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

1. *(4 points)* Decide whether the following binary codes are cyclic codes. Explain your reasoning.
   (a) $C_1 = \{00000, 11100, 01110, 00111, 10011, 11001\}$
   (b) $C_2 = C \cup (1\dots1 + C)$, where C is a binary cyclic code and $1\dots1$ is the all **1** codeword.

2. *(2 points)* Let σ denote a *circular right shift* operation. Find all binary words w
   (a) of length n such that $\sigma(w) = w$;
   (b) of length 6 such that $\sigma^2(w) = w$;
   (c) of length 6 such that $\sigma^3(w) = w$.

3. *(5 points)* For a binary code $C = \langle 1 + x^2 + x^3 \rangle$ in R_7.
   (a) Find the generator matrix G.
   (b) Find the parity check matrix H.
   (c) Using polynomials, encode the message 1010.

4. *(3 points)*
   (a) How many binary cyclic codes of length 9 are there?
   (b) How many ternary cyclic codes of length 9 are there?
   (c) How many ternary cyclic codes of length 9 have dimension 7?

5. *(5 points)* A code C is called *self-orthogonal*, if $C \subseteq C^\perp$. Let $g(x)$ be a generator polynomial of a cyclic code C of length n, and $x^n - 1 = g(x)h(x)$. Show that C is self-orthogonal if and only if the reciprocal polynomial $\bar{h}(x)$ divides $g(x)$.

6. *(5 points)* Let C_1 and C_2 be cyclic codes of the same block length with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Find the generator polynomial of the smallest cyclic code C such that $C_1 \cup C_2 \subseteq C$.

7. *(6 points)* Let first-order Reed-Muller codes $RM(1,m)$, $m \geq 1$, be defined recursively as follows.
   - $RM(1,1) = \{00, 01, 10, 11\}$
   - $RM(1,m) = \{(x,x) \mid x \in RM(1,m-1)\} \cup \{(x, x + \mathbf{1}) \mid x \in RM(1,m-1)\}$ for $m > 1$.

   (a) List all codewords of $RM(1,3)$ and $RM(1,4)$.
   (b) Provide a recursive construction of generating matrices for $RM(1,m)$.
   (c) Prove that $RM(1,m)$ is $[2^m, m+1, 2^{m-1}]$-code whose codewords, except the all zeroes **0** and all ones **1**, have weight 2^{m-1}.