*IV054 Coding, Cryptography and Cryptographic Protocols*
**2015 - Exercises I.**

1. Consider a perfect binary $(n, M, 5)$-code. Find the two lowest values of $n$ for which such a code exists.

2. Let $C = \{111111, 101000, 000101, 010010\}$. Suppose the codewords are transmitted using a binary symmetric channel with an error probability $p < \frac{1}{2}$.

   (a) How many errors can $C$ detect?

   (b) How many errors can $C$ correct?

   (c) Calculate the probability of an undetected error.

3. Let $n$, $q$ be positive integers and let $q \geq 2$. Show that

$$A_q(2n, 2) \geq A_{2q}(n, 4).$$

4. Consider a source producing 8 letters (A-H) with probabilities given in the table below.

| Letter | Probability |
|---|---|
| A | 0.40 |
| B | 0.27 |
| C | 0.10 |
| D | 0.08 |
| E | 0.06 |
| F | 0.04 |
| G | 0.03 |
| H | 0.02 |

   (a) Construct the Huffman code for this source.

   (b) Calculate the average length of codewords of this code and compare it to the bound given by Shannon's coding theorem.

5. (a) Give an example of a ternary $(6, 7, 4)$-code, all of whose words are palindroms (*ie.* their $i$-th letter is equal to their $(7 - i)$-th letter for $i \in \{1, 2, 3\}$).

   (b) Give an example of four binary pairwise disjoint $(4, 4, 2)$-codes.

6. For $n \in \mathbb{N}$, we will denote the set of all binary codewords of length $n$ as $\mathcal{C}_n$.

   (a) Let $n \in \mathbb{N}$ and $p = (p_1, \ldots, p_n) \in (\mathbb{R}^+)^n$ and define a function $d_p : \mathcal{C}_n \times \mathcal{C}_n \to \mathbb{R}_0^+$ as

$$d_p(w_1, w_2) = \sum_{i=1}^{n} p_i \cdot |w_1(i) - w_2(i)|,$$

   where $w(i)$ denotes the $i$-th coordinate of the word $w$. Show that $d_p$ is a metric which generalizes the Hamming distance on $\mathcal{C}_n$.

   (b) Let $n \in \mathbb{N}$ and $p = (p_1, \ldots, p_n) \in (\mathbb{R}^+)^n$. Calculate the sum

$$\sum_{w_i, w_j \in \mathcal{C}_n} d_p(w_i, w_j).$$