

# Information theory and coding

Rasmus Bækgaard

February 17, 2014

## Contents

<b>Contents</b>	<b>1</b>
<b>1 Codeblocks</b>	<b>2</b>
<b>2 Cyclic Codes</b>	<b>3</b>
2.1 Polynomial Representation of codewords . . . . .	3
2.1.1 Addition and multiplication . . . . .	3
2.2 Generator polynomial of cyclic code . . . . .	3
2.3 Cyclic codes in systematic form . . . . .	4
2.3.1 Generator matrix of a cyclic code . . . . .	5
<b>Bibliography</b>	<b>6</b>

# 1 Codeblocks

## 2 Cyclic Codes

### 2.1 Polynomial Representation of codewords

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

Right shift the original vector for  $i$  times, the new vector is:

$$c^{(i)} = (c_{n-i}, c_{n-i+1}, \dots, c_{n-1}, c_0, c_1, \dots)$$

**Cyclic code**,  $C_{cyc}(n, k)$  can be represented as a polynomials:

$$c = (c_0, c_1, \dots, c_{n-1})$$

$$c(X) = c_0 + c_1X + \dots + c_{n-1}X^{n-1} \in GF(2^m)$$

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

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

#### 2.1.1 Addition and multiplication

**Addition** [1, p. 6-7]

$$c_1(x) \oplus c_2(x) = (c_{0,1} \oplus c_{0,2}) + (c_{1,1} \oplus c_{1,2})X + \dots + (c_{n-1,1} \oplus c_{n-1,2})X^{n-1}$$

**Multiplication:** [1, p. 6-7]

**Division:** [1, p. 9] "Polynomial division." [http://en.wikipedia.org/wiki/Polynomial\\_long\\_division](http://en.wikipedia.org/wiki/Polynomial_long_division)

### 2.2 Generator polynomial of cyclic code

$$[1, \text{p. 10-11}] \quad C^{(i)}(x) = C_{n-i} + C_{n-i+1}x + \dots + C_{n-i-1}x^{n-i}$$

$$C^{(i)} = x^i C(x) \bmod (x^n + 1)$$

$$x^1 C(x) = \dots$$

$$\begin{aligned}
 C &= (0110100) & \Rightarrow C^{(3)} &= (1000110) \\
 C(x) &= x + x^2 + x^4 & C^{(3)}(x) &= 1 + x^4 + x^5
 \end{aligned}$$

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

$$x^4 + x^5 + x^7 \Rightarrow \text{division} \dots = x^5 + x^4 + 1$$

[1, p. 14]

$$\begin{aligned}
 g(x) &= 1 + g_1x + \dots + g_{r-1}x^{r-1} + x^r \\
 x\dot{g}(x) &= x\dot{g}(x) \bmod (x^n + 1) & &= g^{(1)}(x) \\
 x^2\dot{g}(x) &= x^2\dot{g}(x) \bmod (x^n + 1) & &= g^{(2)+(x)} \\
 &\dots \\
 x^{n-r-1}g(x) &= g^{(n-r-1)}(x)
 \end{aligned}$$

$c(x) = m(x)\dot{g}(x)$  [1, 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.

## 2.3 Cyclic codes in systematic form

$c(x) = m(x)g(x)$  – This is non-systematic (which means the messages is inside the code vector [1, p. 20-21]).

$$\begin{aligned}
 x^{n-k} \cdot m(x) \\
 p(x) &= x^{n-k} \cdot m(x) \bmod g(x) \\
 x^{n-k} \cdot m(x) &= q(x) \cdot g(x) + p(x) \\
 q(x) \cdot g(x) &= x^{n-k}m(x) + p(x)
 \end{aligned}$$

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

Summary on [1, p. 24]

### 2.3.1 Generator matrix of a cyclic code

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

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

# Bibliography

- [1] Q. Zhang, “Cyclic codes.” iha.Campusnet.dk, 02 2014. CLC-handout.