# Digital Communications 2
# Written exam on December 10, 2013

Institute of Telecommunications
Vienna University of Technology

**Please note:**

- You are allowed to use the official lecture notes, a pocket calculator, and a collection of mathematical formulas.
- You are not allowed to use handwritten lecture notes, materials from exercise classes, and precalculated problems.
- Readable handwriting and a clear presentation are mandatory.
- Provide detailed derivations and calculations. If results from the lecture notes are used, they have to be referenced unambiguously.
- Due to changes of the modus operandi for the exercise class since the 08/09 winter semester, the maximum number of achievable credits will be scaled from 80 to 90 for the corresponding candidates.

**Problem 1 (20 credits)**

Consider transmission of codewords $\mathbf{c} = (c_0\ c_1\ c_2\ c_3\ c_4)^T$ with $c_n \in \{0, 1, 2, 3\}$ over a memoryless HISO channel $q_n = a_n + z_n$, where $c_n = 0, 1, 2,$ and 3 correspond to $a_n = -6, -3, 3,$ and 6, respectively. The $z_n$ are statistically independent with pdf

$$f_{Z_n}(z) = \begin{cases} \frac{1}{16}(4 - |z|)\,, & |z| \leq 4 \\ 0\,, & \text{otherwise.} \end{cases}$$

**a)** The receiver first performs symbol-by-symbol ML detection of $a_n$ based on $q_n$, thereby converting the HISO channel to a HIHO channel $c_n \rightarrow v_n$. Sketch that HIHO channel and calculate its transition probabilities. Is it a symmetric DMC?

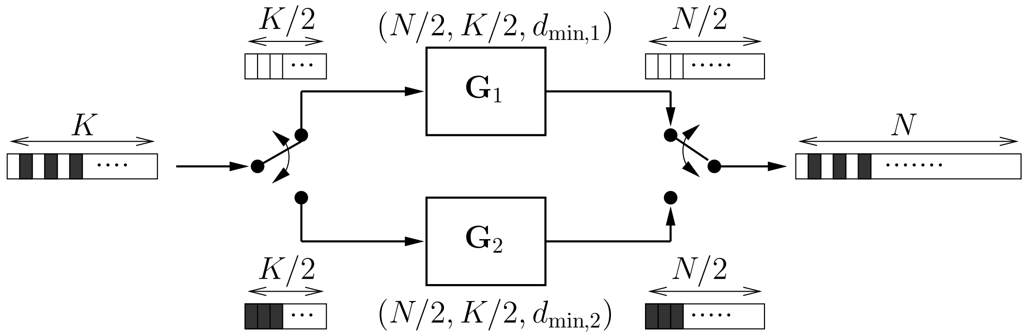
**b)** Calculate the block transition probability $p_{\mathbf{V}|\mathbf{C}}(\mathbf{v}^{(1)}|\mathbf{c}^{(1)})$ of the HIHO channel for the codeword $\mathbf{c}^{(1)} \leftrightarrow \mathbf{a}^{(1)} = (-3\ \ -3\ \ 6\ \ 3\ \ -6)^T$ and the senseword $\mathbf{v}^{(1)} = (2\ \ 1\ \ 3\ \ 1\ \ 0)^T$. Determine $d_{\mathrm{H}}(\mathbf{c}^{(1)}, \mathbf{v}^{(1)})$.

**c)** Find a codeword $\mathbf{c}^{(2)}$ such that

$$p_{\mathbf{V}|\mathbf{C}}(\mathbf{v}^{(1)}|\mathbf{c}^{(2)}) > p_{\mathbf{V}|\mathbf{C}}(\mathbf{v}^{(1)}|\mathbf{c}^{(1)}) \quad \text{even though} \quad d_{\mathrm{H}}(\mathbf{c}^{(2)}, \mathbf{v}^{(1)}) > d_{\mathrm{H}}(\mathbf{c}^{(1)}, \mathbf{v}^{(1)})\,.$$

**d)** Is the block decoder defined by the decision rule $\hat{\mathbf{c}}(\mathbf{v}) = \arg\min_{\mathbf{c}\in\mathcal{C}} d_{\mathrm{H}}(\mathbf{c}, \mathbf{v})$ equal to the ML block decoder?

Encoder A:




Encoder B:

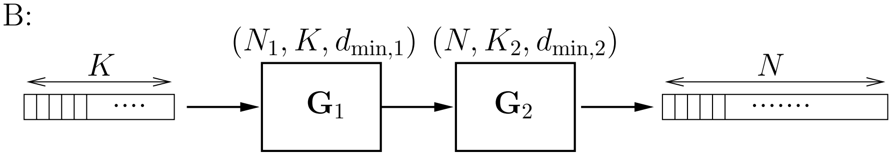



Figure 1: The two encoders.

**Problem 2 (20 credits)**

The two encoders A and B depicted in Figure 1 implement the encoding of binary block codes $\mathcal{C}_{\mathrm{A}}$ (minimum distance $d_{\mathrm{min,A}}$) and $\mathcal{C}_{\mathrm{B}}$ (minimum distance $d_{\mathrm{min,B}}$), respectively. The generator matrices $\mathbf{G}_1$ and $\mathbf{G}_2$ in Figure 1 define linear component codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with minimum distances $d_{\mathrm{min},1}$ and $d_{\mathrm{min},2}$, respectively (note that these component codes are generally different for encoder A and encoder B).

**a)** Are the codes $\mathcal{C}_{\mathrm{A}}$ and $\mathcal{C}_{\mathrm{B}}$ linear? Are the encoders A and B systematic, if the encoders for $\mathcal{C}_1$ and $\mathcal{C}_2$ are systematic?

**b)** Find the minimum distance $d_{\mathrm{min,A}}$ of code $\mathcal{C}_{\mathrm{A}}$.

**c)** Consider code $\mathcal{C}_{\mathrm{B}}$. Is it possible that $d_{\mathrm{min,B}} < d_{\mathrm{min},2}$?

**d)** For encoder A, assume that both $\mathcal{C}_1$ and $\mathcal{C}_2$ are $(4,3)_2$ single-parity-check codes. Calculate the rate $R_{\mathrm{A}}$ of $\mathcal{C}_{\mathrm{A}}$, find a generator matrix $\mathbf{G}_{\mathrm{A}}$ and a check matrix $\mathbf{H}_{\mathrm{A}}$, and determine the resulting minimum distance $d_{\mathrm{min,A}}$.

**e)** For encoder B, assume that $\mathcal{C}_1$ is a $(7,4)_2$ Hamming code and $\mathcal{C}_2$ is a single-parity-check code. Specify the blocklength and dimension of $\mathcal{C}_2$. Calculate the rate $R_{\mathrm{B}}$ of $\mathcal{C}_{\mathrm{B}}$, find a generator matrix $\mathbf{G}_{\mathrm{B}}$ and a check matrix $\mathbf{H}_{\mathrm{B}}$, and determine the resulting minimum distance $d_{\mathrm{min,B}}$.

**Problem 3 (20 credits)**

Consider the polynomial $g(x) = x^3 + x^2 + 1$.

**a)** Show that $g(x)$ is the generator polynomial of a primitive cyclic code of blocklength $N=7$ over GF(2).

**b)** What is the dimension of that code?

**c)** Calculate all zeros of $g(x)$ in the (smallest possible) splitting field.

**d)** Use the result of part c) to check if $v_1(x) = x^4 + x^2 + x + 1$ and $v_2(x) = x^4 + x + 1$ are codewords.

**e)** What is the rate of the dual code?

**Problem 4 (20 credits)**

In the following dual codes of Reed-Solomon codes are investigated. Consider a Reed-Solomon code $\mathcal{C}$ over GF($q$) with minimum Hamming distance $d_{\min}$ and frequency parameter $k_1$.

**a)** Show that the dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is a Reed-Solomon code. Determine the minimum Hamming distance $d_{\min}^{\perp}$ and the frequency parameter $k_1^{\perp}$ of $\mathcal{C}^{\perp}$.

**b)** Use the results of **a)** to show that no *self-dual* Reed-Solomon code can exist ($\mathcal{C}$ is self-dual iff $\mathcal{C} = \mathcal{C}^{\perp}$).

**c)** Design a Reed-Solomon code over $\mathrm{GF}(8) = \{0, 1, z, z^2, z^3, z^4, z^5, z^6\}$ ($z \in \mathrm{GF}(8)$ is a primitive element, i.e. $z^3 + z + 1 = 0$), such that its dual code has a minimum Hamming distance $d_{\min}^{\perp} = 5$ and a frequency parameter $k_1^{\perp} = 3$.

**c1)** Determine the blocklength $N = N^{\perp}$, the rates $R$ and $R^{\perp}$, $d_{\min}$ and $k_1$.

**c2)** Calculate the generator polynomials $g(x)$ and $g^{\perp}(x)$ and the check polynomials $h(x)$ and $h^{\perp}(x)$.

**c3)** Consider a systematic encoding of the dataword $\mathbf{u} = (z^0\ z^5\ z^1)^T$ for the dual code in the frequency domain. Determine the corresponding codeword in time and frequency domain.

**c4)** Check whether $\mathbf{c} = (z^0\ z^5\ z^3\ z^1\ z^6\ z^4\ z^2)^T$ is a valid codewort of the dual code.