1 Materials and Methods

(Teori om encoding og decoding)

1.1 Encoding

When a code is in systematic form the message vector can be directly extracted from the encoded information.
Encoding a message vector into a linear cyclic code, $C_{cyc}(n,k)$, in systematic form can be achieved as follows:
First the message polynomial (in the form of $m(X) = m_0 + m_1X + ... + m_{k-1}X^{k-1}$) should be converted into a vector of the length n. This is attained by multiplying the message vector by X^{n-k}, which results in a shift of the message $n-k$ to the right and forms the right-shifted message polynomial $X^{n-k}m(X)$.
Secondly, the right-shifted message polynomial should be divided by a generator polynomial, $g(X)$, fitting the conditions for being a generator polynomial of a linear cyclic code. The result of this division is a remainder polynomial (redundancy polynomial).
Finally, the code polynomial in systematic form can be obtained by adding the right-shifted message polynomial and the remainder polynomial:

$$c(X) = X^{n-k}m(X) + p(X) \tag{1}$$

The following equations describe the relationships between the right-shifted message polynomial, $X^{n-k}m(X)$, the factor, $q(X)$, the generator polynomial, $g(X)$, and the remainder polynomial, $p(X)$.

$$X^{n-k}m(X) = q(X)g(X) + p(X) \tag{2}$$

$\leftrightarrow$

$$X^{n-k}m(X) + p(X) = q(X)g(X) \tag{3}$$

1.1.1 Encoding Example

A concrete example with the generator polynomial $g(X) = 1 + X^4 + X^6 + X^7 + X^8$ is used to encode the following message polynomial: $m(X) = 1 + X^2 + X^4 + X^6$, corresponding to $m = [1010101]$. The code is a cyclic code, $C_{cyc}(15,7)$.
First the message is right shifted $n-k$ times.

$$X^{15-7}m(X) = X^8 + X^{10} + X^{12} + X^{14} \tag{4}$$

Find $p(X)$ by taking the remainder from $X^{n-k}m(x)$ divided by $g(X)$.

$$
\begin{array}{lllll|lllll}
 & & & & & X^6 & +X^5 & +X^4 & +X^2 & +1 \\
\hline
X^8 & +X^7 & +X^6 & +X^4 & +1 & X^{14} & +X^{12} & +X^{10} & +X^8 & \\
 & & & & & X^{14} & +X^{13} & +X^{12} & +X^{10} & +X^6 \\
\hline
 & & & & & & X^{13} & & +X^8 & +X^6 \\
 & & & & & & X^{13} & +X^{12} & +X^{11} & +X^9 & +X^5 \\
\hline
 & & & & & & & X^{12} & +X^{11} & +X^9 & +X^8 & +X^6 & +X^5 \\
 & & & & & & & X^{12} & +X^{11} & +X^{10} & +X^8 & & +X^4 \\
\hline
 & & & & & & & & X^{10} & +X^9 & +X^6 & +X^5 & +X^4 \\
 & & & & & & & & X^{10} & +X^9 & +X^8 & +X^6 & +X^2 \\
\hline
 & & & & & & & & & X^8 & +X^5 & +X^4 & +X^2 & \\
 & & & & & & & & & X^8 & +X^7 & +X^6 & +X^4 & +1 \\
\hline
 & & & & & p(X) = & & & & & X^7 & +X^6 & +X^5 & +X^2 & +1
\end{array}
$$

Now $c(X)$ can be calculated:

$$c(X) = X^8 m(X) + p(X) = 1 + X^2 + X^5 + X^6 + X^7 + X^8 + X^{10} + X^{12} + X^{14} \tag{5}$$

$$c = [101001111010101] \tag{6}$$

It is easily seen that the encoded vector is in systematic form, hence the message vector corresponds to the last 7 bits.

1.2 Decoding

In general when decoding a received vector the syndrome vector (S) is needed to find out if any error have occurred. To find this the generator polynomial is used to make the generator matrix (G) which further is used to find the parity check matrix (H). The formula to find the syndrome vector for a received vector (r) is:

$$S = r \circ H^T = (s_0, s_1, ..., s_{n-k-1}) \tag{7}$$

To do all this by hand will look like the example below. A generator polynomial could be $1+X+X^3$. The generator polynomial for this will be $G_{k\times n}$ where k = 4 and n = 7:

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

To find the parity check matrix, the generator matrix need to be in systematic form. This is done by creating a identity matrix at the end with detentions ($k \times k$). In systematic form the generator matrix is:

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

The first n - k columns is the parity matrix. The parity check matrix is in the form:

$$H = [I_{(n-k)\times(n-k)} \quad P^T_{(n-k)\times k}] \tag{8}$$

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