Channel Coding I

Exercises

– SS 2016 –

Lecturer: Dirk Wübben, Carsten Bockelmann
Tutor: Ahmed Emara, Matthias Woltering
NW1, Room N 2400, Tel.: 0421/218-62392
E-mail: {wuebben, bockelmann, emara, woltering}@ant.uni-bremen.de

Universität Bremen*

Universität Bremen, FB 1
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 June 13, 2016

Exercises

General Information

- The dates for the exercises are arranged in the lectures and take place in room N 2250 or N 2410. 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 variance $\sigma_{\mathrm{N}}^2 = 1$. 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 thresholds in each case lies in the middle of two symbols. Calculate the transition probabilities $P(Y_\mu|X_\nu)$ of the channel and represent them in a matrix.

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

c) Determine the joint probabilities $P(X_\nu, Y_\mu)$ for equally probable transmitting symbols.

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

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

Exercise 1.2 **Statistics of the discrete channel**

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

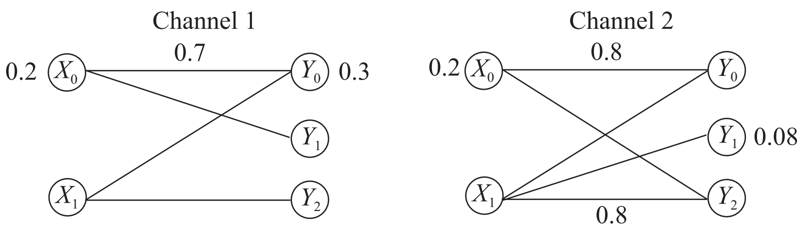


Fig. 1: Discrete channel models

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

a) The word 0110100 is transmitted by a BSC with the error probability $P_{\mathrm{e}} = 0.01$. 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 $P_{\mathrm{e}} = 0.01$, the probability of more than 2 errors at words of the length 31 shall be determined.

Exercise 1.4 **Serial concatenation of two BSC**

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

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

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

2 Information theory

Exercise 2.1 **Entropy**

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

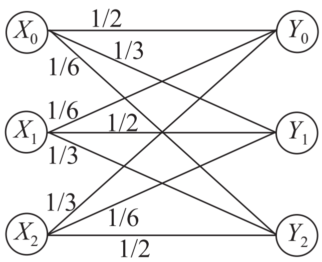
b) The random vector $(X_1 X_2 X_3)$ can exclusively carry the values (000), (001), (011), (101) and (111) each with a probability of $1/5$.

   Determine the entropies:

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

Exercise 2.2 **Channel capacity of a discrete memory-free channel**

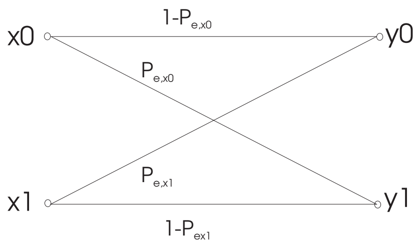
Determine the channel capacity for the following discrete memory-free channel on condition that $P(X_\nu) = 1/3$ is valid.



Exercise 2.3 **Channel capacity of a BSC**

a) Derive the capacity for equally probable input symbols $P(X_0) = P(X_1) = 0.5$ in dependence on the error probability for a binary symmetric channel (BSC).

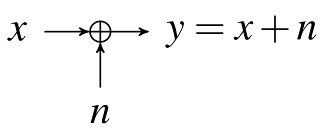
b) Prepare a MATLAB program, which calculates the capacity of an unsymmetric binary channel for the input probabilities $P(x) = 0 : 0.01 : 1$. It shall be possible to set the error probabilities $P_{e,x0}$ and $P_{e,x1}$ at the program start. (Attention: $P(y)$ must be calculated!)



c) Determine the channel capacity for several error probabilities P_e at a fixed input probability $P(x)$ within MATLAB. Plot $C(P_e)$.

Exercise 2.4 **Channel capacity of the AWGN**

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



3 Linear block codes

3.1 Finite field algebra

Exercise 3.1 **Polynomial 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 reference to $GF(2)$ or primitive in the $GF(2^6)$ by 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 $GF(2^6)$ by using the MATLAB-command `gfprimfd`.

d) Determine all irreducible polynomials of the degree $m = 6$ that are no primitive polynomials with a MATLAB-routine.

Exercise 3.2 **Field**

Given are the sets $M_q := \{0, 1, \ldots, q-1\}$ and the 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* of for $GF(3^2)$ (i.e. a table of all elements of this field in exponential representation). Use $D^2 + D + 2$ as a primitive polynomial over $GF(3)$.

Exercise 3.4 **Extension of a binary Field $GF(2^4)$**

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

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

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

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 the length $n = 5$ that is composed of any possible words with the weight $w_H(\mathbf{c}) = 2$. Specify the code $\mathcal{C}$. 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 undetected error for the considered code at a binary symmetric channel. The transition probabilities 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.

d) Check the result of c) by simulating a data transmission scheme in MATLAB and measuring the not detected errors for certain error probabilities P_e of the BSC.
Hint: Choose N code words by random and conduct a BPSK-modulation. Subsequently, the words are superimposed with additive white, Gaussian noise, where its power corresponds to the desired error probability $P_e = 0.5 \cdot \mathrm{erfc}(\sqrt{E_s/N_0})$ of the BSC. After a hard-decision of the single bit, the MLD can be realized at the receiver by a correlation of the received word and all possible code words with subsequent determination of the maximum. Subsequently, the errors have to be counted.

e) Calculate the error probability P_w at soft-decision-ML-decoding for the AWGN-channel.

f) Check the results of e) with the help of simulations in the range $-2\ \mathrm{dB} \leq E_s/N_0 \leq 6\ \mathrm{dB}$. Compare the obtained error rates with the uncoded case.
Hint: You can use the same transmission scheme as in item d). But this time, the hard-decision has to be conducted after the ML-decoding.

3.2 Distance properties of block codes

Exercise 3.6 **Error correction**

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

a) Determine the maximal 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.

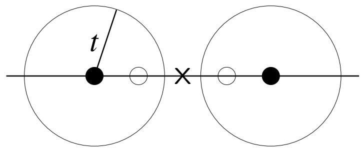


Fig. 2: Example of a Code with $d_{\mathrm{min}} = 4$

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 at the transmission over a disturbed channel.

Exercise 3.7 **Sphere-packing bound (Hamming-Schranke)**

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

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

b) A binary code $\mathcal{C}$ 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, if a binary code with the parameters $n = 23, k = 12, d_{min} = 7$ can exist.

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

3.5 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 degree 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 which connection is between the minimal distance of a code and the number of linear independent columns of the parity check matrix $\mathbf{H}$ by means of this example.

Exercise 3.9 **Expansion, shortening, and puncturing of codes**

a) Given is the systematical $(7, 4, 3)$-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 $\mathbf{H}_S$ and note the result from 3.8c.

b) Shortening a code means the decrease of the cardinality of the field of code words, i.e. information bits are cancelled. Shorten the Hamming code from above to the half of the code words and state the generator matrix $\mathbf{G}_K$ and the parity check matrix $\mathbf{H}_K$ for the systematic case. What minimal distance does the shortened code have?

c) Puncturing a code means gating out code bits which serves for increasing the code rate. Puncture the Hamming code from above to the rate $R_c = 2/3$. What minimal distance does the new code have?

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.

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 greatest 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**

a) Write a MATLAB-programm which codes and again decodes a certain number of input data bits. Besides it shall be possible to insert errors before the decoding. 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.

b) Extend the MATLABprogram for taking up bit error curves in the range $0 : 20$ dB.

3.6 Cyclic Codes

Exercise 3.12 **Polynomial multiplication**

Given are the 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 nonrecursive 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 the 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 systematical 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 an 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 the 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) Generate the generator polynomial for a CRC code of the length $n = 15$.

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

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

Exercise 3.18 **Reed-Solomon-codes**

a) A RS-code in the $GF(2^3)$ that can correct $t = 1$ error shall be generated. Determine the parameters k, n and R_c and state the maximal length of a correctable error in bit.

b) Give the generator polynomial $g(D)$ of the Reed-Solomon-code. Use the commands `rsgenpoly` resp. 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 does the position of the error affect on the decoding result?

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

e) The word $\mathbf{y} = (110\ 010\ 111\ 111\ 001\ 010\ 010)$ is received. Determine the number of errors, corrected code and the transmitted message (correction with `rsdec(rec_code,n,k,genpoly)`).

4 Convolution codes

4.1 Fundamental principles

Exercise 4.1 **Convolution code**

Given is a convolution code with the code rate $R = 1/3$, 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 chart in the case of the under a) given input sequence.

c) Sketch the state diagram of the encoder.

d) Determine the corresponding free distance d_f.

4.2 Characterization of convolution codes

Exercise 4.2 **Catastrophic codes**

Given is the convolution code with the generator polynomial $g(D) = (1 + D^2, 1 + D)$. Show that this is a catastrophic code and explain the consequences.

4.3 Optimal decoding with Viterbi-algorithm

Exercise 4.3 **Viterbi-decoding**

Given is a convolution code with $g_0(D) = 1 + D + D^2$ and $g_1(D) = 1 + D^2$, where a terminated code shall be used.

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

b) Conduct the Viterbi-decoding respectively 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 $y_2 = (11\ 11\ 10\ 01\ 10\ 11)$ and describe the differences.

c) Check the results with the help of a MATLAB-program.

Define the convolution 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,length(c)/n,1)`.

Decode now the sequences `y_1` and `y_2`.

Exercise 4.4 **Viterbi-decoding with puncturing**

Given is a convolution code with $g_0(D) = 1 + D + D^2$ and $g_1(D) = 1 + D^2$, out of which shall be generated a punctured code by puncturing with the scheme

$$\mathbf{P}_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

a) Determine the code rate of the punctured code.

b) Conduct the Viterbi-decoding in the case of the undisturbed receiving sequence $y = (1\ 1\ 0\ 0\ 0\ 1\ 0\ 1)$ (pay attention to the puncturing!).

Exercise 4.5 **Coding and decoding of a RSC code**

a) We now consider the recursive systematic convolution code with the generator polynomials $\tilde{g}_0(D) = 1$ and $\tilde{g}_1(D) = (1 + D + D^3)/(1 + D + D^2 + D^3)$. Generate the Trellis diagram of the code with the help of the MATLAB-command `make_trellis([11;15],2)`.

b) Conduct a coding for the input sequence $u(\ell) = (1\ 1\ 0\ 1\ 1)$. The coder 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?

c) Now the decoding of convolution codes with the help of the Viterbi-algorithm shall be considered. For the present the sequence $u(\ell) = (1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0)$ has to be coded (with termination), modulated with BPSK and subsequently superposed by Gaussian distributed noise. Choose a signal-to-noise ratio of $E_b/N_0 = 4$ dB. With the help of the program `viterbi` the decoding now can be made. By setting the parameter `demo=1` the sequence of the decoding is represented graphically by means of the Trellis diagram. What's striking concerning the error distribution if the Trellis is considered as not terminated?

d) Now the influence of the error structure at the decoder input shall be examined. Therefor specifically add four errors, that you once arrange bundled and another time distribute in a block, to the coded and BPSK-modulated sequence. How does the decoding behave in both cases?

Exercise 4.6 **Investigation to Viterbi-decoding**

a) Simulate a data transmission system with the convolution code from exercise 4.5, a BPSK-modulation, an AWGN-channel and a Viterbi-decoder. The block length of the terminated convolution code shall be $L = 100$ bits. Decode the convolution code with the decision depths ($K_1 = 10$, $K_2 = 15$, $K_3 = 20$, $K_4 = 30$ und $K_5 = 50$). The signal-to-noise ratio shall be $E_b/N_0 = 4$ dB. What influence does the decision depth have on the bit error rate?

b) Now puncture the convolution code to the rate $R_c = 3/4$ and repeat item a). What about the decision depths now?

c) Conduct simulations for an unknown final state. Evaluate the distribution of the decoding errors at the output. What's striking?

Exercise 4.7 **Simulation of a convolution-coder and -decoder**

Generate a MATLAB-program that codes, BPSK-modulates, transmits over an AWGN-channel and subsequently hard decodes an information sequence u of the length $k = 48$ with the terminated convolution code $g = (5, 7)$. Take with this program the bit error 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.

Therefor 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,10)
```