IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises II.

1. Let $C_1, C_2 \subseteq F_q^n$ be linear codes. Decide whether the following codes are linear codes. Prove your answer.
   (a) $C_1 \cap C_2$
   (b) $C_1 \cup C_2$
   (c) $(C_1 \cup C_2) \setminus (C_1 \cap C_2)$

2. Consider a ternary code C such that the following holds:

$$x_1x_2x_3x_4 \in C \Leftrightarrow 2x_1 + x_2 + 2x_3 + x_4 \equiv 0 \pmod 3 \wedge x_1 + x_2 + 2x_3 + 2x_4 \equiv 0 \pmod 3$$

   (a) Show that C is a linear code.
   (b) Determine the generator matrix G for the code C in the standard form.

3. Consider a binary $[n, k]$-code C with the following parity check matrix

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

   (a) Determine parameters n, k, $h(C)$ and $|C|$.
   (b) Find the standard form of the generator matrix G for the code C.
   (c) Construct a standard array for C.

4. Let C_1 be an $[n, k_1, d]$-code and C_2 be an $[n, k_2, 2d]$-code. Let C be the code consisting of all codewords of the form

$$C = \{(x_1, x_2, \dots, x_n, x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) \mid (x_1, \dots, x_n) \in C_1 \text{ and } (y_1, \dots, y_n) \in C_2\}.$$

   Determine parameters n, k and d of C.

5. Let M_{2n}, the matrix used in construction of Hadamard codes, be defined recursively as follows

$$M_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

   and

$$M_{2n} = \begin{bmatrix} M_n & M_n \\ M_n & \bar{M}_n, \end{bmatrix}$$

   where $\bar{M_n}$ is the complementary matrix to M_n (with 0 and 1 interchanged).
   Show that any two rows of M_{2n} differ in exactly n positions.

6. A code C is *self-orthogonal* if $C \subseteq C^\perp$.
   A code C is *self-dual* if $C = C^\perp$.

   Proof the following:
   Let C be an $[n, k]$-code. Then C is self-dual if and only if C is self-orthogonal and $n = 2k$.

7. For $n \in \mathbb{N}$, $n > 2$, and q a power of a prime, give an example of a q-ary $[n, k]$-code ($k \in \mathbb{N}$ can be chosen arbitrarily) that is maximum distance separable (MDS) such that its dual code is an MDS-code as well.