Channel Coding I

Solutions

– 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 April 4, 2019

1 Introduction

Solution of exercise 1.1 **Design of a discrete channel**

Item a)
Relative to the hard-decision, the decision thresholds shall lie in the middle of two adjacent symbols, therefore at -2, 0 and +2. The several classes then correspond to the channel output values Y_μ like in **figure 3**.

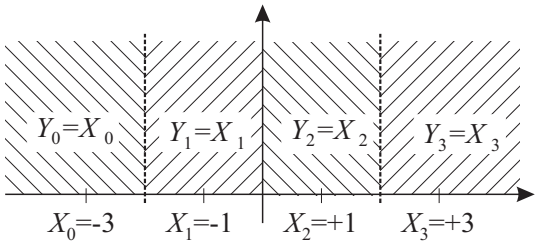

Fig. 3: Hard-decision at quaternary input signal and AWGN channel

The transition probabilities $\Pr\{Y_\mu|X_\nu\}$ can now be calculated in the following way. For the transmitting symbol $X_0 = -3$ the Gaussian distribution $p_n(\xi)$ of the AWGN channel is shifted by X_0. The probability of the symbol X_0 being falsely detected as X_1 then results from the area under the shifted probability density function $p_n(\xi - X_0)$ between -2 and 0

$$\Pr\{Y_1 \mid X_0\} = \int_{-2}^{0} \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{(\xi+3)^2}{2\sigma_n^2}\right) d\xi \; .$$

With the substitution $\zeta = \frac{\xi+3}{\sqrt{2}\sigma_n}$ the relation $d\xi = \sqrt{2}\sigma_n d\zeta$ follows and $\Pr\{Y_1 \mid X_0\}$ is given by (with $\sigma_n = 1$)

$$\begin{aligned} \Pr\{Y_1 \mid X_0\} &= \frac{1}{\sqrt{\pi}} \int_{1/\sqrt{2}\sigma_n}^{3/\sqrt{2}\sigma_n} e^{-\zeta^2} d\zeta = \frac{1}{2}\left[\mathrm{erf}\left(\sqrt{4.5}\right) - \mathrm{erf}\left(\sqrt{0.5}\right)\right] \\ &= \frac{1}{2}\left[\mathrm{erfc}\left(\frac{1}{\sqrt{2}}\right) - \mathrm{erfc}\left(\frac{3}{\sqrt{2}}\right)\right] = 0.1573 \; . \end{aligned}$$

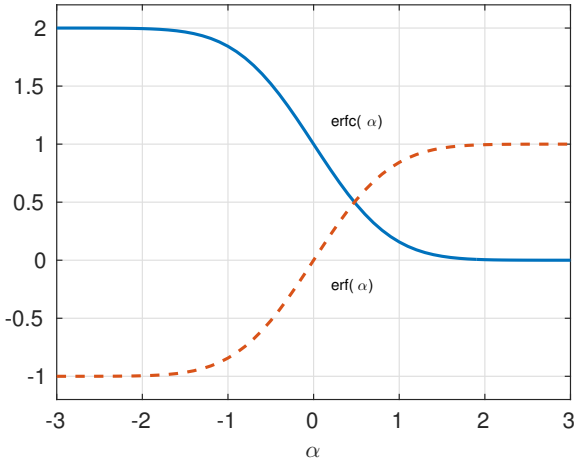

Fig. 4: $\mathrm{erf}(\alpha)$ and $\mathrm{erfc}(\alpha)$

Hint: The Gaussian error function resp. the complementary Gaussian error function are defined according to

eq. (1.20) as

$$\operatorname{erf}(\alpha) = \frac{2}{\sqrt{\pi}} \int_0^{\alpha} e^{-\zeta^2} d\zeta \qquad \operatorname{erfc}(\alpha) = 1 - \operatorname{erf}(\alpha) = \frac{2}{\sqrt{\pi}} \int_{\alpha}^{\infty} e^{-\zeta^2} d\zeta \tag{1}$$

with $\operatorname{erf}(\infty) = 1$ and $\operatorname{erfc}(-\infty) = 2$. The general relation $\sigma_n^2 \neq 1$, $\mu \neq 0$ is:

$$\frac{1}{\sqrt{2\pi\sigma_n^2}} \int_{\alpha}^{\infty} \exp\left(-\frac{(\xi-\mu)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2} \operatorname{erfc}\left(\frac{\alpha-\mu}{\sqrt{2}\sigma_n}\right) \tag{2}$$

The remaining transition probabilities are calculated in the same way:

$$\begin{aligned}
\Pr\{Y_0 \mid X_0\} &= \int_{-\infty}^{-2} \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{(\xi+3)^2}{2\sigma_n^2}\right) d\xi = 1 - \int_{-2}^{\infty} \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{(\xi+3)^2}{2\sigma_n^2}\right) d\xi \\
&= 1 - \frac{1}{2} \operatorname{erfc}\left(\frac{1}{\sqrt{2}}\right) = 0.8413 \\
\Pr\{Y_2 \mid X_0\} &= \int_{0}^{2} \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{(\xi+3)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2}\left[\operatorname{erfc}\left(\frac{3}{\sqrt{2}}\right) - \operatorname{erfc}\left(\frac{5}{\sqrt{2}}\right)\right] = 0.0013 \\
\Pr\{Y_3 \mid X_0\} &= \int_{2}^{\infty} \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{(\xi+3)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2} \operatorname{erfc}\left(\frac{5}{\sqrt{2}}\right) = 2.87 \cdot 10^{-7}
\end{aligned}$$

and the transition probabilities $\Pr\{Y_\mu \mid X_1\}$ are

$$\begin{aligned}
\Pr\{Y_0 \mid X_1\} &= \int_{-\infty}^{-2} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(\xi+1)^2}{2\sigma_n^2}\right) d\xi = 1 - \frac{1}{2} \operatorname{erfc}\left(\frac{-1}{\sqrt{2}}\right) = 0.1587 \\
\Pr\{Y_1 \mid X_1\} &= \int_{-2}^{0} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(\xi+1)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2}\left[\operatorname{erfc}\left(\frac{-1}{\sqrt{2}}\right) - \operatorname{erfc}\left(\frac{1}{\sqrt{2}}\right)\right] = 0.6827 \\
\Pr\{Y_2 \mid X_1\} &= \int_{0}^{2} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(\xi+1)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2}\left[\operatorname{erfc}\left(\frac{1}{\sqrt{2}}\right) - \operatorname{erfc}\left(\frac{3}{\sqrt{2}}\right)\right] = 0.1573 \\
\Pr\{Y_3 \mid X_1\} &= \int_{2}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(\xi+1)^2}{2\sigma_n^2}\right) d\xi = \frac{1}{2} \operatorname{erfc}\left(\frac{3}{\sqrt{2}}\right) = 0.0013
\end{aligned}$$

The other transition probabilities can be determined in the same way, therefore the resulting values follow:

$\Pr\{Y_\mu \mid X_\nu\}$	$Y_0 = -3$	$Y_1 = -1$	$Y_2 = +1$	$Y_3 = +3$
$X_0 = -3$	0.8413	0.1573	0.0013	2.87e-7
$X_1 = -1$	0.1587	0.6827	0.1573	0.0013
$X_2 = +1$	0.0013	0.1573	0.6827	0.1587
$X_3 = +3$	2.87e-7	0.0013	0.1573	0.8413

You can see by the main diagonal that the probability for a correct decision is always the greatest where the inner symbols X_1 and X_2 have a greater error probability. The reason is the possibility of being mixed up with their left as well as their right neighbor while the outer symbols are susceptible to errors just in one side. The more two symbols are distant the smaller is their transition probability. The recognizable symmetries are directly explained by figure 3.

Item b)
A simple check of the results consists in building the sum of all rows. The sum has to result in one according to

$$\sum_{Y_\mu \in \mathcal{A}_{out}} \Pr\{Y_\mu \mid X_\nu\} = \sum_{Y_\mu \in \mathcal{A}_{out}} \frac{\Pr\{X_\nu, Y_\mu\}}{\Pr\{X_\nu\}} = 1$$

because for each hypothetic transmitting symbol appears any output symbol with absolute assurance.

But pay attention: This is not true for the summation of all columns!

$$\sum_{X_\nu \in \mathcal{A}_{in}} \Pr\{Y_\mu \mid X_\nu\} = \sum_{X_\nu \in \mathcal{A}_{in}} \frac{\Pr\{X_\nu, Y_\mu\}}{\Pr\{X_\nu\}} \neq 1$$

Item c)
You get the joint probabilities $\Pr\{X_\nu, Y_\mu\}$ by multiplying the transition probabilities $\Pr\{Y_\mu|X_\nu\}$ with the occurrence probabilities $\Pr\{X_\nu\}$ of the transmitting symbols. They are summarized for $\Pr\{X_\nu\} = 0.25$ in the following table.

$\Pr\{X_\nu, Y_\mu\}$	$Y_0 = -3$	$Y_1 = -1$	$Y_2 = +1$	$Y_3 = +3$
$X_0 = -3$	0.2103	0.0393	0.0003	7.17e-8
$X_1 = -1$	0.0397	0.1707	0.0393	0.0003
$X_2 = +1$	0.0003	0.0393	0.1707	0.0397
$X_3 = +3$	7.17e-8	0.0003	0.0393	0.2103

Item d)
Probabilities of the received symbols is given by

$$\Pr\{Y_\mu\} = \sum_{X_\nu \in \mathcal{A}_{in}} \Pr\{X_\nu, Y_\mu\} \; .$$

We get

	$Y_0 = -3$	$Y_1 = -1$	$Y_2 = +1$	$Y_3 = +3$
$\Pr\{Y_\mu\}$	0.2503	0.2497	0.2497	0.2503

Due to the specific statistics of the channel the output symbols occur with different probabilities although the input symbols are equally distributed.

Item e)
Important for judging the transmission quality of a channel is the error probability for a given input alphabet. An error occurs unless the transmitted symbol is detected. The probability for this case is

$$P_e\{X_\nu\} = \sum_{\substack{Y_\mu \in \mathcal{A}_{out} \\ Y_\mu \neq X_\nu}} \Pr\{Y_\mu \mid X_\nu\} = 1 - \Pr\{Y_\nu \mid X_\nu\} \; .$$

We get the following values.

	$X_0 = -3$	$X_1 = -1$	$X_2 = +1$	$X_3 = +3$
$P_e\{X_\nu\}$	0.1600	0.3160	0.3160	0.1600

The error probability of the two inner symbols is about two times as big as that of the outer symbols because of the above discussed arrangement of the symbols. As mean overall error probability we get

$$P_e = \sum_{\nu=0}^{3} P_e\{X_\nu\} \cdot \Pr\{X_\nu\} = 0.238 \; .$$

Solution of exercise 1.2 **Statistics of the discrete channel**

In **figure 5** the remaining probabilities were added. They result from the equations

$$\sum_{X_\nu \in \mathcal{A}_{in}} \Pr\{X_\nu\} = 1 \qquad \Pr\{X_\nu, Y_\mu\} = \Pr\{Y_\mu \mid X_\nu\} \cdot \Pr\{X_\nu\} \qquad \Pr\{Y_\mu\} = \sum_{X_\nu \in \mathcal{A}_{in}} \Pr\{X_\nu, Y_\mu\}$$

according to eq. (1.2), eq. (1.3) and eq. (1.6).

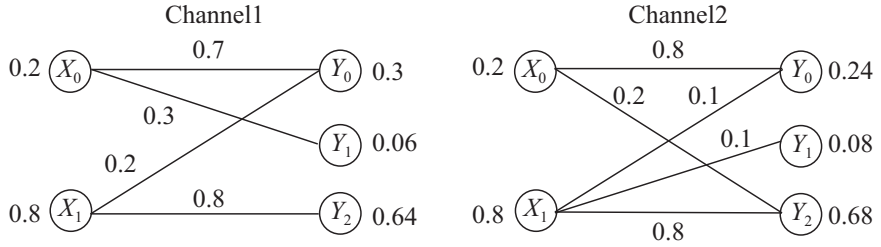

Fig. 5: Discrete channel models

Solution of exercise 1.3 **Binary symmetric channel (BSC)**

Item a)
The probability that exactly m errors occur at certain positions when a sequence of length n is transmitted over a BSC is given by (according to eq. (1.27))

$$\Pr\{m \text{ bits of } n \text{ incorrect}\} = P_e^m \cdot (1 - P_e)^{n-m} \; .$$

In this case exactly $m = 2$ errors occur and 5 bits are correct in a sequence of length $n = 7$. Accordingly, the desired probability is

$$\Pr\{2 \text{ bits of 7 incorrect}\} = P_e^2 \cdot (1 - P_e)^{7-2} = 0.01^2 \cdot 0.99^5 = 9.5099 \cdot 10^{-5} \approx 10^{-4} \; .$$

Item b)
The probability of m errors occurring in a sequence of length n can be calculated by eq. (1.28):

$$P_f(m) = \Pr\{m \text{ errors in a sequence of length } n\} = \binom{n}{m} \cdot P_e^m \cdot (1 - P_e)^{n-m} \; ,$$

where

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

is the number of possibilities of choosing m elements out of n different elements without consideration of the succession (*combinations*).

Item c)
Method of approach 1: The probability of more than 2 errors occurring results from the sum of error probabilities for $3, \ldots, 31$ errors:

$$P_f(m > 2) = \sum_{r=3}^{31} \binom{31}{r} \cdot P_e^r \cdot (1 - P_e)^{31-r} \approx \binom{31}{3} \cdot P_e^3 \cdot (1 - P_e)^{31-3} \approx 0,0034$$

Method of approach 2: By a simple consideration the calculation of the probability can be simplified. Because of the completeness property of the probabilities:

$$P_f(m > 2) = \text{Pr}\{\text{more than 2 errors}\} = 1 - P_f(m = 0) - P_f(m = 1) - P_f(m = 2) \; .$$

The single error probabilities are calculated as

$$\begin{aligned} P_f(m = 0) &= \binom{31}{0} \cdot 0.01^0 \cdot 0.99^{31} = 1 \cdot 1 \cdot 0.99^{31} \approx 0.7323 \\ P_f(m = 1) &= \binom{31}{1} \cdot 0.01^1 \cdot 0.99^{30} = 31 \cdot 0.01^1 \cdot 0.99^{30} \approx 0.2293 \\ P_f(m = 2) &= \binom{31}{2} \cdot 0.01^2 \cdot 0.99^{29} = 465 \cdot 0.01^2 \cdot 0.99^{29} \approx 0.0347 \end{aligned}$$

and for the desired probability follows

$$P_f(m > 2) = 1 - 1 \cdot 0.99^{31} - 31 \cdot 0.99^{30} \cdot 0.01^1 - 465 \cdot 0.99^{29} \cdot 0.01^2 \approx 0.0036 \; .$$

Solution of exercise 1.4

Serial concatenation of two BSCs

Because the resulting channel is also symmetric, the consideration of one error case is sufficient for the determination of the error probability. The probability of the transmitting symbol X_0 being mapped to the output symbol Y_1 can be calculated as:

$$\begin{aligned} \text{Pr}\{Y_1 \mid X_0\} &= \text{Pr}\{Y_1 \mid Z_0\} \cdot \text{Pr}\{Z_0 \mid X_0\} + \text{Pr}\{Y_1 \mid Z_1\} \cdot \text{Pr}\{Z_1 \mid X_0\} \\ &= P_{e,2} \cdot (1 - P_{e,1}) + (1 - P_{e,2}) \cdot P_{e,1} \\ &= P_{e,1} + P_{e,2} - 2 \cdot P_{e,1} \cdot P_{e,2} \end{aligned}$$

For the resulting BSC we obtain $P_e = P_{e,1} + P_{e,2} - 2 \cdot P_{e,1} \cdot P_{e,2}$. At consideration of two channels with $P_{e,1} = 0.01$ and $P_{e,2} = 0.02$ it becomes obvious that the resulting BSC with $P_e = 0.01 + 0.02 - 2 \cdot 0.01 \cdot 0.02 = 0.0296 \approx 0.03$ has a considerably greater error probability.

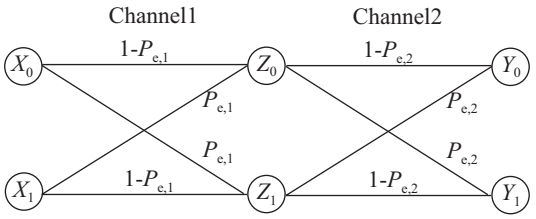

Fig. 6: Serial concatenation of two BSCs

2 Survey of Information Theory

Solution of exercise 2.1 **Entropy**

Item a)
According to eq. (2.2), the mean information content $\mathcal{H}(X_\nu)$ of signal X_ν is determined by

$$\mathcal{H}(X_\nu) = -\text{Pr}\{X_\nu\} \cdot \text{ld}\,\text{Pr}\{X_\nu\} \tag{3}$$

The maximum of $\mathcal{H}(X_\nu)$ results from the derivation being equal to zero:

$$\frac{\partial \mathcal{H}(X_\nu)}{\partial \text{Pr}\{X_\nu\}} \stackrel{!}{=} 0$$

With application of the relation $\text{ld}\,x = \ln x / \ln 2$ and $d \ln x/dx = 1/x$ follows

$$\begin{aligned}
\frac{\partial \mathcal{H}(X_\nu)}{\partial \text{Pr}\{X_\nu\}} &= -\frac{\partial}{\partial \text{Pr}\{X_\nu\}} \text{Pr}\{X_\nu\} \cdot \text{ld}\,\text{Pr}\{X_\nu\} \\
&= -\text{ld}\,\text{Pr}\{X_\nu\} - \frac{\text{Pr}\{X_\nu\}}{\ln 2} \cdot \frac{\partial}{\partial \text{Pr}\{X_\nu\}} \ln \text{Pr}\{X_\nu\} \\
&= -\text{ld}\,\text{Pr}\{X_\nu\} - \frac{\text{Pr}\{X_\nu\}}{\ln 2} \cdot \frac{1}{\text{Pr}\{X_\nu\}} \\
&= -\text{ld}\,\text{Pr}\{X_\nu\} - \frac{1}{\ln 2} \\
&\stackrel{!}{=} 0
\end{aligned}$$

For $\text{Pr}\{X_\nu\} = P_{max}$ then follows

$$\text{Pr}\{X_\nu\} = P_{max} = 2^{-1/\ln 2} = 0.3679 \tag{4}$$

and for the maximal entropy

$$\mathcal{H}(X_\nu)_{max} = -P_{max} \cdot \text{ld}\,P_{max} = -0.3679 \cdot \text{ld}\,0.3679 = 0.531 \tag{5}$$

You get the same result with MATLAB by numerical calculation of the partial entropy, as shown in **figure 7**.

Item b)
Corresponding to the task only the following five events can occur:

X_1	X_2	X_3
0	0	0
0	0	1
0	1	1
1	0	1
1	1	1

1. $\mathcal{H}(X_1)$ describes the entropy of the symbol X_1 and is calculated as in eq. (2.3) to:
   $\mathcal{H}(X_1) = -\sum \text{Pr}\{X_1\} \cdot \text{ld}\,\text{Pr}\{X_1\} = -\frac{3}{5}\,\text{ld}\,\frac{3}{5} - \frac{2}{5}\,\text{ld}\,\frac{2}{5} = 0.971$
   Because X_1 is not equally distributed, its entropy is not maximal and therefore less than one.
2. $\mathcal{H}(X_2) = -\sum \text{Pr}\{X_2\} \cdot \text{ld}\,\text{Pr}\{X_2\} = -\frac{3}{5}\,\text{ld}\,\frac{3}{5} - \frac{2}{5}\,\text{ld}\,\frac{2}{5} = 0.971$
3. $\mathcal{H}(X_3) = -\sum \text{Pr}\{X_3\} \cdot \text{ld}\,\text{Pr}\{X_3\} = -\frac{1}{5}\,\text{ld}\,\frac{1}{5} - \frac{4}{5}\,\text{ld}\,\frac{4}{5} = 0.722$
4. The joint entropy $\mathcal{H}(X_1, X_2)$ describes the average information content of the (super)symbol X_1X_2:
   $\mathcal{H}(X_1, X_2) = -\sum \text{Pr}\{X_1, X_2\} \cdot \text{ld}\,\text{Pr}\{X_1, X_2\} = -\frac{2}{5}\,\text{ld}\,\frac{2}{5} - \frac{1}{5}\,\text{ld}\,\frac{1}{5} - \frac{1}{5}\,\text{ld}\,\frac{1}{5} - \frac{1}{5}\,\text{ld}\,\frac{1}{5} = 1.922$

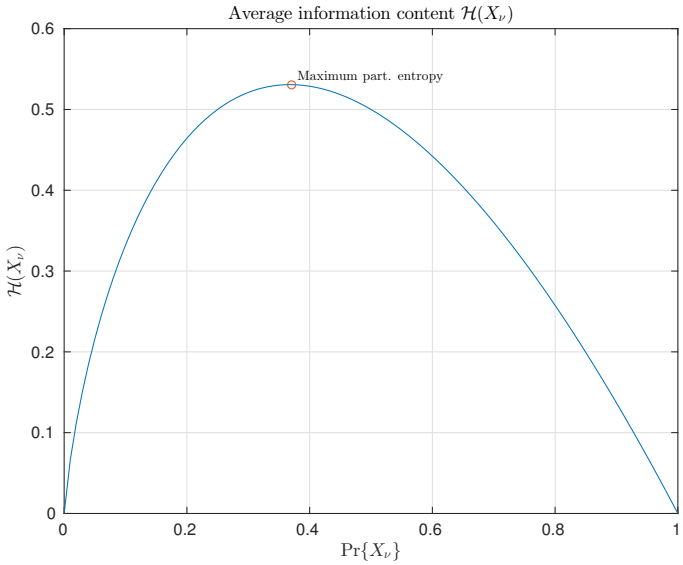

Fig. 7: Mean information content $\mathcal{H}(X_\nu)$ in dependence on the symbol probability $\Pr\{X_\nu\}$

5. $\mathcal{H}(X_1, X_2, X_3) = 5 \cdot \left(-\frac{1}{5} \operatorname{ld} \frac{1}{5}\right) = 2.322$
6. The conditional entropy $\mathcal{H}(X_2|X_1)$ describes the information content of X_2, if X_1 is already known:
   $\mathcal{H}(X_2|X_1) = \mathcal{H}(X_1, X_2) - \mathcal{H}(X_1) = 1.9219 - 0.971 = 0.9509$
7. The conditional entropy $\mathcal{H}(X_2|X_1 = 0)$ describes the information content of X_2, if $X_1 = 0$ is already known:
   $\mathcal{H}(X_2|X_1 = 0) = -\frac{2}{3} \operatorname{ld} \frac{2}{3} - \frac{1}{3} \operatorname{ld} \frac{1}{3} = 0.918$
8. The conditional entropy $\mathcal{H}(X_2|X_1 = 1)$ describes the information content of X_2, if $X_1 = 1$ is already known:
   $\mathcal{H}(X_2|X_1 = 1) = -\frac{1}{2} \operatorname{ld} \frac{1}{2} - \frac{1}{2} \operatorname{ld} \frac{1}{2} = 1$
   $\mathcal{H}(X_2|X_1 = 1) = 1$ means, that due to $X_1 = 1$ there isn't any knowledge about X_2 and consequently the symbol has the maximal entropy.
9. The conditional entropy $\mathcal{H}(X_3|X_1, X_2)$ describes the information content of X_3, if X_1 and X_2 are already known:
   $\mathcal{H}(X_3|X_1, X_2) = \mathcal{H}(X_1, X_2, X_3) - \mathcal{H}(X_1, X_2) = 2.3219 - 1.9219 = 0.4$

Solution of exercise 2.2

Channel capacity of a discrete memoryless channel

The channel capacity follows with the help of eq. (2.20)

$$C = \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu|X_\nu\} \cdot \Pr\{X_\nu\} \cdot \operatorname{ld} \frac{\Pr\{Y_\mu|X_\nu\}}{\Pr\{Y_\mu\}} \tag{6}$$

As the input alphabet with $\Pr\{X_\nu\} = 1/3$ is equally distributed and it is a symmetric channel, also the output alphabet is equally distributed with $\Pr\{Y_\mu\} = 1/3$. For the channel capacity then follows:

$$\begin{aligned} C &= \frac{1}{3} \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu|X_\nu\} \cdot \operatorname{ld}\left(3 \cdot \Pr\{Y_\mu|X_\nu\}\right) \\ &= \frac{1}{3}\left[3\,\frac{1}{2} \operatorname{ld} \frac{3}{2} + 3\,\frac{1}{3} \operatorname{ld} \frac{3}{3} + 3\,\frac{1}{6} \operatorname{ld} \frac{3}{6}\right] \\ &= \frac{1}{3}\left[\frac{3}{2} \operatorname{ld} \frac{3}{2} + \operatorname{ld} 1 + \frac{1}{2} \operatorname{ld} \frac{1}{2}\right] = 0.126 \end{aligned}$$

Solution of exercise 2.3 **Channel capacity of the BSC**

Item a)
As the channel is symmetric and the input symbols are equally distributed, the output symbols are also equally distributed ($\Pr\{Y_0\} = \Pr\{Y_1\} = 0.5$).

The channel capacity is calculated according to eq. (2.21) as

$$C = \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu|X_\nu\} \cdot \Pr\{X_\nu\} \cdot \mathrm{ld} \frac{\Pr\{Y_\mu|X_\nu\}}{\Pr\{Y_\mu\}}.$$

The transition probabilities $\Pr\{Y_\mu|X_\nu\}$ for the BSC are:

$$\Pr\{Y_\mu|X_\nu\} = \begin{cases} 1-P_e & y = x \\ P_e & y \neq x \end{cases}$$

So the channel capacity of the BSC is:

$$\begin{aligned}
C^{\mathrm{BSC}} &= \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu|X_\nu\} \cdot \Pr\{X_\nu\} \cdot \mathrm{ld} \frac{\Pr\{Y_\mu|X_\nu\}}{\Pr\{Y_\mu\}} \\
&= \Pr\{Y_0|X_0\} \cdot \Pr\{X_0\} \cdot \mathrm{ld} \frac{\Pr\{Y_0|X_0\}}{\Pr\{Y_0\}} + \Pr\{Y_1|X_0\} \cdot \Pr\{X_0\} \cdot \mathrm{ld} \frac{\Pr\{Y_1|X_0\}}{\Pr\{Y_1\}} \\
&\quad + \Pr\{Y_0|X_1\} \cdot \Pr\{X_1\} \cdot \mathrm{ld} \frac{\Pr\{Y_0|X_1\}}{\Pr\{Y_0\}} + \Pr\{Y_1|X_1\} \cdot \Pr\{X_1\} \cdot \mathrm{ld} \frac{\Pr\{Y_1|X_1\}}{\Pr\{Y_1\}} \\
&= (1-P_e) \cdot 0.5 \cdot \mathrm{ld} \frac{1-P_e}{0.5} + P_e \cdot 0.5 \cdot \mathrm{ld} \frac{P_e}{0.5} + P_e \cdot 0.5 \cdot \mathrm{ld} \frac{P_e}{0.5} + (1-P_e) \cdot 0.5 \cdot \mathrm{ld} \frac{1-P_e}{0.5} \\
&= \mathrm{ld} \frac{1-P_e}{0.5} \cdot (0.5 - 0.5 \cdot P_e + 0.5 - 0.5 \cdot P_e) + \mathrm{ld} \frac{P_e}{0.5} \cdot (0.5 \cdot P_e + 0.5 \cdot P_e) \\
&= \mathrm{ld}\ [2\,(1-P_e)] \cdot (1-P_e) + \mathrm{ld}\,(2\,P_e) \cdot P_e \\
&= [\mathrm{ld}\,2 + \mathrm{ld}\,(1-P_e)] \cdot (1-P_e) + [\mathrm{ld}\,2 + \mathrm{ld}\,P_e] \cdot P_e \\
&= [1 + \mathrm{ld}\,(1-P_e)] \cdot (1-P_e) + [1 + \mathrm{ld}\,P_e] \cdot P_e \\
&= 1 - P_e + (1-P_e)\,\mathrm{ld}\,(1-P_e) + P_e + P_e\,\mathrm{ld}\,P_e \\
&= 1 + (1-P_e) \cdot \mathrm{ld}\,(1-P_e) + P_e \cdot \mathrm{ld}\,P_e
\end{aligned}$$

You get the same result with the help of eq. (2.14):

$$\begin{aligned}
C^{\mathrm{BSC}} &= \mathcal{H}(X) + \mathcal{H}(Y) - \mathcal{H}(X,Y) \\
&= -\sum_{\nu=0}^{1} \Pr\{X_\nu\} \cdot \mathrm{ld}\,\Pr\{X_\nu\} - \sum_{\mu=0}^{1} \Pr\{Y_\mu\} \cdot \mathrm{ld}\,\Pr\{Y_\mu\} + \sum_{\nu=0}^{1} \sum_{\mu=0}^{1} \Pr\{X_\nu, Y_\mu\} \cdot \mathrm{ld}\,\Pr\{X_\nu, Y_\mu\} \\
&= 1 + (1-P_e) \cdot \mathrm{ld}\,(1-P_e) + P_e \cdot \mathrm{ld}\,P_e\ . \qquad (7)
\end{aligned}$$

For the extreme cases of $P_e = 0$ and $P_e = 1$ the channel capacity achieves the value of 1 bit/s/Hz, consequently an error-free transmission is possible without any channel coding. On the other hand, $C = 0$ for $P_e = 0.5$, i.e., no reliable transmission is possible as the output symbols occur quite randomly.

Item b)
It applies:

$$\mathcal{I}(X;Y) = \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu|X_\nu\} \cdot \Pr\{X_\nu\} \cdot \mathrm{ld} \frac{\Pr\{Y_\mu|X_\nu\}}{\Pr\{Y_\mu\}}$$

Because it is an asymmetric channel the occurrence probability of the receiving symbols has to be determined. With

$$\Pr\{Y_\mu\} = \sum_{\nu=0}^{1} \Pr\{X_\nu, Y_\mu\} = \sum_{\nu=0}^{1} \Pr\{Y_\mu|X_\nu\} \cdot \Pr\{X_\nu\}$$

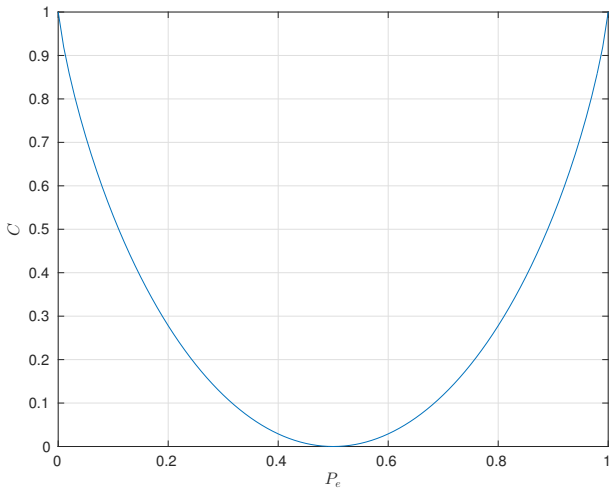

Fig. 8: Channel capacity of the BSC for equiprobable input symbols in dependence on the error probability P_e

$\Pr\{Y_0\}$ and $\Pr\{Y_1\}$ are given by:

$$\begin{aligned}\Pr\{Y_0\} &= \Pr\{Y_0|X_0\}\cdot\Pr\{X_0\}+\Pr\{Y_0|X_1\}\cdot\Pr\{X_1\} = (1-P_{e,0})\cdot\Pr\{X_0\}+P_{e,1}\cdot\Pr\{X_1\}\\ \Pr\{Y_1\} &= \Pr\{Y_1|X_0\}\cdot\Pr\{X_0\}+\Pr\{Y_1|X_1\}\cdot\Pr\{X_1\} = P_{e,0}\cdot\Pr\{X_0\}+(1-P_{e,1})\cdot\Pr\{X_1\}\,.\end{aligned}$$

Accordingly, we can write in matrix notation:

$$\begin{aligned}\begin{pmatrix}\Pr\{Y_0\}\\ \Pr\{Y_1\}\end{pmatrix} &= \begin{pmatrix}\Pr\{Y_0|X_0\} & \Pr\{Y_0|X_1\}\\ \Pr\{Y_1|X_0\} & \Pr\{Y_1|X_1\}\end{pmatrix}\cdot\begin{pmatrix}\Pr\{X_0\}\\ \Pr\{X_1\}\end{pmatrix}\\ &= \begin{pmatrix}1-P_{e,0} & P_{e,1}\\ P_{e,0} & 1-P_{e,1}\end{pmatrix}\cdot\begin{pmatrix}\Pr\{X_0\}\\ \Pr\{X_1\}\end{pmatrix}\end{aligned}$$

Figure 9 shows the (input-output)mutual information of a symmetric channel $P_{e,0} = P_{e,1}$ for several error probabilities in dependence on the occurrence probability $\Pr\{X_0\}$. The mutual information decreases with increasing error probability P_e.

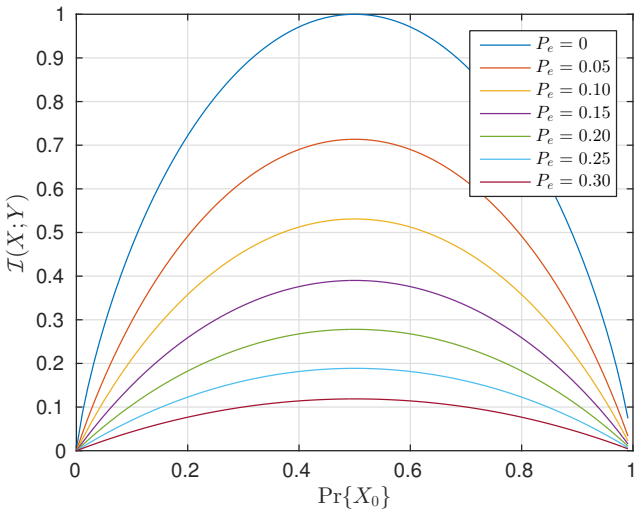

Fig. 9: Mutual information of the binary symmetric channel ($P_{e,0} = P_{e,1} = P_e$) for several P_e in dependence on the occurrence probability $\Pr\{X_0\}$

Figure 10a shows the (input-output)mutual information of a binary channel for a varying error probability $P_{e,0}$ and a fixed error probability $P_{e,1} = 0.1$ in dependence on the occurrence probability $\Pr\{X_0\}$. The mutual information

again decreases with increasing error probability P_e but now is not symmetric anymore w.r.t. $\Pr\{X_0\}$. This effect becomes more clear in **figure 10b** with $P_{e,1} = 0.3$.

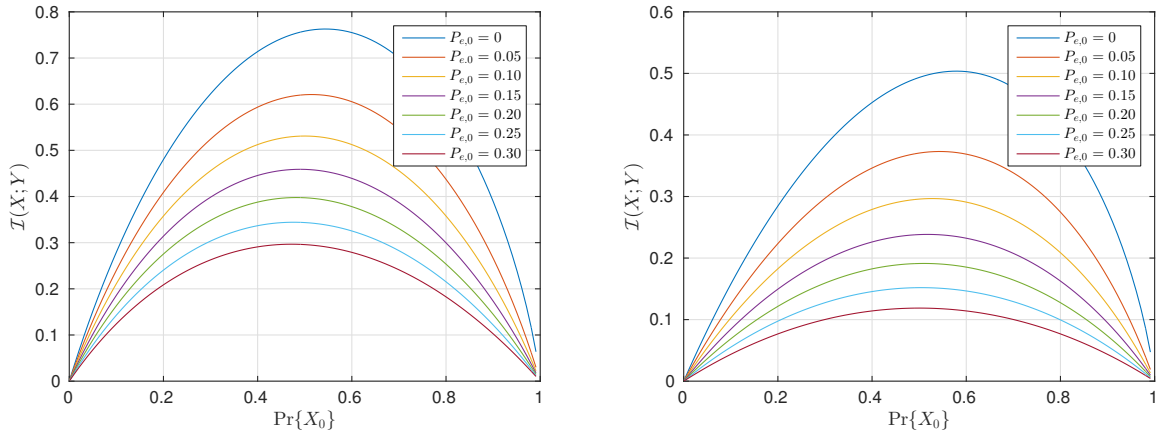

Fig. 10: Mutual information of the binary channel for several $P_{e,0}$ in dependence on the occurrence probability $\Pr\{X_0\}$ for a) $P_{e,1} = 0.1$ and b) $P_{e,1} = 0.3$

Item c)

Figure 11 shows the (input-output)mutual information of the binary symmetric channel for several input statistics $\Pr\{X_0\}$ in dependence on the error probability P_e (cmp. fig. 2.3).

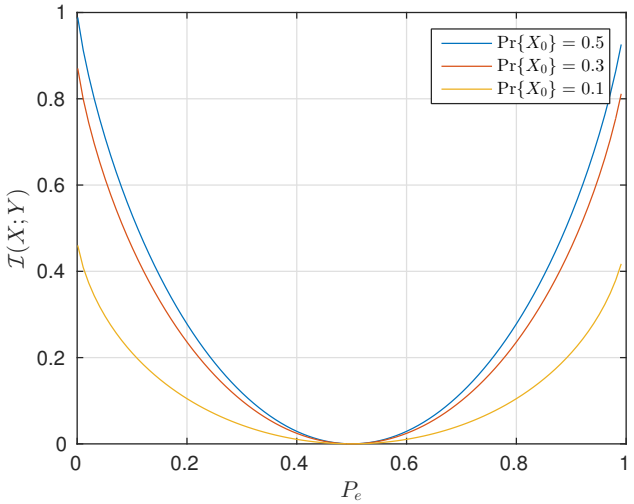

Fig. 11: Mutual information of the binary symmetric channel for several occurrence probabilities $\Pr\{X_0\}$ in dependence on the error probability P_e

Solution of exercise 2.4 **Channel capacity of the AWGNC**

According to eq. (2.26)

$$C = \sup_{p_x(\xi)} [\mathcal{H}(Y) - \mathcal{H}(Y|X)]$$

the channel capacity is determined as the difference of the differential entropies. By using the output distribution

$$p_y(\vartheta) = \frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}}$$

the differential entropy $\mathcal{H}(Y)$ becomes

$$\begin{aligned} \mathcal{H}(Y) &= -\int_{-\infty}^{\infty} p_y(\vartheta) \cdot \mathrm{ld} p_y(\vartheta)\, d\vartheta \\ &= -\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}} \cdot \mathrm{ld}\left[\frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}}\right] d\vartheta\ . \end{aligned} \tag{8}$$

With application of the relation $\mathrm{ld}(x) = \mathrm{ld}(e) \cdot \ln(x)$ the term $\mathrm{ld}(\cdot)$ in (8) can be simplified:

$$\begin{aligned} \mathrm{ld}\left[\frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}}\right] &= \mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) + \mathrm{ld}\left(e^{-\frac{\vartheta^2}{2\sigma_y^2}}\right) \\ &= \mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) + \mathrm{ld}e \cdot \ln\left(e^{-\frac{\vartheta^2}{2\sigma_y^2}}\right) \\ &= \mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) + \mathrm{ld}e \cdot \left(-\frac{\vartheta^2}{2\sigma_y^2}\right) \end{aligned}$$

and for the differential entropy follows:

$$\begin{aligned} \mathcal{H}(Y) &= -\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}} \cdot \left[\mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) + \mathrm{ld}e \cdot \left(-\frac{\vartheta^2}{2\sigma_y^2}\right)\right] d\vartheta \\ &= -\mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) \cdot \underbrace{\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}}\, d\vartheta}_{\int_{-\infty}^{\infty} p_y(\vartheta)\, d\vartheta = 1} - \mathrm{ld}e \cdot \left(-\frac{1}{2\sigma_y^2}\right) \cdot \underbrace{\int_{-\infty}^{\infty} \frac{\vartheta^2}{\sqrt{2\pi\sigma_y^2}} \cdot e^{-\frac{\vartheta^2}{2\sigma_y^2}}\, d\vartheta}_{\int_{-\infty}^{\infty} \vartheta^2 \cdot p_y(\vartheta)\, d\vartheta = \sigma_y^2} \\ &= -\mathrm{ld}\left(\frac{1}{\sqrt{2\pi\sigma_y^2}}\right) + \mathrm{ld}e \cdot \frac{1}{2\sigma_y^2} \cdot \sigma_y^2 = \frac{1}{2}\,\mathrm{ld}\left(2\pi\sigma_y^2\right) + \frac{1}{2}\,\mathrm{ld}e \\ &= \frac{1}{2}\,\mathrm{ld}\left(2\pi e\sigma_y^2\right)\ . \end{aligned}$$

For the irrelevance $\mathcal{H}(Y|X)$ follows analogously:

$$\mathcal{H}(Y|X) = \mathcal{H}(N) = \frac{1}{2}\,\mathrm{ld}\left(2\pi e\sigma_n^2\right)\ ,$$

such that the channel capacity results as the difference of the output entropy and the irrelevance to

$$\begin{aligned} C &= \mathcal{H}(Y) - \mathcal{H}(Y|X) = \frac{1}{2}\,\mathrm{ld}\left(2\pi e\sigma_y^2\right) - \frac{1}{2}\,\mathrm{ld}\left(2\pi e\sigma_n^2\right) \\ &= \frac{1}{2}\,\mathrm{ld}\left(\frac{\sigma_y^2}{\sigma_n^2}\right) = \frac{1}{2}\,\mathrm{ld}\left(\frac{E_s + N_0/2}{N_0/2}\right) \\ &= \frac{1}{2}\,\mathrm{ld}\left(1 + 2\,\frac{E_s}{N_0}\right). \end{aligned}$$

3 Linear Block Codes

3.1 Finite Field Algebra

Solution of exercise 3.1 **Polynomials in the GF(2)**

Item a)
The *communications system toolbox* from MATLAB offers for this exercise the function `gfprimck(a)` with its output carrying the possible values:

$$\texttt{gfprimck(a)} = \begin{cases} +1 & p(D) \text{ is a primitive polynomial} \\ 0 & p(D) \text{ is irreducible, but not primitive} \\ -1 & p(D) \text{ is neither irreducible nor primitive} \end{cases}$$

In our example it yields the value -1, therefore $p(D)$ is neither primitive nor irreducible.

Item b)
As $p(D)$ is not irreducible, there must be polynomials $p_i(D)$ of degree less than $m = 6$, that divide $p(D)$ without rest in the GF(2). As neither '0' nor '1' are zeros, we check $p(D)$ with the polynomial $p_1(D) = 1 + D + D^2$. We get the following result:

$$(D^6 + D^5 + D^4 + D^3 + 1) : (D^2 + D + 1) = D^4 + D + 1$$

Item c)
The primitive polynomials of a Galois field GF(p) can be determined in MATLAB with the command `gfprimfd`. (`gfprimdf` only yields the default primitive polynomials). We get the polynomials

$1 + D + D^6$	$1 + D^5 + D^6$
$1 + D + D^3 + D^4 + D^6$	$1 + D + D^2 + D^5 + D^6$
$1 + D^2 + D^3 + D^5 + D^6$	$1 + D + D^4 + D^5 + D^6$

Item d)
The irreducible but not primitive polynomials can be found by the inquiry `gfprimck` = 0.

$1 + D^3 + D^6$
$1 + D + D^2 + D^4 + D^6$
$1 + D^2 + D^4 + D^5 + D^6$

Solution of exercise 3.2 **Fields**

Item a)
Following, the connection tables for $q = 2, 3, 4, 5, 6$ are given.

$q = 2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$q = 3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$q = 4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$q = 5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$q = 6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Item b)
For $q = 4$ and $q = 6$, the multiplicative inverse does not always exist. As explained in ch. 3.2.1, the Galois fields GF(q) only exist for $q = p^m$, where p is a prime number and m is a natural number. As $q = 6$ cannot be represented as the power of a prime number, a Galois field to the basis $q = 6$ does not exist. For the basis $q = 4 = 2^2$ does exist a Galois field, but it is not a prime field. In ch. 3.2.2, the definition of the Galois fields was therefore completed to the so-called extension fields.

Item c)
For $q = 3$, the primitive element is 2. As for $q = 5$, both 2 and 3 are primitive elements:

2^0	1
2^1	2
2^2	4
2^3	3
2^4	1

3^0	1
3^1	3
3^2	4
3^3	2
3^4	1

The element 4 is not primitive because $4^0 = 1,\ 4^1 = 4,\ 4^2 = 1 \mod 5$.

Solution of exercise 3.3

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

$$p(D) = D^2 + D + 2$$
$$p(\alpha) = 0$$
$$\alpha^2 = 2\alpha + 1$$

$\alpha^{-\infty}$	0
α^0	1
α^1	α
α^2	$2\alpha+1$
α^3	$2\alpha^2+\alpha = 4\alpha+2+\alpha = 2\alpha+2$
α^4	$2\alpha^2+2\alpha = 4\alpha+2+2\alpha = 2$
α^5	2α
α^6	$2\alpha^2 = 4\alpha+2 = \alpha+2$
α^7	$\alpha^2+2\alpha = 2\alpha+1+2\alpha = \alpha+1$
α^8	$\alpha^2+\alpha = 2\alpha+1+\alpha = 1$

Solution of exercise 3.4

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

$$p(D) = D^4 + D + 1$$
$$p(\alpha) = 0 \rightarrow \alpha^4 = \alpha + 1$$

$\alpha^{-\infty}$	0
α^0	1
α^1	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$
α^5	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2$
α^7	$\alpha^4+\alpha^3 = \alpha^3+\alpha+1$
α^8	$\alpha^4+\alpha^2+\alpha = \alpha+1+\alpha^2+\alpha = \alpha^2+1$
α^9	$\alpha^3+\alpha$
α^{10}	$\alpha^4+\alpha^2 = \alpha+1+\alpha^2 = \alpha^2+\alpha+1$
α^{11}	$\alpha^3+\alpha^2+\alpha$
α^{12}	$\alpha^4+\alpha^3+\alpha^2 = \alpha^3+\alpha^2+\alpha+1$
α^{13}	$\alpha^4+\alpha^3+\alpha^2+\alpha = \alpha+1+\alpha^3+\alpha^2+\alpha = \alpha^3+\alpha^2+1$
α^{14}	$\alpha^4+\alpha^3+\alpha = \alpha+1+\alpha^3+\alpha = \alpha^3+1$
α^{15}	$\alpha^4+\alpha = \alpha+1+\alpha = 1$

Item a)

$$\begin{aligned}
p_1(D) &= (D-\alpha)(D-\alpha^2)(D-\alpha^4)(D-\alpha^8) \\
&= (D^2-\alpha^5 D+\alpha^3)(D^2-\alpha^5 D+\alpha^{12}) \quad \text{because} \quad \alpha^5 = \alpha+\alpha^2,\ \alpha^4+\alpha^8 = \alpha^5 \\
&= D^4 - \alpha^5 D^3 + \alpha^{12} D^2 \\
&\quad - \alpha^5 D^3 + \alpha^{10} D^2 - \alpha^2 D \\
&\quad + \alpha^3 D^2 - \alpha^8 D + \alpha^{15} \\
&= D^4 - \underbrace{(\alpha^5+\alpha^5)}_{0} D^3 + \underbrace{(\alpha^{12}+\alpha^{10}+\alpha^3)}_{0} D^2 - \underbrace{(\alpha^2+\alpha^8)}_{1} D + \underbrace{\alpha^{15}}_{1} \\
&= D^4 - D + 1 = D^4 + D + 1
\end{aligned}$$

Item b)

$$
\begin{aligned}
p_2(D) &= (D-\alpha)(D-\alpha^2)(D-\alpha^3)(D-\alpha^4) \\
&= (D^2-\alpha^5 D+\alpha^3)(D^2-\alpha^7 D+\alpha^7) \quad \text{because} \quad \alpha^5=\alpha+\alpha^2,\ \alpha^3+\alpha^4=\alpha^7 \\
&= D^4-\alpha^7 D^3+\alpha^7 D^2 \\
&\quad -\alpha^5 D^3+\alpha^{12} D^2-\alpha^{12} D \\
&\quad +\alpha^3 D^2-\alpha^{10} D+\alpha^{10} \\
&= D^4-(\alpha^7+\alpha^5)D^3+(\alpha^{12}+\alpha^7+\alpha^3)D^2-(\alpha^{12}+\alpha^{10})D+\alpha^{10} \\
&= D^4-\alpha^{13} D^3+\alpha^6 D^2-\alpha^3 D+\alpha^{10} = D^4+\alpha^{13} D^3+\alpha^6 D^2+\alpha^3 D+\alpha^{10}
\end{aligned}
$$

Item c)

$p_1(D)$ has its coefficients in GF(2) and not in GF(2^4).

Solution of exercise 3.5 **2-out-of-5-code**

Item a)
The field of code words consists of exactly $\binom{5}{2}$=10 elements. They are listed in the following table.

index	code words					index	code words				
1	1	1	0	0	0	6	0	1	0	1	0
2	1	0	1	0	0	7	0	1	0	0	1
3	1	0	0	1	0	8	0	0	1	1	0
4	1	0	0	0	1	9	0	0	1	0	1
5	0	1	1	0	0	10	0	0	0	1	1

The code is not linear because for example the modulo 2 addition of the code words $(1\ 1\ 0\ 0\ 0)$ and $(0\ 0\ 0\ 1\ 1)$ results in the word $(1\ 1\ 0\ 1\ 1)$ which is not an element of the field of code words. Hence, the property of being closed is violated.

Item b)
Because of the non-linearity of the code, the all-zero word cannot be used as reference for determination of the distance properties (in this case it isn't an element of the field of code words anyway). Rather the distances of all pairs of code words have to be determined. The solution of this exercise can quickly be finished by a small MATLAB routine. We get the following table.

index	1	2	3	4	5	6	7	8	9	10
1	0	2	2	2	2	2	2	4	4	4
2	2	0	2	2	2	4	4	2	2	4
3	2	2	0	2	4	2	4	2	4	2
4	2	2	2	0	4	4	2	4	2	2
5	2	2	4	4	0	2	2	2	2	4
6	2	4	2	4	2	0	2	2	4	2
7	2	4	4	2	2	2	0	4	2	2
8	4	2	2	4	2	2	4	0	2	2
9	4	2	4	2	2	4	2	2	0	2
10	4	4	2	2	4	2	2	2	2	0

You can see that each code word **c** has 6 neighbors with the distance 2 and 3 neighbors with the distance 4. Because of this regular structure, it is possible to determine the error probabilities without great expense in the following items.

Item c)
The probability of the occurrence of an undetectable error can be calculated with eq. (3.14). With the assumption that all code words are equally probable and because of the identical distance properties for all code words it is sufficient to calculate P_{ue} for any code word. The probability is

$$P_{ue} = 6 \cdot P_e^2 \cdot (1 - P_e)^3 + 3 \cdot P_e^4 \cdot (1 - P_e)$$

and is shown in **figure 12** in dependence on P_e (double logarithmic representation).

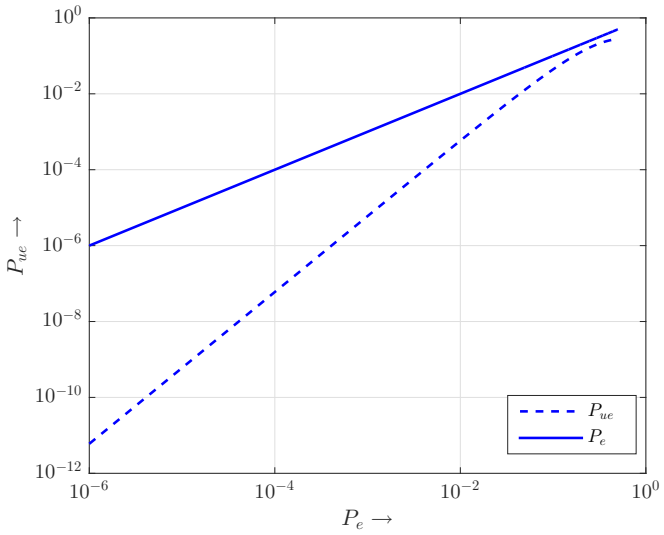

Fig. 12: Undetectable error probability for the 2-out-of-5-code at the BSC

3.2 Distance Properties of Block Codes

Solution of exercise 3.6 **Error correction**

Item a)
The maximum number of correctable errors is determined with eq. (3.3) to:

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{8 - 1}{2} \right\rfloor = 3 \, .$$

With eq. (3.4) results for the number of detectable errors at pure error detection:

$$t' = d_{\min} - 1 = 8 - 1 = 7 \, .$$

Item b)
At simultaneous correction of t errors and detection of $t' > t$ errors, eq. (3.5) must be fulfilled. With $t = 2$ and $t' = 5$ follows for the minimum distance:

$$d_{\min} \geq t + t' + 1 = 2 + 5 + 1 = 8 \, .$$

Accordingly results the field of code words shown in **figure 13** with a Hamming distance $d_{\min} = 8$.

Item c)
At the transmission, the following cases for the change of a code word according to **figure 14** have to be distinguished.

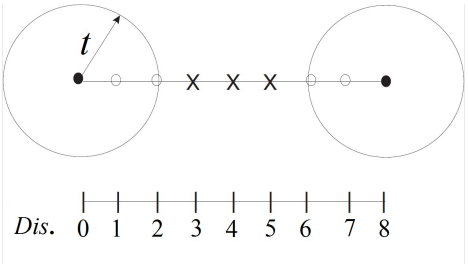

Fig. 13: Field of code words for $d_{\text{min}} = 8$

- 1. Error-free transmission
- 2. Correctable error pattern ⇒ right correction
- 3. As false detectable error pattern (invalid word)
- 4. Correctable error pattern ⇒ false correction
- 5. Received word = other code word ⇒ neither error detection nor error correction

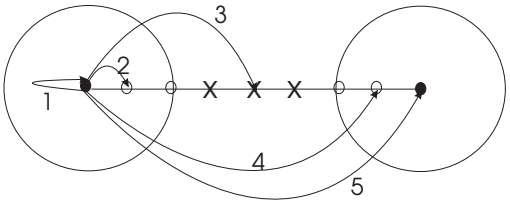

Fig. 14: Field of code words for $d_{min} = 8$

Solution of exercise 3.7 **Sphere-Packing bound (Hamming bound)**

Item a)

For a $(n, 2)_2$-block code, the information word $\mathbf{u}$ of length $k = 2$ is mapped onto a code word $\mathbf{x}$ of length n, where each digit can carry $q = 2$ different values. With eq. (3.3) follows for the maximum number of correctable errors with $d_{\text{min}} = 5$:

$$t = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor = \left\lfloor \frac{5-1}{2} \right\rfloor = 2 \, .$$

For a $(n, k, d_{\text{min}})_q$-code that shall correct t errors, the sphere-packing bound is fulfilled with eq. (3.7):

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

To determine the minimum block length n, the code parameters $k = 2$, $t = 2$, $q = 2$ are set in the sphere-packing bound and then follows

$$\begin{aligned} 2^{n-2} &\geq \sum_{r=0}^{2} \binom{n}{r} \cdot (2-1)^r \\ &\geq \binom{n}{0} + \binom{n}{1} + \binom{n}{2} \\ &\geq 1 + n + \binom{n}{2} \end{aligned}$$

For $n = 6$ results:

$$\begin{aligned} 2^{6-2} &\overset{?}{\geq} 1 + 6 + \binom{6}{2} \\ 16 &\not\geq 1 + 6 + 15 = 22 \,, \end{aligned}$$

so the sphere-packing bound is not fulfilled. For $n = 7$ results

$$\begin{aligned} 2^{7-2} &\overset{?}{\geq} 1 + 7 + \binom{7}{2} \\ 32 &> 1 + 7 + 21 = 29 \,, \end{aligned}$$

so the sphere-packing bound is fulfilled. The minimum block length therefore is $n = 7$.

Item b)
The solution follows analogously to item a). The maximum number of correctable errors with $d_{\text{min}} = 5$ is determined with eq. (3.3):

$$t = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor = \left\lfloor \frac{5 - 1}{2} \right\rfloor = 2 \,.$$

The existence of the code is then checked with the help of the sphere-packing bound eq. (3.7) with $n = 15$, $k = 7$, $t = 2$ and $q = 2$:

$$q^{n-k} \overset{?}{\geq} \sum_{r=0}^{t} \binom{n}{r} \cdot (q-1)^r \tag{9}$$

$$2^{15-7} \overset{?}{\geq} \sum_{r=0}^{2} \binom{15}{r} \cdot (2-1)^r \tag{10}$$

$$2^8 \overset{?}{\geq} \binom{15}{0} + \binom{15}{1} + \binom{15}{2} \tag{11}$$

$$256 > 1 + 15 + 105 = 121 \,. \tag{12}$$

Thus, the Hamming bound is fulfilled and therefore a $(15, 7, 5)_2$-code may exist.

- Left side: q^{n-k} different possible syndromes
- Right side: Number of error patterns with maximum weight t

Statement: To be able to correct up to t errors, it must be possible to assign each error pattern to a unique syndrome. q^k times the difference of both sides results in the number of words in the vector field of dimension n that do not lie in any of the correction spheres (around all code words).

Item c)
To check the existence possibility of a $(15, 7, 7)_2$-code, first the maximum number of correctable errors is determined as

$$t = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor = \left\lfloor \frac{7 - 1}{2} \right\rfloor = 3$$

and then the validity of the sphere-packing bound is checked:

$$q^{n-k} \overset{?}{\geq} \sum_{r=0}^{t} \binom{n}{r} \cdot (q-1)^r \tag{13}$$

$$2^{15-7} \overset{?}{\geq} \sum_{r=0}^{3} \binom{15}{r} \cdot (2-1)^r \tag{14}$$

$$2^8 \overset{?}{\geq} \binom{15}{0} + \binom{15}{1} + \binom{15}{2} + \binom{15}{3} \tag{15}$$

$$256 \not\geq 1 + 15 + 105 + 455 = 576 \,. \tag{16}$$

As the sphere-packing bound is not fulfilled, this code cannot exist!

Item d)
To check the existence possibility of a $(23, 12, 7)_2$-code, first the number of correctable errors is determined

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{7-1}{2} \right\rfloor = 3$$

and then the validity of the sphere-packing bound is checked:

$$q^{n-k} \overset{?}{\geq} \sum_{r=0}^{t} \binom{n}{r} \cdot (q-1)^r \tag{17}$$

$$2^{23-12} \overset{?}{\geq} \sum_{r=0}^{3} \binom{23}{r} \cdot (2-1)^r \tag{18}$$

$$2^{11} \overset{?}{\geq} \binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} \tag{19}$$

$$2048 = 1 + 23 + 253 + 1771 = 2048\ . \tag{20}$$

As the sphere-packing bound is fulfilled such a code may exist and if so, it will be a perfect code! (Special code: $(23, 12, 7)_2$-Golay code)

Item e)
An input alphabet with 16 equiprobable different symbols corresponds to an input word $\mathbf{u}$ of length $k = 4$.

$$q^{n-k} \overset{?}{\geq} \sum_{r=0}^{t} \binom{n}{r} \cdot (q-1)^r \tag{21}$$

$$2^{n-4} \overset{?}{\geq} \sum_{r=0}^{4} \binom{n}{r} \cdot (2-1)^r \tag{22}$$

$$2^{n-4} \overset{?}{\geq} \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} \tag{23}$$

$$\tag{24}$$

For $n = 14$ results:

$$\begin{aligned} 2^{14-4} &\overset{?}{\geq} \binom{14}{0} + \binom{14}{1} + \binom{14}{2} + \binom{14}{3} + \binom{14}{4} \\ 2^{10} &\overset{?}{\geq} 1 + 14 + 91 + 364 + 1001 \\ 1024 &\not\geq 1471\ , \end{aligned}$$

so the sphere-packing bound is not fulfilled. For $n = 15$ results

$$\begin{aligned} 2^{15-4} &\overset{?}{\geq} \binom{15}{0} + \binom{15}{1} + \binom{15}{2} + \binom{15}{3} + \binom{15}{4} \\ 2^{11} &\overset{?}{\geq} 1 + 15 + 105 + 455 + 1365 \\ 2048 &> 1941\ , \end{aligned}$$

so the sphere-packing bound is fulfilled. The minimum possible block length therefore is $n = 15$ and for the code rate R_c follows:

$$R_c = \frac{k}{n} \leq \frac{4}{15} = 0.2667\ .$$

3.3 Matrix Description of Block Codes

Solution of exercise 3.8 **Generator and parity check matrices**

Item a)
Generator and parity check matrices of the (4,1,$d_{\min} = 4$)-repetition code in systematic form: (see ch. 3.5.7)

$$\mathbf{G} = (1 \mid 1\ 1\ 1) \qquad \mathbf{H} = \left(\begin{array}{c|ccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right).$$

For the dual code, the parity check matrix is now used as the generator matrix. The consideration of $\mathbf{H}$ shows, that a simple (4,3,$d_{\min} = 2$)-SPC code results, that puts a test sum in front of the three information bits. Furthermore, the product $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$ illustrates the orthogonality of both codes.

Item b)
The parity check matrix of a Hamming code of rank $r = 3$ can easily be produced by assigning the dual numbers from 1 to 7 in columns

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

The generator matrix cannot be directly produced with eq. (3.31) from this non-systematic form. In order to achieve the generator matrix we construct an equivalent systematic code $\mathbf{H}_{sys}$ by exchanging the columns of $\mathbf{H}$ and calculate the corresponding systematic generator matrix $\mathbf{G}_{sys}$

$$\mathbf{H}_{sys} = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \quad \Longrightarrow \quad \mathbf{G}_{sys} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

To finally get the generator matrix $\mathbf{G}$ that fits to $\mathbf{H}$, the exchange of columns has to be undone. The generator matrix of the original code then has the form

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

Item c)
The consideration of $\mathbf{H}$ shows, that there exist no two linearly dependent (identical) columns. Nevertheless, there are combinations of three columns that are linearly dependent (for instance the first three columns). This is exactly the minimum distance of the code. The general connection is, that the minimum distance of the code is identical to the minimum number of linearly dependent columns of its parity check matrix. Thus, every selection of $d_{\min} - 1$ columns is linearly independent and there exists at least one selection of $d_{\min}$ linearly dependent columns.

Solution of exercise 3.9 **Expansion, shortening and puncturing**

Item a)
An additional test bit c_7 implies for the parity check matrix $\mathbf{H}_{sys}$ of the original code, that the number of columns (length of the code words) and rows (number of test bits) is increased for both by one. If the expanded code shall have the minimum distance $d_{\min} = 4$, its parity check matrix $\mathbf{H}_E$ must contain according to exercise 3.8c at least 4 linearly dependent columns. The easiest expansion consists of first adding a column of zeros, whereby the decoding of the original code is not affected. Then, a row of ones is added, that forms an additional parity-check-sum over all $n = 7$ bits of the original code. Therefore, each code word of the expanded code has an even weight,

i.e., the odd minimum distance $d_{\min} = 3$ is increased to $d_{\min,E} = 4$. The new parity check matrix is

$$\mathbf{H}_E = \begin{pmatrix} \mathbf{H}_{sys} & \mathbf{0} \\ \mathbf{1} & 1 \end{pmatrix} = \left(\begin{array}{ccccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right) .$$

We get the corresponding generator matrix $\mathbf{G}_E$ by adding an additional column $\mathbf{g}^+$ for the added test bit c_7. As $c_7 = \mathbf{u} \cdot \mathbf{g}^+$ represents the test sum of all c_i with $0 \leq i < 7$, the condition for $\mathbf{g}^+$ is

$$c_7 = \mathbf{u} \cdot \mathbf{g}^+ \stackrel{!}{=} \sum_{i=0}^{6} c_i \bmod 2 = \mathbf{u} \cdot \mathbf{G}_{sys} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \quad \Longrightarrow \quad \mathbf{g}^+ = \mathbf{G}_{sys} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} .$$

The column $\mathbf{g}^+$ can thus be calculated from the modulo 2 sum of all columns of $\mathbf{G}_{sys}$. The generator matrix of the expanded code has the form

$$\mathbf{G}_E = (\mathbf{G}_{sys} \mid \mathbf{g}^+) = \left(\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) .$$

Item b)
The bisection of the field of code words is reached by cancellation of one information bit, which results in a half rate (6,3)-code. Using the systematic coder from exercise 3.8, each of the four information bits of the original code can be canceled. In each case the minimum distance remains the same, i.e., $d_{\min,S} = 3$. The generator matrix results by canceling the ith row and column of $\mathbf{G}_{sys}$, $1 \leq i \leq k$, at the parity check matrix accordingly the ith column of $\mathbf{H}_{sys}$. Both matrices for the example of $i = 4$ are:

$$\mathbf{G}_S = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad , \quad \mathbf{H}_S = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} .$$

Item c)
The punctured generator matrix is achieved by canceling the ith column ($k + 1 \leq i \leq n$) of $\mathbf{G}_{sys}$, at the parity check matrix accordingly the $(i - k)$th row and the ith column. The minimum distance is then $d_{\min,P} = 2$. The difference to item b) is in the fact, that still 16 code words exist.

$$\mathbf{G}_P = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad , \quad \mathbf{H}_P = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} .$$

Solution of exercise 3.10 **Coset decomposition and syndrome decoding**

Item a)
The (7,4,3)-Hamming code has $n - k = 3$ test bits, so the overall $2^{n-k} = 8$ syndromes (included $\mathbf{s} = \mathbf{0}$) can be formed. Furthermore, a single error can always be corrected due to $d_{\min} = 3$. Because of the word length of $n = 7$ there are exactly 7 different single error patterns. Thus, the number of non-zero syndromes corresponds to the number of correctable error patterns and therefore the Hamming code is a perfect code.

Item b)
For the Hamming code, the columns of $\mathbf{H}$ represent all non-zero syndromes $\mathbf{s} \neq \mathbf{0}$. Because of $t = 1$, the error words $\mathbf{e}$ with the Hamming weight $w_{\mathrm{H}}(\mathbf{e}) = 1$ form the coset leaders. Now, only the assignment has to be determined. The following table results:

syndrome $\mathbf{s}_\mu$	coset leader $\mathbf{e}_\mu$
1 1 0	1 0 0 0 0 0 0
1 0 1	0 1 0 0 0 0 0
0 1 1	0 0 1 0 0 0 0
1 1 1	0 0 0 1 0 0 0
1 0 0	0 0 0 0 1 0 0
0 1 0	0 0 0 0 0 1 0
0 0 1	0 0 0 0 0 0 1

Hint: Let $\mathbf{e}_\mu$ denote the μth row of the $n \times n$ identity matrix, i.e. $\mathbf{e}_\mu$ contains a one at the μth position and zeros elsewhere. Then $\mathbf{s} = \mathbf{e}_\mu \cdot \mathbf{H}^T$ corresponds to the μth row of $\mathbf{H}^T$.

Item c)
The syndrome for the received word is

$$\mathbf{s} = \mathbf{y} \cdot \mathbf{H}^T = (1\,0\,1)\ .$$

So, there is an error. The coset leader belonging to the syndrome can be found in the second row of the table from item b). The correction can be realized by adding $\mathbf{y}$ and $\mathbf{e}_2 = (0\,1\,0\,0\,0\,0\,0)$.

$$\hat{\mathbf{c}} = \mathbf{y} + \mathbf{e}_2 = (1\,0\,0\,1\,0\,0\,1)$$

The estimated information word thus is $\hat{\mathbf{u}} = (1\,0\,0\,1)$.

Item d)
To be able to use the syndrome $\mathbf{s}$ directly for addressing the coset leader, the position of the one within the coset leader has to correspond to the decimal representation of $\mathbf{s}$ (See hint for item a)). The parity check matrix is

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

Solution of exercise 3.11 **Coding program**

The $(7, 4, 3)$-Hamming code maps $k = 4$ information symbols onto $n = 7$ code symbols. Within the MATLAB program, k information symbols are randomly chosen using `randi` and encoded by the generator matrix. A randomly determined error vector is added and the syndrome is calculated. If the syndrome is non-zero, the corresponding coset leader is added to the received word. Please notice: all calculations have to be executed within GF(2).

3.4 Cyclic codes

Solution of exercise 3.12 **Polynomial multiplication**

Item a)
Multiplication of $f(D)$ and $g(D)$:

$$\begin{aligned}(D^3 + D + 1) \cdot (D + 1) &= D^4 + D^2 + D + D^3 + D + 1 \\ &= D^4 + D^3 + D^2 + 1\end{aligned}$$

Item b)

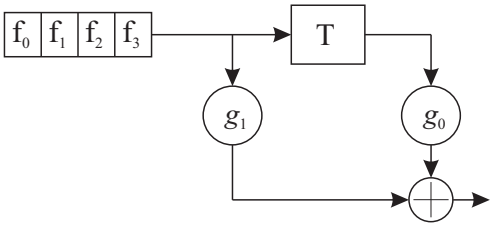

Fig. 15: Block diagram of a non-recursive system for the sequential multiplication of two polynomials

Item c)
With in $\longrightarrow$ memory$^+$ and out $=$ in $\oplus$ memory, the corresponding function table is achieved.

clock	in	memory	out
0	0	0	0
1	1	0	1
2	0	1	1
3	1	0	1
4	1	1	0
5	0	1	1

The output $(1, 1, 1, 0, 1)$ corresponds to the solution $D^4 + D^3 + D^2 + 1$ achieved in item a).

Solution of exercise 3.13 **Polynomial division**

Item a)
Division of $f(D)$ by $g(D)$.

$$\begin{array}{llll:lll} D^3 & & +D & +1 & : & D^2+D+1 = & D+1 \\ \cline{1-4} D^3 & +D^2 & +D & & & & \\ \cline{1-4} & D^2 & & +1 & & & \\ & D^2 & +D & +1 & & & \\ \cline{2-4} & & D & & & & \end{array}$$

$\Rightarrow$ remainder $R_{g(D)}[f(D)] = D$

Item b)

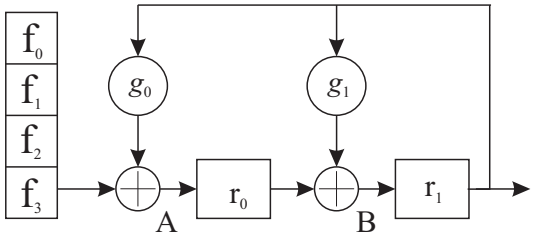

Fig. 16: Block diagram of a recursive system for the sequential division of two polynomials

Item c)
By defining A = Out $\oplus$ In $\longrightarrow r_0^+$ and B = Out $\oplus\, r_0 \longrightarrow r_1^+$, the function table is easily generated.

clock	In	A	r_0	B	r_1	Out
0	0	0	0	0	0	0
1	1	1	0	0	0	0
2	0	0	1	1	0	0
3	1	0	0	1	1	1
4	1	0	0	1	1	1
5	0	-	0	-	1	1

Solution of exercise 3.14 **Generator polynomial**

Item a)
If $g(D)$ shall be a generator polynomial, $R_{g(D)}[D^n - 1] = 0$ has to be fulfilled according to ch. 3.6.2. With $n = 15$ and $g(D) = D^8 + D^7 + D^6 + D^4 + 1$ follows

$$(D^{15} - 1) : \underbrace{(D^8 + D^7 + D^6 + D^4 + 1)}_{g(D)} = \underbrace{D^7 + D^6 + D^4 + 1}_{h(D)} \;\Rightarrow \text{rest} = 0\ ,$$

so the required condition is fulfilled.

Item b)
With eq. (3.56) the code word **c** can be divided into two parts at systematic coding:

$$c(D) = p(D) + D^{n-k} \cdot u(D)$$

with the parity check polynomial

$$p(D) = R_{g(D)}[-D^{n-k} \cdot u(D)]\ .$$

With the code parameters $n = 15,\ k = 7,\ n-k = 8$ follows $D^{n-k} \cdot u(D) = D^8 \cdot (D^4 + D + 1) = D^{12} + D^9 + D^8$. Therefore results for the parity check polynomial

$$(D^{12} + D^9 + D^8) : (D^8 + D^7 + D^6 + D^4 + 1) = D^4 + D^3 \;\Rightarrow \text{rest} = p(D) = D^7 + D^4 + D^3$$

and for the code word

$$\begin{aligned} c(D) &= D^{n-k} \cdot u(D) + p(D) \\ &= \underbrace{D^{12} + D^9 + D^8}_{D^8 \cdot u(D)} + \underbrace{D^7 + D^4 + D^3}_{p(D)} \\ &= 001\ 0011\ 1001\ 1000\ . \end{aligned}$$

Item c)
The required condition for $y(D) = D^{14} + D^5 + D + 1$ to be a valid code word is that it must be divisible by $g(D)$ i.e., $s(D) = R_{g(D)}[y(D)] = 0$.

$$(D^{14} + D^5 + D + 1) : (D^8 + D^7 + D^6 + D^4 + 1) = D^6 + D^5 + D^3 \;\Rightarrow \text{rest} = s(D) = D^7 + D^6 + D^3 + D + 1$$

Thus $s(D) \neq 0$ and therefore $y(D)$ cannot be a valid code word.

Solution of exercise 3.15 **Syndrome**

Item a)
For now, all coset leaders are collected in the matrix $\mathbf{E}$

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

and different syndromes are collected in the matrix $\mathbf{S}$

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

With eq. (3.35) is

$$\mathbf{S} = \mathbf{E} \cdot \mathbf{H}^T$$

Therefore the parity check matrix $\mathbf{H}$ can be determined by

$$\mathbf{H}^T = \mathbf{E}^{-1} \cdot \mathbf{S} = \mathbf{E} \cdot \mathbf{S} = \mathbf{S}$$

so that

$$\mathbf{H} = \left(\begin{array}{ccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) = (\mathbf{P}_{3,5}^T | \mathbf{I}_{5,5})$$

results. With the decomposition of the parity check matrix $\mathbf{H} = (-\mathbf{P}_{k,n-k}^T | \mathbf{I}_{n-k,n-k})$ with eq. (3.31) results for the generator matrix with eq. (3.30)

$$\begin{aligned} \mathbf{G} &= (\mathbf{I}_{k,k} | \mathbf{P}_{k,n-k}) = (\mathbf{I}_{3,3} | \mathbf{P}_{3,5}) \\ &= \left(\begin{array}{ccc|ccccc} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right). \end{aligned}$$

Item b)
From the parity check matrix $\mathbf{H} = (-\mathbf{P}_{k,n-k}^T | \mathbf{I}_{n-k,n-k})$ it is directly readable that the number of test digits $n - k = 5$ and the number of information digits $k = 3$.

Item c)
In ch. 3.62 it is explained how to calculate the generator matrix from the generator polynomial $g(D)$. The connection is

$$\mathbf{G} = \begin{pmatrix} g_0 & \dots & g_{n-k} & 0 & 0 \\ 0 & g_0 & \dots & g_{n-k} & 0 \\ 0 & 0 & g_0 & \dots & g_{n-k} \end{pmatrix} .$$

From the first row (10010100) of the generator matrix found in item a) therefore results the generator polynomial $g(D) = 1 + D^3 + D^5$.

Item d)
According to the number of information digits $k = 3$, $2^3 = 8$ different code words can be generated.

Item e)
For the detection of transmission errors the syndrome corresponding to the receiving word $\mathbf{y}_1$ is determined:

$$\mathbf{s} = \mathbf{y}_1 \cdot \mathbf{H}^T = (0\,2\,1\,2\,2) \text{ modulo } 2 \; = (0\,0\,1\,0\,0) \; .$$

As the syndrome is not equal to zero, $\mathbf{y}_1$ is not a code word. By comparing with the syndrome table we find $\mathbf{s} = \mathbf{s}_6$, so for the corresponding error vector we conclude $\mathbf{e}_6 = 00000100$. According to eq. (3.38)

$$\begin{aligned} \hat{\mathbf{c}} &= \mathbf{y}_1 + \mathbf{e}_6 \\ &= (0\,1\,1\,0\,1\,0\,1\,1) + (0\,0\,0\,0\,0\,1\,0\,0) \\ &= (0\,1\,1\,0\,1\,1\,1\,1) \; . \end{aligned}$$

Item f)
For the decoding of the receiving word $\mathbf{y}_2 = (1\,0\,1\,1\,0\,1\,1\,1)$ again the corresponding syndrome is determined:

$$\mathbf{s} = \mathbf{y}_2 \cdot \mathbf{H}^T = (2\,0\,3\,1\,2) \text{ modulo } 2 \; = (0\,0\,1\,1\,0) \; .$$

Thus $\mathbf{y}_2$ is not a code word. As the syndrome is not contained in the syndrome table, no error correction can follow.

Solution of exercise 3.16 **Primitive polynomials**

A polynomial $p(D)$ of degree m (with coefficients $p_i \in$GF(p)) is called *irreducible* if it cannot be factorized into polynomials of degree $< m$ (with coefficients from GF(p)). Consequently it does not have any zeros in the GF(p).

An irreducible polynomial $p(D)$ of degree m (with $p_i \in$GF(p)) is called *primitive polynomial* if there exists an $\alpha \in$GF(p^m) such that $p(\alpha) = 0$ and the powers $\alpha^1, \cdots, \alpha^n$ with $n = p^m - 1$ form the non-zero elements of the extension field GF(p^m). α is called *primitive element* of GF(p^m) and n is the order of α.

Polynomial $p(D) = g_1(D) = D^4 + D + 1$:

For primitive element α the auxiliary condition $\alpha^4 = \alpha + 1$ is valid with $p(\alpha) = \alpha^4 + \alpha + 1 = 0$.

$$
\begin{array}{lllllll}
\alpha^0 & = & & & & = & 1 \\
\alpha^1 & = & & & & = & \alpha \\
\alpha^2 & = & & & & = & \alpha^2 \\
\alpha^3 & = & & & & = & \alpha^3 \\
\alpha^4 & = & & & & = & \alpha + 1 \\
\alpha^5 & = & \alpha \cdot \alpha^4 & & \alpha \cdot (z+1) & = & \alpha^2 + \alpha \\
\alpha^6 & = & \alpha \cdot \alpha^5 & & \alpha \cdot (z^2+z) & = & \alpha^3 + \alpha^2 \\
\alpha^7 & = & \alpha^2 \cdot \alpha^5 & = & \alpha^4 + \alpha^3 & = & \alpha^3 + \alpha + 1 \\
\alpha^8 & = & \alpha^4 \cdot \alpha^4 & = & (\alpha+1) \cdot (\alpha+1) & = & \alpha^2 + 1 \\
\alpha^9 & = & \alpha \cdot \alpha^8 & = & \alpha \cdot (\alpha^2+1) & = & \alpha^3 + \alpha \\
\alpha^{10} & = & \alpha \cdot \alpha^9 & = & \alpha^4 + \alpha^2 & = & \alpha^2 + \alpha + 1 \\
\alpha^{11} & = & \alpha \cdot \alpha^{10} & = & \alpha \cdot (\alpha^2 + \alpha + 1) & = & \alpha^3 + \alpha^2 + \alpha \\
\alpha^{12} & = & \alpha \cdot \alpha^{11} & = & \alpha^4 + \alpha^3 + \alpha^2 & = & \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^{13} & = & \alpha \cdot \alpha^{12} & = & \alpha^4 + \alpha^3 + \alpha^2 + \alpha & = & \alpha^3 + \alpha^2 + 1 \\
\alpha^{14} & = & \alpha \cdot \alpha^{13} & = & \alpha^4 + \alpha^3 + \alpha & = & \alpha^3 + 1 \\
\alpha^{15} & = & \alpha \cdot \alpha^{14} & = & \alpha^4 + \alpha & = & 1
\end{array}
$$

For polynomial $g_1(D)$ therefore results the order $n_1 = 15 = 2^4 - 1$ and thus it is a primitive polynomial.

Polynomial $p(D) = g_2(D) = D^4 + D^3 + D^2 + D + 1$:

For primitive element α the auxiliary condition $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$ is valid with $p(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$.

$$
\begin{array}{lllllll}
\alpha^0 & = & & & & = & 1 \\
\alpha^1 & = & & & & = & \alpha \\
\alpha^2 & = & & & & = & \alpha^2 \\
\alpha^3 & = & & & & = & \alpha^3 \\
\alpha^4 & = & & & & = & \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 & = & \alpha \cdot \alpha^4 & = & \alpha^4 + \alpha^3 + \alpha^2 + \alpha & = & 1
\end{array}
$$

As $\alpha^0 = \alpha^5 = 1$, for the polynomial $g_2(D)$ follows the order $n_2 = 5 < 2^4 - 1$ so it is not a primitive polynomial.

Solution of exercise 3.17

CRC codes

Item a)

A CRC code has the parameters $n = 2^r - 1$ and $k = 2^r - r - 2$. For $n = 15$ is accordingly $r = 4$ and hence $k = 10$. Besides, the generator polynomial can be factorized to $g(D) = p(D) \cdot (1 + D)$, such that $p(D)$ is a primitive polynomial of degree 4 ($g(D)$ is of degree $n - k = 5$). Considering the solution of previous task, the primitive polynomial can be chosen as $p(D) = 1 + D + D^4$. Therefore the corresponding generator polynomial is

$$g(D) = 1 + D^2 + D^4 + D^5 \ .$$

Item b)

MATLAB calculates the generator matrix $\mathbf{G}$ and the parity check matrix $\mathbf{H}$ from the generator polynomial $g(D)$ with the help of the command `cyclgen`.

$$
\mathbf{H} = \left(\begin{array}{ccccc|ccccccccc}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1
\end{array}\right)
$$

$$\mathbf{G} = \left(\begin{array}{ccccc|ccccccccccc} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Item c)
If only burst errors are considered that do not contain any correct digits, all such error patterns are detectable as the corresponding syndromes are always not equal to zero. To prove this, it suffices to show that there exists no valid code word which consists of l_e successive ones (and zeros elsewhere). For l_e being odd, the proof is straightforward, as the code word (polynomial) will not be divisible by $D+1$. For l_e being even, a direct approach using `gfdeconv` shows that the corresponding remainder (division of $1+D+...+D^{l_e-1}$ by $g(D)$) is non-zero.

Solution of exercise 3.18

Reed-Solomon codes

Item a)
For the extension field GF(2^3) shall be constructed a Reed-Solomon code that is able to correct $t=1$ error. Hence it results the code parameters $n=2^3-1=7$ and $n-k=2t=2 \Rightarrow k=5$ and $d=n-k+1=3$ from which can be calculated the code rate $R_c=5/7\approx 0.714$. Thus we get a $(7,5,3)_8$-code with $8^5=32.768$ code words.

Item b)
The command `rsgenpoly(n,k)` yields the generator polynomial $g(D)$ of a (n,k)-RS-code. Applying $n=7$ and $k=5$, the vector $[1 \quad 6 \quad 3]$ results. The entries are the decimal representation of the corresponding coefficients of different powers of D in descending order. Hence, the corresponding generator polynomial follows as: $g(D)=D^2+(\alpha^2+\alpha)D+(\alpha+1)$ in which α is the primitive element with respect to the default primitive polynomial.

Item c)
The coding can follow with the help of the command `rsenc`. We get the code word

$$\mathbf{c} = (110\,010\,111\,000\,001\,010\,010)\ .$$

As exactly one false symbol can be corrected with $t=1$, the maximum correctable error length is $m=3$ bits. The superposition of a 3-bit error is only disturbing the transmission if two or three code symbols of the GF(8) are affected. If only one symbol is altered the error can be corrected.

A binary code with the same correction ability would have to have a minimum distance of $d_{\min}=7$. Hereby becomes clear, that RS codes are suitable for the correction of burst errors. If the three bits of error appear in different symbols of the GF(8), they correspond to three single errors and are not correctable anymore.

Item d)
With the same extension field shall be constructed a $t=2$-errors correcting code, from which directly results the requirement for $d_{\min}=5$. The further parameters are $k=2^3-d_{\min}=3$ and $R_c=3/7\approx 0.429$. The code thus consists of $(8)^3=512$ code words.

Applying $n=7$ and $k=3$ to the command `rsgenpoly(n,k)`, the vector $[1 \;\; 3 \;\; 1 \;\; 2 \;\; 3]$ results. The entries are the decimal representation of the corresponding coefficients of different powers of D in descending order. Hence, the corresponding generator polynomial follows as: $g(D)=D^4+(\alpha+1)D^3+D^2+\alpha D+(\alpha+1)$ in which α is the primitive element with respect to the default primitive polynomial.

Item e)
This task can be addressed using the command `[decoded,cnumerr,ccode] = rsdec(code,n,k)`. Applying $n = 7$, $k = 3$ and the received word as `gf([6 2 7 3 2 6 6],3)`, the transmitted message, the number of errors and the corrected code word are achieved directly.

Solution of exercise 3.19

BCH codes

Item a)
The MATLAB command `gfcosets` yields the following cyclotomic cosets for the extension field GF(2^4):

$$\mathcal{K}_1 = \{1,\ 2,\ 4,\ 8\}, \qquad \mathcal{K}_3 = \{3,\ 6,\ 12,\ 9\}$$
$$\mathcal{K}_5 = \{5,\ 10\}, \qquad \mathcal{K}_7 = \{7,\ 14,\ 13,\ 11\}\ .$$

To fulfill the requirement of $t = 3$ correctable errors, a union set $\mathcal{M}$ must contain at least $d-1 = 2t = 6$ successive elements. This aim is reached with

$$\mathcal{M}_1 = \mathcal{K}_1 \cup \mathcal{K}_3 \cup \mathcal{K}_5 = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 9,\ 10,\ 12\}$$

and also

$$\mathcal{M}_2 = \mathcal{K}_3 \cup \mathcal{K}_5 \cup \mathcal{K}_7 = \{3,\ 5,\ 6,\ 7,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14\}\ .$$

Thus we get a BCH code of the length $n = 2^4 - 1 = 15$ with the dimension $k = n - |\mathcal{M}| = 15 - 10 = 5$. One may note, that the BCH code with $R_c = 1/3$ requires smaller code rate for the correction of three errors compared to the RS code ($R_c = 5/7$) from exercise 3.18. Nevertheless, it is able to correct single errors, while the RS code can only correct three successive errors.

Item b)
With $n = 15$ and $k = 5$, MATLAB yields the generator polynomial $g(D)$ as

$$g(D) = 1 + D + D^2 + D^4 + D^5 + D^8 + D^{10}\ .$$

Item c)
We get the code word

$$c(D) = D^2 + D^4 + D^9 + D^{10} + D^{11} + D^{13} + D^{14}$$

for the information word $u(D) = 1 + D + D^3 + D^4$. The roots of a polynomial can be quickly determined with the command `gfroots`. They are

$$c(D) = 0 \quad \text{for} \quad D \in \{0\ ,\ \alpha\ ,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^8,\ \alpha^9,\ \alpha^{10},\ \alpha^{12}\}\ .$$

It can be seen, that $c(D)$ has its roots at successive lower powers of α. The reason behind is the choice of the cyclotomic cosets to generate the code, i.e., $\mathcal{M}_1$ is chosen.

Item d)
The function `gf_dft` executes a transformation into the spectral domain. The output polynomial $C(D)$ is represented in the exponential format, i.e., the coefficients represent powers of the primitive element α (the input polynomial $c(D)$ also has to have this format). We get

$$\mathbf{C} = (1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ \alpha^3,\ 0,\ 0,\ 0,\ \alpha^9,\ 0,\ \alpha^{12},\ \alpha^6)\ .$$

The powers of α that form the roots of the code word $c(D)$ correspond exactly to the positions, at which $\mathbf{C}$ has coefficients equal to zero.

4 Convolutional Codes

4.1 Fundamental Principles

Solution of exercise 4.1

Convolutional codes

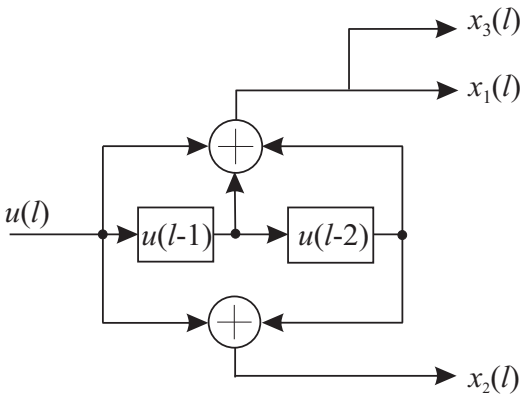

Fig. 17: Shift register structure for the code of the rate $R_c = 1/3$

Item a)
For the input sequence $u = (0\,1\,1\,0\,1\,0)$ results the following output sequence:

$$\mathbf{c} = (000\,111\,010\,010\,000\,101)\ .$$

Thus it is not a systematic encoder.

Item b)
For the input sequence $u = (0\,1\,1\,0\,1\,0)$ results the path in the Trellis diagram shown in **figure 18**.

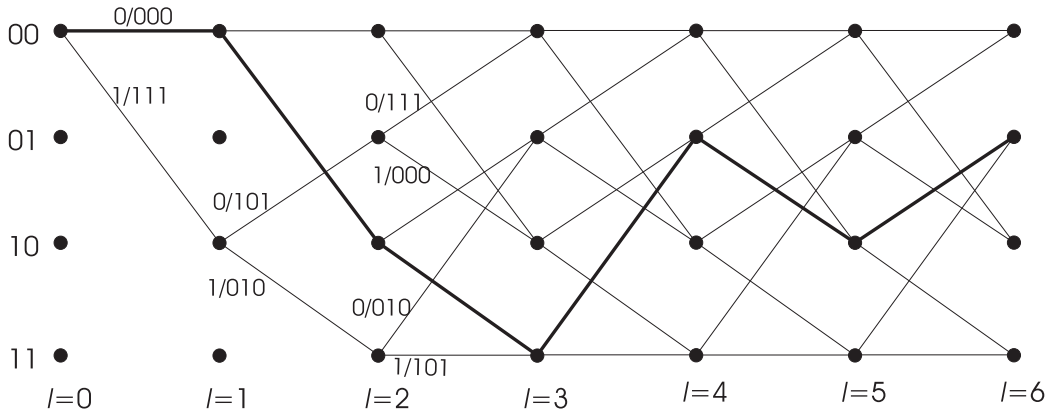

Fig. 18: Trellis diagram for the input sequence $u = (0\,1\,1\,0\,1\,0)$

Item c)
The corresponding state diagram is given in **figure 19**.

Item d)
The free distance d_f gives the minimum Hamming distance between any two sequences. Because of the linearity of convolutional codes, the comparison of sequences with the all-zero sequence is sufficient for determination of

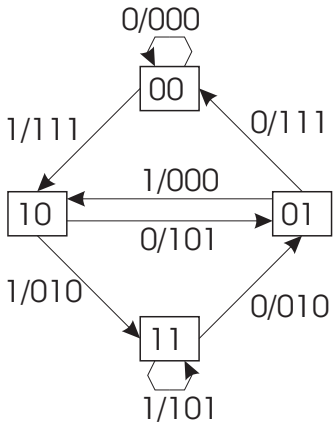

Fig. 19: State diagram for the code of the rate $R_c = 1/3$

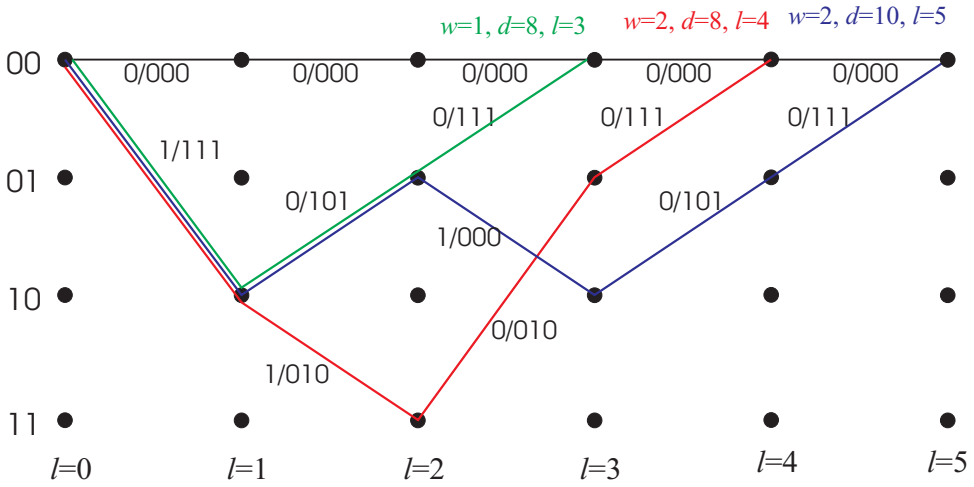

Fig. 20: Free distance for the code of the rate $R_c = 1/3$

the Hamming distance. The **figure 20** shows three sequences, that are different from the all-zero sequence, with $l = 3$, $l = 4$ and $l = 5$, respectively.

The first sequence corresponds to the input sequence $u = (1\,0\,0)$ (input weight $w = 1$) and to the output sequence $c = (111\,101\,111)$. By comparison with the all-zero sequence ($u = (0\,0\,0)$ and $c = (000\,000\,000)$) results the Hamming distance $d = 8$.

The second sequence corresponds to the input sequence $u = (1\,1\,0\,0)$ (input weight $w = 2$) and to the output sequence $c = (111\,010\,010\,111)$, such that again the Hamming distance is $d = 8$.

The third sequence corresponds to the input sequence $u = (1\,0\,1\,0\,0)$ (input weight $w = 2$) and to the output sequence $c = (111\,101\,000\,101\,111)$, such that the Hamming distance is $d = 10$.

The free distance therefore is $d_f = 8$.

4.2 Characterization of Convolutional Encoders

Solution of exercise 4.2 **Catastrophic encoders**

In **figure 21** the shift register structure and the state diagram of the encoder is shown. As in the state diagram exists a closed loop with the weight zero (closed loop in the state 11 has the weight zero), it is a catastrophic encoder.

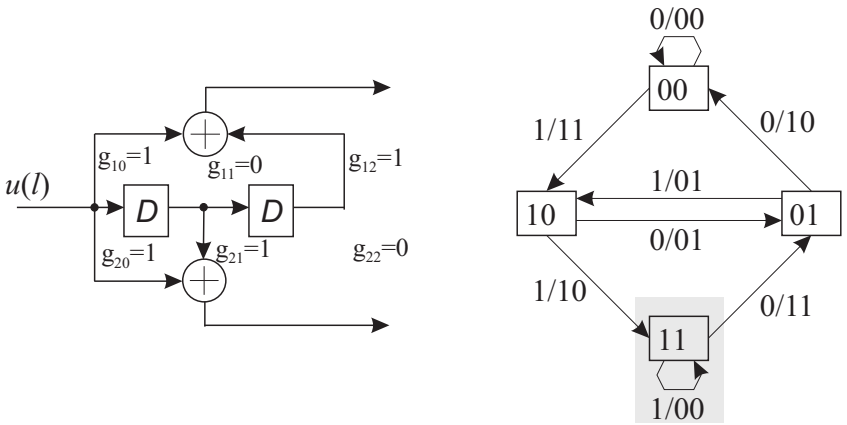

Fig. 21: Shift register structure and state diagram for catastrophic encoder

Further characteristic: as can be seen in **figure 21**, all adders have an even number of connections. Because of these properties a finite number of transmission errors can lead to an infinite number of errors after decoding.

4.3 Optimal Decoding with Viterbi Algorithm

Solution of exercise 4.3 **Viterbi decoding**

Item a)
In **figure 22** the Trellis diagram for the convolutional code is presented.

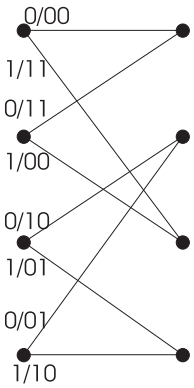

Fig. 22: Trellis diagram of the convolutional code with $g_1(D) = 1 + D + D^2$ and $g_2(D) = 1 + D^2$

For the terminated information sequence $u(\ell) = (1\,1\,0\,1(\,0\,0))$ follows the code sequence $x = (11\,01\,01\,00\,10\,11)$.

Item b)
The decoding of the code sequence $x = (11\,01\,01\,00\,10\,11)$ is shown in **figure 23**. From the decoding follows the transmitted data sequence $u(\ell) = (1\,1\,0\,1\,(0\,0))$.

Figure 24 shows the decoding for the disturbed receiving sequence $y_1 = (11\,\underline{1}1\,01\,0\underline{1}\,10\,11)$ and the estimated data sequence $u_1 = (1\,1\,0\,1\,(0\,0))$ follows, such that the two transmission errors were corrected.

Figure 25 shows the decoding for the disturbed receiving sequence $y_2 = (11\,\underline{1}1\,\underline{10}\,0\underline{1}\,10\,11)$ and the estimated data sequence $u_2 = (1\,\underline{0}\,0\,1\,(0\,0))$ follows which doesn't correspond to the transmitted data sequence.

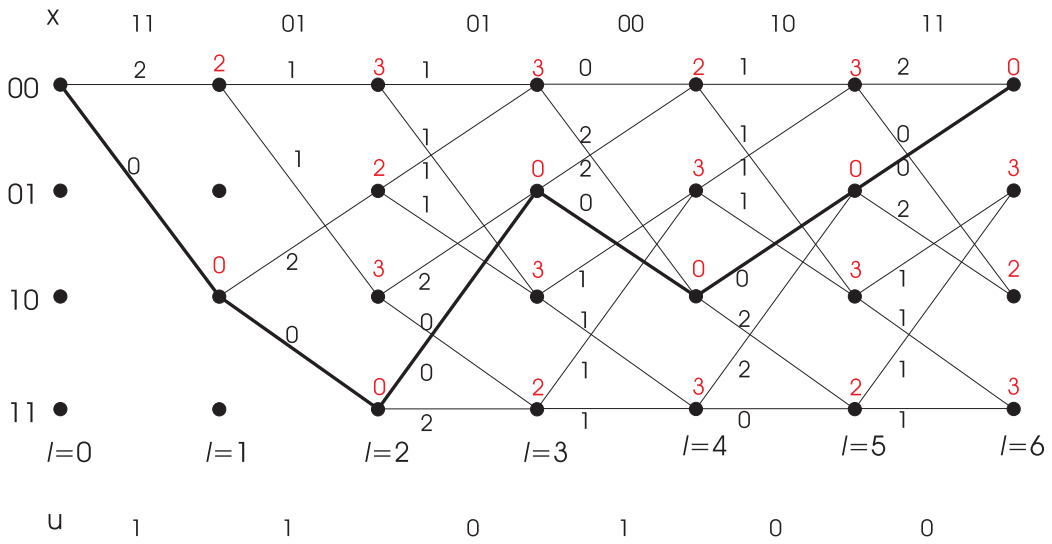

Fig. 23: Viterbi decoding of x

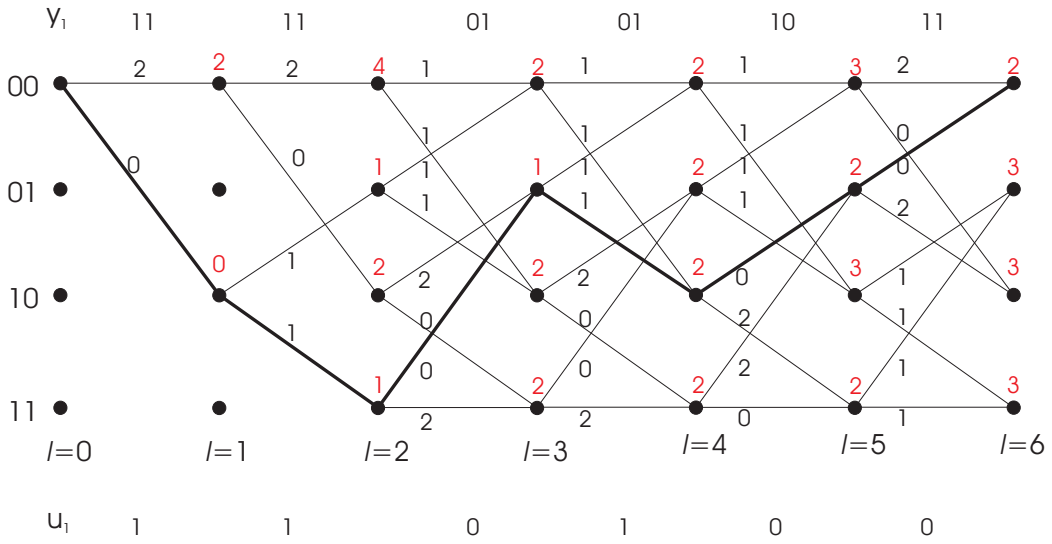

Fig. 24: Viterbi decoding of $y_1 = (11\ \underline{1}1\ 01\ 0\underline{1}\ 10\ 11)$

Solution of exercise 4.4 **Viterbi decoding with puncturing**

Item a)
The puncturing matrix $\mathbf{P}$

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

consists of $n = 2$ rows and $L_P = 4$ columns. Only 5 bits of the originally $n \cdot L_P = 8$ code bits are transmitted after the puncturing, such that the code rate of the punctured code results

$$R_{c,punc} = \frac{1}{2} \cdot \frac{8}{5} = \frac{4}{5}.$$

Item b)
Under consideration of the puncturing scheme follows from the receiving sequence $y = (1\ 1\ 0\ 0\ 0\ 1\ 0\ 1)$ the punctured receiving sequence $y = (11\ 0x\ 0x\ x0\ 10\ 1x)$ (with placeholder x for the punctured bits).

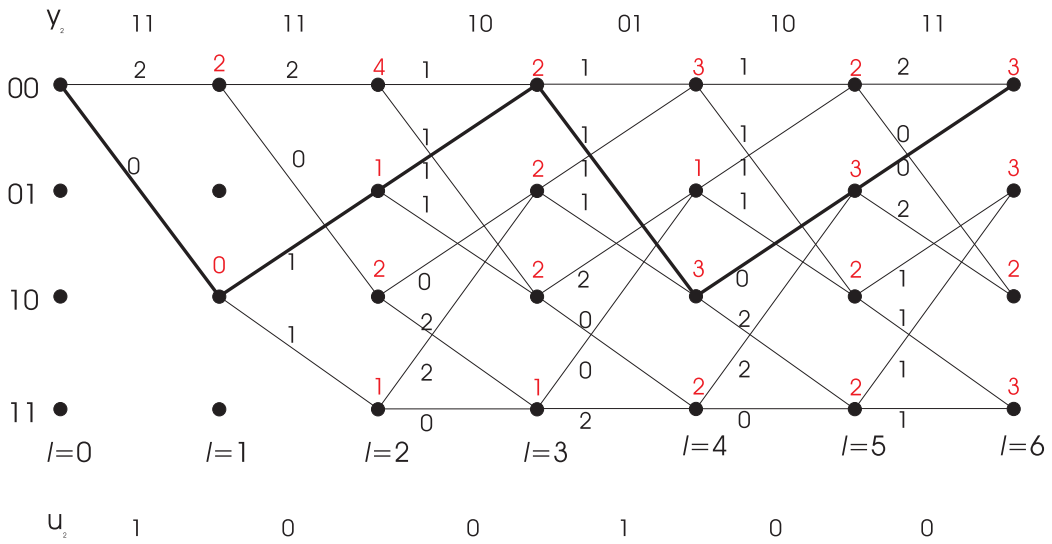

Fig. 25: Viterbi decoding of $y_2 = (11\ \underline{11}\ \underline{10}\ \underline{01}\ 10\ 11)$

The decoding is presented in **figure 26** and it is correctly decided to $u = (1\ 1\ 0\ 1\ (0\ 0))$.

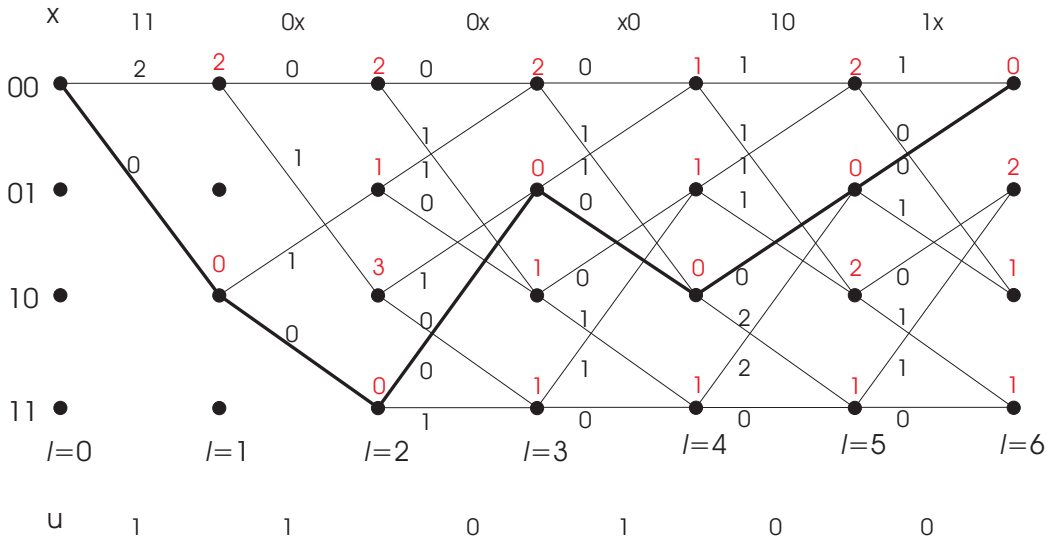

Fig. 26: Viterbi decoding with puncturing

Solution of exercise 4.5

RSC encoders

Item a)
Figure 27 shows a Trellis segment for the considered convolutional code. The dashed lines typify transitions for an information bit $u = 1$, the solid lines for $u = 0$. The 2-bit-words at the right margin represent the code words of the respective state transitions, where the upper code word is assigned to the upper path, that arrives at the respective state.

Item b)
The input sequence of the information bits is given by $u(\ell) = (1\ 1\ 0\ 1\ 1)$. Tail bits have to be added at the end of the sequence to conduct the encoder to the zero state. As this is a recursive encoder, the tail bits cannot be determined until the end of the input sequence $u(\ell)$. We get the following scheme and therefore the tail bits are $(1\ 0\ 1)$.

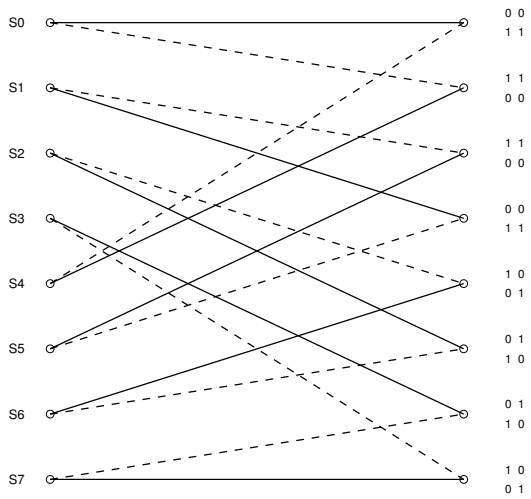

Fig. 27: Trellis segment for convolutional code with the generators $\tilde{g}_1(D) = 1$ and $\tilde{g}_2(D) = (1+D+D^3)/(1+D+D^2+D^3)$

$u(\ell)$	state	successor state	output
1	0 0 0	1 0 0	1 1
1	1 0 0	0 1 0	1 1
0	0 1 0	1 0 1	0 1
1	1 0 1	1 1 0	1 1
1	1 1 0	1 1 1	1 0
1	1 1 1	0 1 1	1 0
0	0 1 1	0 0 1	0 1
1	0 0 1	0 0 0	1 1

Solution of exercise 4.6

Simulation of a convolutional encoder and decoder

The curve of the simulated bit error rates is shown in **figure 28**.

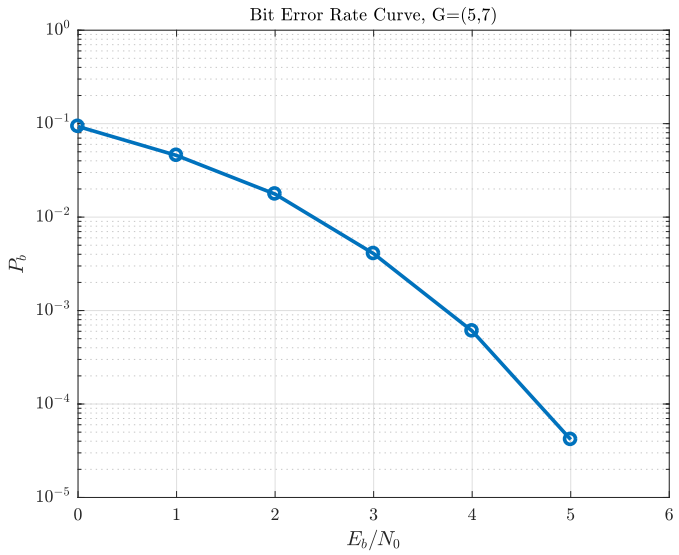

Fig. 28: Simulation result for the bit error rates of the convolutional code $(5, 7)_8$