1 Cyclic Codes

1.1 Polynomial Representation of codewords

For a given vector of n components, $c = (c_0, c_1, \ldots, c_{n-1}$, a right-shift of its components generates a different vector.

Right shift the original vector for i times, the new vector is:
$c^{(i)} = (c_{n-i}, c_{n-i+1}, \ldots c_{n-1}, C_0, c_1 \ldots)$

Cyclic code, $C_{cyc}(n,k)$ can be represented as a polynomials:
$c = (c_0, c_1, \ldots, c_{c_n-1}$
$c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}c_i \in GF(2^m)$

Example: $1011 \Rightarrow 1 + X^2 + X^3$

In a $C(n,k)$ there will be n polynoms.

1.1.1 Addition and multiplication

Addition [**?**, p. 6-7]
$c_1(x) \bigoplus c_2(x) = (c_01 \bigoplus c_02) + (c_11 \bigoplus c_12)X + \ldots + (c_{n-1,1} \bigoplus c_{n-1,2})X^{n-1}$

Multiplication: [**?**, p. 6-7]

Division: [**?**, p. 9] "Polynomial division." http://en.wikipedia.org/wiki/Polynomial_long_division

1.2 Generator polynomial of cyclic code

[**?**, p. 10-11] $C^{(i)}(x) = C_{n-i} + C_{n-i+1} + \ldots + C_{n-i-1}c^{n-1}$
$C^{(i)} = x^1C(x)mod(x^n + 1)$
$x^1C(c) = \ldots$

$$C = (0110100) \qquad \Rightarrow C^{(3)} = (1000110)$$
$$C(x) = x + x^2 + x^4 \qquad C^{(3)}(x) \qquad = 1 + x^4 + x^5$$

$x^3\dot{C}(x)mod(x^7+1)$

$x^4 + x^5 + x^7 \Rightarrow division \ldots = x^5 + x^4 + 1$

[**?**, p. 14]

$$g(x) = 1 + g_1x + \ldots + g_{r-1}x^{r-1} + x^r$$
$$x\dot{g}(x) = x\dot{g}(x)mod(x^n+1) \qquad = g^{(1)(x})$$
$$x^2\dot{g}(x) = x^2\dot{g}(x)mod(x^n+1) \qquad = g^{(2)+(x)}$$
$$\ldots$$
$$x^{n-r-1}g(x) = g^{(n-r-1)}(x)$$

$c(x) = m(x)\dot{g}(x)$ [**?**, p.15]. It means a code polynomial $c(x)$ is a multiple of the non-zero minimum-degree polynomial $g(x)$.

In a cyclic code $C_{cyc}(n,k)$ there is a unique non-zero minimum-degree code polynomial, and any other polynomial is a multiple of this polynomial.
The non-zero minimum-degree code polynomial completely determines and generates the cyclic code. It is called generator polynomial.

1.3 Cyclic codes in systematic form

$c(x) = m(x)g(x)$ – This is non-systematic (which means the messages is inside the code vector [**?**, p. 20-21].

$$x^{n-k} \cdot m(x)$$
$$p(x) = x^{n-k} \cdot m(x)modg(x)$$
$$x^{n-k} \cdot m(x) = q(x) \cdot g(x) + p(x)$$
$$q(x) \cdot g(x) = x^{n-k}m(x) + p(x)$$

Code vector can be expressed based on code polynomial as: $c = (p_0, p_1, \ldots, p_{n-k-1}, m_0, m_1, \ldots, m_{k-1})$ [**?**, p. 23]

Summary on [?, p. 24]

1.3.1 Generator matrix of a cyclic code

$$\begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ \ldots & \ldots & & & & & & & \\ 0 & 0 & & \ldots & g_0 & g_1 & g_2 & \ldots & g_{n-k} \end{bmatrix}$$ Where $g_0 = g_{n-k} = 1$ [**?**, p. 26]

$g(x) = 1 + x \Rightarrow r(rank) = 1$(power of x) [**?**, p. 28]