D) = (1 + D + D^3)/(1 + D + D^2 + D^3)$. Generate the Trellis diagram of the code with the help of the MATLAB command `make_trellis([11;15],2)`.

b) Perform the encoding for the input sequence $u(\ell) = (1\,1\,0\,1\,1)$. The encoder shall be conducted to the zero state by adding tail bits (command `conv_encoder(u,[11;15],2,1)`). What are the output and the state sequences?

Exercise 4.6 **Simulation of a convolutional encoder and decoder**

Generate a MATLAB program that encodes, BPSK modulates, transmits over an AWGN channel and subsequently hardly decodes an information sequence u of the length $k = 48$ with the terminated convolutional code `G=[5;7]`. Take with this program the bit error rate curve for $E_b/N_0 = 0 : 1 : 6$ dB corresponding to fig. 4.14 by transmitting $N = 1000$ frames per SNR, adding the bit errors per SNR and subsequently determining the bit error rate per SNR.

To do so, use the following MATLAB functions:

```
trellis = make_trellis(G,r_flag)

c = conv_encoder(u,G,r_flag,term)

u_hat = viterbi(y,trellis,r_flag,term,15)
```