TUHH
Technische Universität Hamburg-Harburg

INSTITUT FÜR NACHRICHTENTECHNIK
PROF. DR.-ING. GERHARD BAUCH

Exam SS 2016 **(Solved)**

# Information Theory and Coding

| | | |
|---|---|---|
| Name: ………………………………………………….. | Immatriculation number: …………………………… | |
| | Points | of |
| Problem 1 | | |
| Problem 2 | | |
| Problem 3 | | |
| Total points | | |
| Grade | | |

- The following aids are allowed in this exam:
  - 2 Din A4 sheets, handwritten on both sides (4 pages in total)
  - calculator (non-programmable)
  - Pens
- Other aids are not allowed.
- Please use a separate solution sheet for each task.
- Write your name and matriculation number on each solution sheet.
- An arrow next to a question means that this part of the task can be solved independently of the previous questions.
- Please do not write with pencils and do not use a red pen.
- The duration of the exam is 90 minutes.
- The exam consists of **5** pages (including this cover page).
- Switch off your cell phones!

Good luck!

**Problem 1:** Conditional Entropy

⇨ Show, that $H(X|Y)=0$ holds for the conditional entropy $H(X|Y)$, if the random variable $X$ is a function of the random variable $Y$.

Help: $0 \cdot \log 0 = 0$ (for convention, since $x \cdot \log x \to 0$ for $x \to 0$).

Answer:

By definition,

$$\begin{aligned} H(X|Y) &= \sum_{X}\sum_{Y} p_{X,Y}(x,y)\log_2 \frac{1}{p_{X|Y}(x|y)} \\ &= \sum_{x}\sum_{y} p_{X|Y}(x|y)P_Y(y)\log_2 \frac{1}{p_{X|Y}(x|y)} \\ &= \sum_{y} P_Y(y)\left\{\sum_{x} p_{X|Y}(x|y)\log_2 \frac{1}{p_{X|Y}(x|y)}\right\} \end{aligned}$$

If random variable $X$ is a function of the random variable $Y$, then

$$p_{X|Y}(x|y) = \begin{cases} 1 & for\ x = f(y) \\ 0 & \text{otherwise} \end{cases}$$

using this fact, the summation inside the brackets will have only two types of terms:

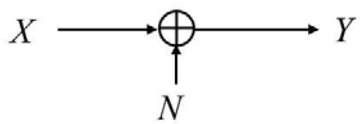
$$\begin{aligned} H(X|Y) = \sum_{y} P_Y(y)\{&1.\log_2 1 + 1.\log_2 1 + \cdots 1.\log_2 1 - 0.\log_2 0 \\ &- 0.\log_2 0 \cdots - 0.\log_2 0\} \end{aligned}$$

Observing that $1.\log_2 1 = 0$ and $0.\log_2 0 = 0$ (from the hint):

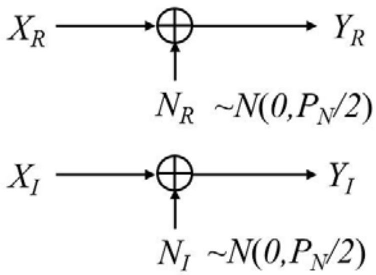
$$H(X|Y) = \sum_{y} P_Y(y).0 = 0$$

**Problem 2:** Capacity of a Complex AWGN Channel

We consider a discrete-time complex AWGN channel as depicted in the following figure:




The complex noise $N$ is circularly symmetric white and Gaussian with power $P_N$. The complex AWGN channel could be the equivalent baseband channel of a bandpass transmission scheme. The complex AWGN channel can be represented by two independent real AWGN subchannels (real part and imaginary part) as depicted in the following figure:




The additive white Gaussian noise in real part and imaginary part is uncorrelated, i.e. $E\{N_R N_I\} = E\{N_R\}\, E\{N_I\}$ and has the same power $E\{N_R^2\} = E\{N_I^2\} = P_N/2$.

The total transmit power of the complex AWGN channel is given by $P_X$.

a) Determine the optimum allocation of the transmit power to the two parallel subchannels (real part and imaginary part).

Answer: According to the waterfilling principle, the transmit power should be uniformly allocated

$$\text{i.e. } P_R = P_I = \frac{P_X}{2}.$$

b) State the equation for the channel capacity of one of the two subchannels, e.g. for the real part, depending on its input power $P_R$.

Answer: Equations for capacity of both real and imaginary subchannels are similar. For the real subchannel:

$$\text{i.e. } C_R = 0.5\log_2\left(1 + \frac{P_R}{P_N/2}\right)$$

c) Derive the equation for the channel capacity of the complex AWGN channel starting from your result from b).

Answer: The capacity of a complex channel is sum of the capacities of its real and imaginary subchannels. Therefore,

$$C = C_R + C_I$$

Using result of subtask b) and a):

$$C = 0.5\log_2\left(1+\frac{P_R}{\frac{P_N}{2}}\right) + 0.5\log_2\left(1+\frac{P_I}{\frac{P_N}{2}}\right)$$
$$= \log_2\left(1+\frac{\frac{P_X}{2}}{\frac{P_N}{2}}\right)$$
$$= \log_2(1+\frac{P_X}{P_N})$$

⇨ d) Sketch qualitatively the channel capacity $C$ of the complex AWGN channel vs. the SNR in dB. Label the axes completely.

Answer: A qualitative rough sketch of a complex AWGN channel is given as:

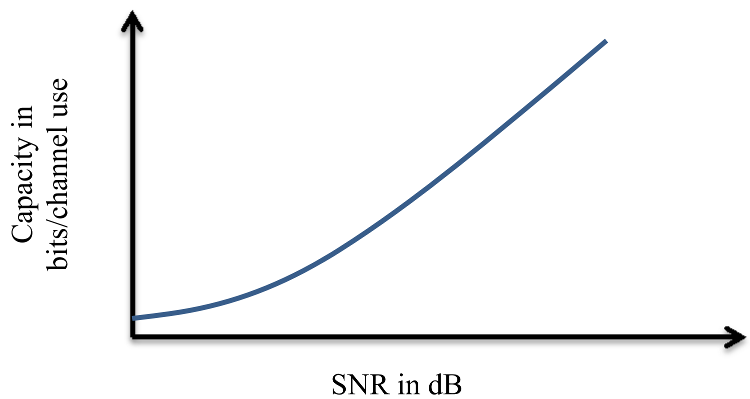



**Figure 1: Capacity of a complex AWGN channel with Gaussian input symbols**

⇨ e) Sketch qualitatively in your plot from d) the capacity $C_{\text{QPSK}}$ of the complex AWGN channel, when the transmit symbols are restricted to QPSK.

Answer: A qualitative rough sketch of a complex AWGN channel with QPSK transmit symbols is given as the red dashed line in the figure below:

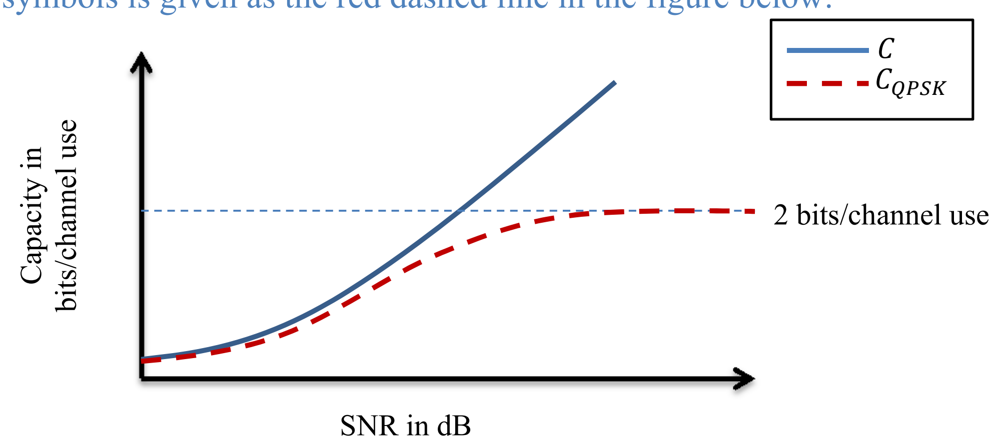



**Figure 2: Capacity of a complex AWGN channel with Gaussian input symbols (blue) and QPSK input symbols (red)**

f) Discuss, if it makes sense from an information theory point of view to apply QPSK modulation at low SNR or high SNR, respectively.

Answer: As seen in Figure 2, the gap between the capacity of AWGN channel with optimum input symbols i.e. $C$, and with QPSK input symbols i.e. $C_{QPSK}$, is small at low SNR. Therefore, it makes sense to use a lower order modulation scheme such as QPSK at low SNR values. Since QPSK transmits 2 bits per channel use, $C_{QPSK}$ cannot exceed 2 bits/channel use. Therefore, the gap between $C$ and $C_{QPSK}$ becomes large at higher SNR and increasing the SNR does not provide any gain in terms of capacity. Hence QPSK is not suitable at high SNR from information theoretic point of view. Instead, higher order modulation schemes such as 16-QAM, 64-QAM etc are preferable.

## **Problem 3:** Code Extension

Code extension refers to a method, where an overall parity check bit is added to each codeword of a given channel code. We denote the parity check matrix of the linear original code by $\mathbf{H}$. The parity check matrix $\mathbf{H}_e$ of the extended code can be obtained by adding first an all-zeros row and then an all-ones column to the original parity check matrix $\mathbf{H}$:

$$\mathbf{H}_e = \begin{bmatrix} & & & 1 \\ & \mathbf{H} & & \vdots \\ & & & 1 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

a) Is the code rate $R_e$ of the extended code increased or decreased compared to the code rate $R$ of the original code? Give reasons !

Answer: For a block code which encodes $K$ bits into $N$ bit code words, its code rate, $R$, is given as:

$$R = K/N$$

Code rate of an extended code will be:

$$R_e = K/(N+1)$$

Since $R_e < R$, code rate is decreased.

b) Assume that the original code has an odd minimum Hamming weight $w_{\min}$. Determine the minimum Hamming distance $d_{\min,e}$ of the extended code depending on the minimum Hamming distance $d_{\min}$ of the original code.

Answer: For linear block codes, the minimum Hamming distance is equal to the minimum hamming weight. The code word with minimum Hamming weight of the original code has an odd number of 1's. Therefore, the additional overall parity check bit in the extended code will be equal to 1 in this code word in order to make the checksum equal to zero.
Therefore, the minimum Hamming weight and consequently the minimum Hamming distance will be increased by 1 compared to the original code. i.e.

$$d_{min,e} = d_{min} + 1$$

c) Assume that the original code has an even minimum Hamming weight $w_{\text{min}}$. Determine the minimum Hamming distance $d_{\text{min},e}$ of the extended code depending on the minimum Hamming distance $d_{\text{min}}$ of the original code.

Answer: For the same reasons explained in b), the additional overall parity check bit in the extended code will be equal to 0 in the code word having minimum Hamming weight.
Therefore, the minimum Hamming weight and consequently the minimum Hamming distance will not be affected by code extension. i.e.

$$d_{min,e} = d_{min}$$

d) Does code extension make sense regarding the error detection/error correction capabilities for codes with even or odd minimum Hamming distance, respectively? Give reasons!

Answer: Error detection/correction capabilities of a code depend on its minimum Hamming distance. For a block code with odd minimum Hamming distance, code extension makes sense because it increases the minimum Hamming distance of the code.
For a block code with even minimum Hamming distance, code extension does not make sense because it does not increase the minimum Hamming distance of the code.

For the remaining problems, we consider an original code with parity check matrix

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

e) Which type of code is defined by the parity check matrix **H** ?

Answer: The parity check matrix defines a rate 1/3 repetition code.

⇨ f) Determine a systematic generator matrix **G** for the original code.

Answer: For a systematic linear block code with parity check matrix of the form $\mathbf{H} = \begin{bmatrix} \mathbf{P}^T \\ \mathbf{I} \end{bmatrix}$ (with $\mathbf{P}$ is $(N-K) \times K$ parity submatrix, $(\quad)^T$ is the transpose operator and $\mathbf{I}$ is $N-K \times N-K$ identity submatrix), its generator matrix is given as:

$$\mathbf{G} = \begin{bmatrix} \mathbf{I} \\ \mathbf{P} \end{bmatrix}$$

where $\mathbf{P}$ is the $(N-K) \times K$ parity submatrix and $\mathbf{I}$ is $K \times K$ identity submatrix. From the given parity check matrix, $\mathbf{P}^T = [1 \quad 1]$. Therefore:

$$\mathbf{G} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

⇨ g) Determine the minimum Hamming distance $d_{\min}$ of the original code.

Answer: Minimum Hamming distance of the rate 1/3 repetition code is $d_{min} = 3$.

⇨ h) Determine the parity check matrix $\mathbf{H}_e$ of the extended code.

Answer: The extended code's parity check matrix will be

$$\mathbf{H}_e = \begin{bmatrix} \mathbf{H} & & 1 \\ & & 1 \\ & & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

i) Determine the set of code words of the extended code.

Answer: The extended code is a rate ¼ repetition code whose code words are

$$\mathbf{x}_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ and } \mathbf{x}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

j) Determine the minimum Hamming distance $d_{\min,e}$ of the extended code.

Answer: since the original code has an odd minimum Hamming distance,

$$d_{min,e} = d_{min} + 1$$

$$d_{min,e} = 3 + 1 = 4.$$