IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises II.

1. Let C be the binary linear code which has the following parity check matrix:

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

   (a) Find a codeword of minimum weight.
   (b) Prove that all codewords have even parity.
   (c) Determine n, k and d.

2. Let C be a code which does not contain any word of even weight. Decide whether the following statements hold. Explain your reasoning.
   (a) C is linear,
   (b) $h(C) = 5$,
   (c) $C \subseteq C^{\perp}$.

3. Show that the following codes are perfect:
   (a) the codes $C = \mathbb{F}_q^n$,
   (b) the codes consisting of exactly one codeword,
   (c) the binary repetition codes of odd length,
   (d) the binary codes of odd length consisting of a vector c and the complementary vector c' (with ones and zeros interchanged),
   (e) the $[23, 12, 7]$ binary Golay code.

4. Give the standard form of generator matrix G and parity check matrix H of a $[15, 11, 3]$ binary Hamming code. Using these matrices to encode the message $u = 11111100000$ and decode the message $v = 111000111000111$.

5. (a) Show that in a linear binary code, either all codewords have even weight, or exactly half have even weight and half have odd weight.
   (b) Show that in a linear binary code, either all codewords begin with 0, or exactly half begin with 0 and half begin with 1.

6. Answer each of the following questions. Explain your reasoning.
   (a) Let C be an $[n, k]$ code over $\mathbb{F}_q$ with a generator matrix G and a parity check matrix H. What is the result of the following expressions:
      - $G \cdot H^T$,
      - $H \cdot G^T$.
   (b) Let C be an $[n, k]$ self-dual code over $\mathbb{F}_q$.
      - What is the relationship between q and the weights of codewords for $q = 2$ and $q = 3$?
      - Can you generalize this result for an arbitrary q?

7. Prove that a perfect t-error-correcting linear code of length n has precisely $\binom{n}{i}$ cosets of weight i $(0 \leq i \leq t)$ and does not have other cosets.