IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises II.

1. (a) What is the maximum number of codewords in a linear binary code of length 8 and minimal distance of 3 bits?
   (b) What is the maximum dimension of a linear ternary code of length 4 in which the Hamming distance between every two of its distinct words is odd?

2. Consider a binary linear code C generated by the matrix

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

   (a) Construct a standard array for C.
   (b) Decode the received word 000101.
   (c) Is this code perfect?
   (d) Find an example of a received word with two errors which is not decoded correctly using the coset decoding method.

3. Consider the following 7-ary codes C_1, C_2 and C_3 of length 3 such that

   (a) $a_1a_2a_3 \in C_1 \iff a_1 \cdot a_2 + a_3 \equiv 0 \pmod 7$;
   (b) $a_1a_2a_3 \in C_2 \iff a_1 + a_2 + a_3 \equiv 0 \pmod 7$;
   (c) $a_1a_2a_3 \in C_3 \iff a_1 + a_2 + a_3 \equiv 3 \pmod 7$.

   Decide whether they are linear codes.

4. What is the number of different binary self-dual $[4, 2]$-codes.

5. Let $n \in \mathbb{N}$ and let C be the ternary code of length n satisfying

$$a_1a_2 \ldots a_n \in C \Leftrightarrow a_1 + a_2 + \cdots + a_n \equiv 0 \pmod 3.$$

   Show that C is linear and determine the number of its words.

6. Let C be a linear code over $\mathbb{F}_q$. Show that either all codewords of C begin with 0 or exactly $\frac{1}{q}$ of codewords of C begin with 0.