IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises III.

1. Consider a binary cyclic code C of length 6 with a generator polynomial $x^4 + x^3 + x + 1$.
   (a) Find a parity check polynomial of C.
   (b) Use the polynomial found to check whether the words 111000 and 111010 belong to C.
2. Which of the following binary codes are cyclic? Which of them are equivalent to a cyclic code?
   (a) $C_1 = \{0000, 1110, 1011, 0111, 1101\}$;
   (b) $C_2 = \{111, 100, 010, 001\}$;
   (c) C_3 with generator matrix G_1:
   $$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix};$$
   (d) C_4 with generator matrix G_2:
   $$G_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$
3. Let C be a binary cyclic code of length 15 and dimension 11 such that each word from $C^\perp$ has even weight and $011111111110000 \in C$. Find a generator polynomial and a minimum distance of C.
4. Which $\mathrm{Ham}(r, 2)$ codes are maximum distance separable?
5. Consider a binary cyclic code C of length 7 with generator polynomial $g(x) = x^3 + x + 1$. Find a parity check matrix and a generator polynomial of $C^\perp$.
6. How many quinary cyclic codes of length 6 are there? Give a generator polynomial for each such code and one generator matrix for each dimension.
7. A cyclic code C is trivial if and only if its generator polynomial is zero. Consider different non-trivial cyclic codes C_1 and C_2 and give an example of a cyclic code C_3 or prove that such does not exist for the following cases:
   (a) $C_3 = \neg C_1 \cap C_2$, where $\neg$ is bitwise negation operator;
   (b) $C_3 = C_1 \circ 0$, where $\circ$ is concatenation operator;
   (c) $C_3 \supseteq C_1 \cup C_2$.