Algorithms of Information Security

Exercises for *Error-correcting codes II*

1. Let C be a binary cyclic code of length 7 over F_2 with a generator polynomial: $g(x) = x^3 + x + 1$.

   a) Verify that the code C is cyclic.

   b) Find the generator matrix and parity check matrix for the given binary cyclic code C.

   Hint for a): Note that every cyclic code is a polynomial code. Verify that g divides $x^7 - 1$.

   [Results: a) $g(x)$ divides $x^7 - 1$ and hence, C is cyclic, b) the generator matrix is

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

   and the parity check matrix is

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

   ]

2. Find all binary cyclic codes of length 3 over F_2.

   Hint: find all divisors of the polynomial $x^3 - 1$.

   [Result:

generator polynomial	code in v $F_2[x]/(x^3-1)$
1	$F_2[x]/(x^3-1)$
$x+1$	$\{0, 1+x, x+x^2, 1+x^2\}$
x^2+x+1	$\{0, 1+x+x^2\}$
x^3-1	$\{0\}$

   ]

   Optional exercise: Find all cyclic codes of length 4 over F_3.

3. Decide whether there is a Reed-Solomon code with parameters $[7, 5, 3]_q$. If such a code exists, find its parity check matrix.

   Hint:

element from F_8^*	modulo x^3+x+1
α	x
α^2	x^2
α^3	$x+1$
α^4	x^2+x
α^5	x^2+x+1
α^6	x^2+1
α^7	1

   [Result:

   $$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2+1 \\ 1 & \alpha^2 & \alpha^2+\alpha & \alpha^2+1 & \alpha & \alpha+1 & \alpha^2+\alpha+1 \end{pmatrix}$$

   ]

4. Consider the Reed-Muller code $R(2,4)$. Find the generator matrix of the code.

   Hint: Consider the following monomials: $\{1, x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4\}$.

   [Result:

$$\begin{pmatrix} 11111111 & 11111111 \\ 01010101 & 01010101 \\ 00110011 & 00110011 \\ 00001111 & 00001111 \\ 00000000 & 11111111 \\ 00010001 & 00010001 \\ 00000101 & 00000101 \\ 00000000 & 01010101 \\ 00000011 & 00000011 \\ 00000000 & 00110011 \\ 00000000 & 00001111 \end{pmatrix}$$

   ]