IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises II.

1. Consider a ternary code C with the following generator matrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

   (a) Find a parity check matrix of C.

   (b) Find a standard array for C and a syndrome for each coset.

   (c) Using the computed syndroms, decode words 0201 and 1111.

2. (a) Consider linear $[2,1]$-codes with 4 codewords. What are the possible values for minimal distance d?

   (b) Find all linear $[2,2]$-codes with 4 codewords.

3. Let G_1, G_2 be generator matrices of an (n_1, k, d_1) linear code and an (n_2, k, d_2) linear code, respectively. Find the values n, k, d of codes with generator matrices

$$\mathbf{G} = [G_1 | G_2]$$

   and

$$\mathbf{G}' = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}.$$

   Explain your reasoning.

4. Consider a ternary code C with the following generator matrix:

$$\mathbf{G} = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 \\ 1 & 2 & 1 & 2 & 0 \\ 1 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

   (a) Transform G to its standard form.

   (b) How many codewords does the code C have?

   (c) How many errors can C correct?

5. Prove that the Reed-Muller code $R(1,m)$ contains $2^{2^m - m - 1}$ cosets.

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

$$C^i = \{x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n \mid x_1 x_2 \dots x_n \in C\}.$$

   (a) Prove that C^i is a linear code.

   (b) Find the values n, k, d of C^i.

7. For every even n, give an example of a self-dual binary linear code of length n.