*IV054 Coding, Cryptography and Cryptographic Protocols*
**2018 - Exercises II.**

1. How many codewords has the smallest ternary linear code that contains codewords 1000000, 0001000, 0000010 and 0001020?

2. Let $C_1, C_2, C_3 \subseteq \mathbb{F}_q^n$ be linear codes. Decide whether the following codes are linear. Prove your answers.

   (a) $C_1 \cdot C_2 = \{u \cdot v \mid u \in C_1, v \in C_2\}$, where $\cdot$ denotes concatenation

   (b) $C_1 \triangle C_2$, where $\triangle$ denotes symmetric difference

   (c) $C_1 \triangle C_2 \triangle C_3$

3. Consider a binary $[n, k]$-code $C$ consisting of all linear combinations from $S = \{100110, 110011, 111100, 010101\}$.

   (a) Find the generator and parity check matrix in standard form.

   (b) Find $n$ and $k$ of this code. What is the minimal distance of $C$?

   (c) Find all coset leaders and their corresponding syndromes. Decode received word 101101 using syndrome decoding.

4. Prove that the code

$$C = \{a_1 \cdots a_n \mid a_1, ..., a_n \in \mathbb{F}_q, \sum_{i=1}^{n} a_i^q = 0\}$$

   is linear and find its parity check matrix.

5. Decide and prove which of the following 5-ary codes are linear:

   (a) $C_1 = \{x_1 \cdots x_5 \mid x_1 + x_2 + x_3 + x_4 + x_5 \pmod 2 = 0\}$

   (b) $C_2 = \{x_1 \cdots x_5 \mid x_1 + x_2 + x_3 + x_4 + x_5 \pmod 2 = 1\}$

   (c) $C_3 = \{x_1 \cdots x_5 \mid f_1(x_1) + f_2(x_2) + f_3(x_3) + f_4(x_4) + f_5(x_5) \pmod 5 = s\}$,
   where $f_i(x) = a_i(x) + b_i$ are linear functions and $s = b_1 + b_2 + b_3 + b_4 + b_5 \pmod 5$.

6. Prove the following statement. Let $C$ be a linear code with the parity check matrix $H$. Then $h(C)$ is the size of the smallest set of linearly dependent rows of $H$.

7. Let $C$ be an $[n, k, d]_q$-code. Consider a code $C'$ constructed from $C$ by removing the $i$-th and $j$-th coordinate of each codeword:

$$C' = \{x_1 \cdots x_{i-1} x_{i+1} \cdots x_{j-1} x_{j+1} \cdots x_n \mid x_1 \cdots x_n \in C\}$$

   (a) Prove that $C'$ is a linear code.

   (b) Find the values $n$, $k$, $d$ of $C'$.

8. Show that the binary code with the following generator matrix is equivalent to a Hamming code.

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