IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises II.

1. *(3 points)* Decide whether the following codes are linear. Justify your answer.
   (a) A binary code consisting of codewords $\{010, 101, 111\}$.
   (b) $C' = \{\bar{c} \mid c \in C\}$, where C is a binary linear code and $\bar{c}$ denotes a bitwise NOT of codeword c.
   (c) $C'' = \{c_1 \otimes c_2 \mid c_1 \in C_1, c_2 \in C_2\}$, for two binary linear codes C_1 and C_2, where $\otimes$ denotes bitwise XOR operation.

2. *(4 points)* Consider the binary linear code C generated by the following matrix:
$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$
   (a) Determine n, k and d of C.
   (b) Construct a standard array for C.
   (c) Use the standard array to decode word 11110 received with errors.

3. *(3 points)* Two linear codes are called *permutation equivalent* if they are equal up to a fixed permutation on the codeword coordinates.

   Decide whether the binary linear codes generated with the following matrices are permutation equivalent.

   (a)
$$G_1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$
   (b)
$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$
   (c) In general, given generator matrices, is it possible to decide the permutation equivalence of the corresponding codes?

4. *(2 points)* Consider the binary linear code C with generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$
   (a) Find the parity-check matrix of C.
   (b) Find the syndrome of the word 100001.

5. *(3 points)* Find the smallest
   (a) binary;
   (b) ternary

   linear code containing codewords $\{1001, 0111, 1110\}$.

6. *(4 points)* Let C be a binary linear code with parity-check matrix
$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$
   Without exhaustively listing all the codewords of C, show that all the codewords have even weight.

7. *(6 points)* For linear codes C_1, C_2, prove that if C_1 is equivalent to C_2, then $C_1^{\perp}$ is equivalent to $C_2^{\perp}$.