Digital Communications 2
Written exam on January 30, 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)

The *weight enumerator* of a linear $(N, K, d_{\min})_q$ block code is defined as

$$A(x) = \sum_{i=0}^{N} A_i x^i \,,$$

where A_i is the number of codewords with Hamming weight i.

a) Prove the following properties:

- **a1)** $A_0 = 1$,
- **a2)** $A_N \leq (q-1)^N$,
- **a3)** $A_i = 0$ for $0 < i < d_{\min}$,
- **a4)** $A_{d_{\min}} \geq 1$,
- **a5)** $A(1) = q^K$.

b) Calculate $A(x)$ for the following $(N, K)_q$ codes:

- **b1)** $(N, 1)_q$ repetition code,
- **b2)** $(7, 4)_2$ Hamming code,
- **b3)** $(N, N-1)_2$ single-parity-check code.

Problem 2 (20 credits)

Consider the binary encoder of $\mathcal{C}$ defined as

$$(u_0 \;\; u_1)^T \to (u_0 - u_1 \;\; u_0 \;\; u_1 \;\; u_1 \;\; u_0)^T \,.$$

a) Find the parameters N and K of $\mathcal{C}$. Is $\mathcal{C}$ a cyclic code?

b) Find a generator and a check matrix for $\mathcal{C}$. What is the minimum distance?

c) Construct a standard array for $\mathcal{C}$. How many codewords are in the interstitial region? Perform MD decoding and BMD decoding for the sensewords $(1\,1\,0\,1\,1)^T$ and $(0\,0\,1\,1\,1)^T$.

d) Construct a decoding table and perform syndrome decoding of the two sensewords given in c).

e) Calculate the probability of an unsuccessful transmission over a BSC with bit inversion probability $p = 0.2$ followed by a BMD. Compare the result to the block error probability of uncoded transmission.

Problem 3 (20 credits)

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

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

b) What is the dimension of that code?

c) Determine the smallest possible splitting field $\mathrm{GF}(q^m)$ of $g(x)$.

d) Calculate all zeros of $g(x)$ and $h(x)$ in the (smallest possible) splitting field. Represent the zeros in terms of a primitive element z of that splitting field.

e) Use two different methods to check if $v_1(x) = x^4 + x^2 + x + 1$ and $v_2(x) = x^4 + x + 1$ are codewords.

f) What is the rate of the dual code?

Problem 4 (20 credits)

Consider a Reed-Solomon (RS) code $\mathcal{C}$ of blocklength $N = 15$, minimum distance $d_{\text{min}} = 13$, and band position parameter $k_1 = 14$.

a) What is the underlying Galois field?

b) Specify the rate R.

c) Provide expressions for the generator and check polynomials in terms of a primitive element $z \in \text{GF}(q)$.

d) Consider systematic encoding of the dataword $\mathbf{u} = (z^0\ z^5\ z^1)^T$ in the frequency domain. Specify the resulting codeword $\mathbf{c}$ in the frequency domain and in the time domain.

Hint: It is known that

$$\mathcal{F}^{-1}\left\{(0\ 0\ 0\ 0\ 0\ z^0\ z^5\ z^1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T\right\}$$
$$= (z^8\ z^{13}\ z^1\ z^{12}\ z^5\ z^{13}\ z^1\ z^2\ z^{13}\ z^7\ z^{11}\ z^0\ z^1\ z^{10}\ z^2)^T .$$

e) Determine the check frequencies of the dual code $\mathcal{C}^\perp$.

f) Is $\mathcal{C}^\perp$ an RS code? If yes, determine the band position parameter $k_1^\perp$.