Digital Communications 2
Written exam on March 05, 2014

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 the $(8,4)_2$ extended binary Hamming code $\mathcal{C}$, which consists of the $(7,4)_2$ Hamming code and a single parity check bit. Furthermore, consider the $(8,7)_2$ single parity check code $\mathcal{C}'$.

a) Find the generator and check matrices of $\mathcal{C}$.

b) Find the weight enumerators of $\mathcal{C}$ and $\mathcal{C}'$.

c) Consider transmission over a binary symmetric channel with bit inversion probability p. Find the probability of an undetected error for $\mathcal{C}$ and $\mathcal{C}'$.

Problem 2 (20 credits)

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

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

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_{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 $d_{\min,\mathrm{A}}$.

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_{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 $d_{\min,\mathrm{B}}$.

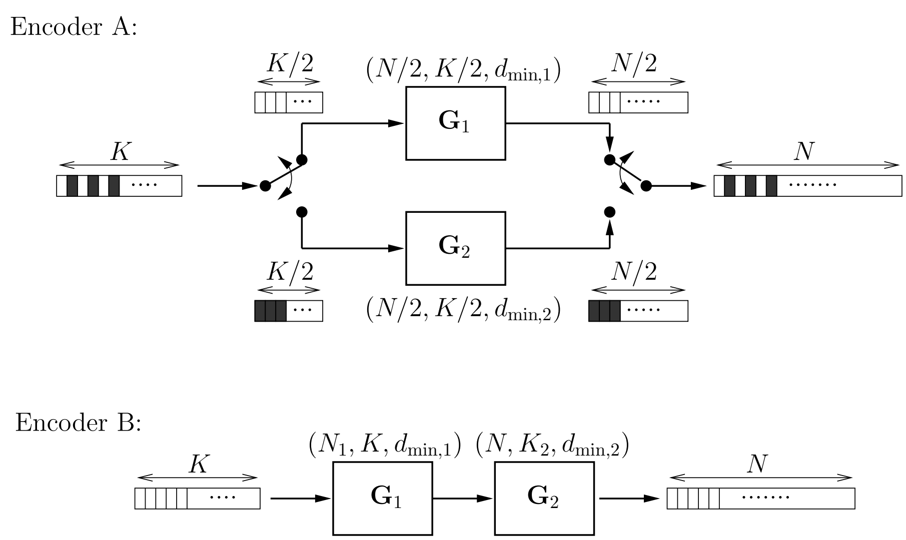

Figure 1: The two encoders.

Problem 3 (20 credits)

Consider the set of all cyclic codes of length $N = 4$ over $\mathrm{GF}(4) = \{0, 1, 2, 3\}$.

a) Determine the addition and multiplication tables for GF(4).

b) Find all generator polynomials and the corresponding code rates. Which of these generator polynomials do not define a useful code?

c) Choose a generator polynomial of degree 2 and use two different methods to check whether $v(x) = 2x^3 + 2x^2 + 1$ is a codeword.

Problem 4 (20 credits)

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 if $\mathcal{C} = \mathcal{C}^{\perp}$).

c) Design a Reed-Solomon code over $\text{GF}(8) = \{0, 1, z, z^2, z^3, z^4, z^5, z^6\}$ ($z \in \text{GF}(8)$ is a primitive element, i.e., $z^3 + z + 1 = 0$) such that its dual code has minimum Hamming distance $d_{\min}^{\perp} = 5$ and 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) For the dual code, consider systematic encoding of the dataword $\mathbf{u} = (z^0\, z^5\, z^1)^T$ in the frequency domain. Determine the corresponding codeword in the frequency domain and in the time 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.