IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises III.

1. Let q, $n \in \mathbb{N}$, where q is a prime number and let C_1, C_2 be cyclic q-ary codes of length n. In each of the following cases, determine if C_3 is necessarily a cyclic code.
   (a) $C_3 = C_1 \setminus C_2$;
   (b) $C_3 = (C_1 \cup C_2) \setminus (C_1 \cap C_2)$;
   (c) $C_3 = \{a_1 b_1 a_2 b_2 \dots a_n b_n \mid a_1 a_2 \dots a_n \in C_1, b_1 b_2 \dots b_n \in C_2\}$;
   (d) $C_3 = \{a_1 b_1 a_2 b_2 \dots a_n b_n \mid a_1 a_2 \dots a_n, b_1 b_2 \dots b_n \in C_1\}$;
   (e) $C_3 = \{w_1 - w_2 \mid w_1 \in C_1, w_2 \in C_2\}$.

2. Consider the following binary $[8, 4]$-code C with a generator matrix

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

   (a) Prove that C is a cyclic code.
   (b) Find the generator polynomial of C.

3. Let C_1, C_2 be q-ary cyclic codes of length n with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Show that $C_3 = C_1 \cap C_2$ is also cyclic. Find the generator polynomial of C_3.

4. Determine the number of
   (a) all cyclic ternary codes of length 16;
   (b) all cyclic quaternary codes of length 12.

5. Find the parity check matrix and list all codewords of the binary cyclic code $C = \langle 1 + x + x^2 \rangle$ in $\mathcal{R}_3$.

6. Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$. Let $v(x)$ be a polynomial in $\mathcal{R}_n$ such that $\gcd(v(x), x^n - 1) = g(x)$ over $\mathbb{F}_q[x]$. Show that $v(x)$ is the generator polynomial of C as well.

7. Find the channel capacity for the channels specified by the following conditional distributions (where $0 \leq e \leq 1$ is the probability of receiving error E, the expression $0 \log 0$ is considered by convention to be equal to zero in information theory):

(a)

x	y	$P_{Y\|X}(y\|x)$
0	0	0.5
0	1	0.5
1	0	0.5
1	1	0.5

(b)

x	y	$P_{Y\|X}(y\|x)$
0	0	$1 - e$
0	1	0
0	E	e
1	0	0
1	1	$1 - e$
1	E	e