IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises II.

1. *(3 points)* For each of the following codes, decide whether it is a linear code.
   (a) $C_1 = \{w \in \{0,1\}^4 \,|\, \text{number of 1's is odd}\}$
   (b) $C_2 = \{w \in \{0,1\}^5 \,|\, \text{number of 1's is even}\}$
   (c) $C_3 = \{021, 201, 102, 111, 210, 000, 222, 120\}$ over $\mathbb{F}_3$

2. *(4 points)* Are the codes given by the following generator matrices equivalent to Hamming codes? Prove your answer.
   (a)
   $$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$
   (b)
   $$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

3. *(3 points)* Prove that all Hamming codes are perfect.

4. *(8 points)* Consider the following parity check matrix of the linear code C.
   $$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$
   (a) Find the standard generator matrix for C.
   (b) What is the minimal distance of C?
   (c) Compute the syndrome decoding table for H and decode the received word 10111.

5. *(4 points)* A code C is called *self-dual* if $C = C^\perp$.
   Decide whether the following generator matrices generate binary self-dual codes.
   (a)
   $$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$
   (b)
   $$G_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

6. *(4 points)* Let C_1 and C_2 be q-ary linear codes of the same length. Define
   $$C_1 + C_2 = \{c_1 + c_2 \,|\, c_1 \in C_1, c_2 \in C_2\}.$$
   Prove that
   $$(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp.$$

7. *(4 points)* Let $B_q(n,d)$ be the largest number of codewords such that there is a q-ary $[n,k,d]$-code. Prove the following theorem.
   $$B_q(n,d) \le qB_q(n-1,d)$$