IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises II.

1. Consider the following parity check matrix of the linear code C

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

   (a) Find the standard generator matrix for C.
   (b) What is the minimal distance of C?
   (c) Use H to determine whether the codeword 1100111 belongs to C?
   (d) Decode the received word 1010101.

2. Consider matrices

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

   (a) Prove that G_1 and G_2 generate binary $[4,2]$-code C_1 and $[5,3]$-code C_2, respectively.
   (b) Consider $[9,5]$-code C where

$$C = \{w_1 w_2 \mid w_1 \in C_1 \wedge w_2 \in C_2\}.$$

   Show that C is also binary linear code and find the generator matrix for C.

3. Consider the following 5-ary codes C_1, C_2, C_3 of length 3 such that

   (a) $a_1a_2a_3 \in C_1 \Leftrightarrow 2a_1 + a_2 - a_3 \equiv 0 \pmod 5$
   (b) $a_1a_2a_3 \in C_2 \Leftrightarrow a_1 \cdot 2a_2 \equiv 0 \pmod 5$
   (c) $a_1a_2a_3 \in C_3 \Leftrightarrow 2a_1 + a_2 - a_3 \equiv 4 \pmod 5$

   Decide whether C_1, C_2, C_3 are linear codes.

4. Consider the following parity check matrix for the linear code C

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

   (a) List all codewords of the code C.
   (b) How many different cosets does C have? Write down all coset leaders.
   (c) Write down all error vectors which form the same coset as the error vector 000011.

5. Prove the following theorem:
   Let C be a q-ary (n,k) code. Every set of $s-1$ columns of its parity check matrix H are linearly independent if and only if $w(C) \geq s$.

6. Consider a ternary code with the following parity check matrix

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

   Show that this code has a minimum distance 4.
   (*Hint:* Use the result from the previous exercise.)

7. Consider a linear $[n,k]$-code C with corresponding parity check matrix H.

   (a) Describe the kernel of linear map represented by H.
   (b) Determine the rank of H. Explain your reasoning.