Coding Theory
Cyclic codes. BCH codes
Linear codes can be determined by their generator or parity-check matrices. For these codes encoding complexity is approximately quadratic function of code length and decoding complexity grows exponentially with code length. Restrictions can be imposed on codes in order to reduce both encoding and decoding complexity. For cyclic codes, a cyclic shift of a codeword is a codeword. A cyclic code can be defined by its generator or parity-check polynomial. Codes with polynomial decoding complexity in a hard decision channel will be presented.
Definition
Linear \([n, k]\)-code over GF\((q)\) is called \textit{cyclic code} if a \textit{cyclic shift} of a codeword is a codeword of the same code.

Example
Sequences 10110, 10001, 00100 correspond to polynomials \(1 + x^2 + x^3\), \(1 + x^4\), \(x^2\).

Theorem
\textit{In the polynomial ring} \(\mathbb{R}_{x^n-1}[x]\) \textit{of polynomial residuals by modulo} \(x^n - 1\) \textit{over GF}(\(p\)), \(p\) is prime, \textit{for any} \(a(x)\) \textit{the polynomial} \(xa(x)\) \textit{is a cyclic shift of} \(a(x)\).
Proof.
Let \( a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}, \ a_i \in GF(2) \).

\[
xa(x) = a_{n-1} + a_0 x + \ldots + a_{n-2} x^{n-1}.
\]

We took into account that \( x^n = 1 \mod x^n - 1 \). The sequence \( a_{n-1}, a_0, \ldots, a_{n-2} \) is a cyclic shift of \( a_0, a_1, \ldots, a_{n-1} \). \( \square \)

**Theorem**

*If \( g(x) \) is a codeword of a cyclic code then for any polynomial \( m(x) \) the product \( g(x)m(x) \) is a codeword too.*

**Proof.**

Since \( g(x)m(x) \) is a linear combination of products \( g(x) \) by monomials, the statement follows from the above Theorem.
Theorem

In a cyclic code there exists only one monic polynomial of smallest degree $h$.

Proof.

If there are two such polynomials of degree $h$ then the codeword equal to their sum has degree smaller than $h$ which contradicts the assumption that $h$ is smallest degree among codewords. 

\[ \square \]
Theorem

Let $g(x)$ be the codeword of the smallest degree $h$. Then any other codeword is multiple of $g(x)$.

Proof.

Let $c(x)$ be a codeword. Its degree is larger than $h$. Therefore, we can represent $c(x)$ as $c(x) = g(x)q(x) + r(x)$. From the above Theorem that $g(x)q(x)$ is codeword. We conclude that the residual $r(x)$ is a codeword. It cannot be nonzero codeword since its degree is smaller than $h$. Therefore, $r(x) = 0$. 

Irina Bocharova, Tartu, 2022
Theorem

Let in \([n, k]\)-code \(g(x)\) be the codeword of the smallest degree \(h\). Then \(g(x)\) divides \(x^n - 1\).

Proof.

Since \(h < n\) we can write

\[
x^n - 1 = q(x)g(x) + r(x),
\]

or \(r(x) = q(x)g(x) \mod x^n - 1\).

which means that \(r(x)\) is either zero or a codeword of degree smaller than \(h\). Therefore, \(r(x) = 0\). \(\square\)
Theorem
Let in \([n, k]\)-code \(g(x)\) be the codeword of the smallest degree \(h\). Then \(h = n - k\).

Proof.
Polynomials \(g(x), xg(x),..., x^{n-h-1}g(x)\) are linearly independent and any codeword \(m(x)g(x)\) mod \(x^n - 1\) can be obtained as their linear combinations. Thus, this set of polynomials is a basis of the code and their number is equal to its dimension, \(n - h = k\).

Definition
The smallest degree monic polynomial \(g(x)\) is called \textit{generator polynomial} of the cyclic code.
Example

Let $n = 7$, $g(x) = 1 + x^2 + x^3$. According to the above Theorem the dimension of the code generated by linear combination of shifts of $g(x)$ is 4. The generating matrix of the code is

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

The minimum distance of this code is 3, therefore the obtained code is the $[7,4]$ Hamming code.
In general, cyclic \([n, k]\)-code with generator polynomial \(g(x)\) has generator matrix

\[
G = \begin{pmatrix}
g_0 & g_1 & g_2 & \cdots & g_r \\
g_0 & g_1 & \cdots & g_{r-1} & g_r \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
g_0 & \cdots & g_{r-1} & g_r
\end{pmatrix},
\]

where empty places correspond to zeros.

For a message polynomial \(m(x) = m_0 + m_1x + \ldots + m_{k-1}x^{k-1}\) the corresponding codewords can be computed as

\[
c(x) = m(x)g(x).
\]
Let

\[ h(x) = \frac{x^n - 1}{g(x)}. \]  \hspace{1cm} (2)

The residual from this division is equal to zero. From this equality we have

\[ h(x)g(x) = 0 \mod x^n - 1. \]

which means that for any \( c(x) = m(x)g(x) \)

\[ c(x)h(x) = 0 \mod x^n - 1. \]

**Definition**

For a cyclic \([n, k]\)-code with generator polynomial \( g(x) \) the polynomial \( h(x) \) of degree \( k \) determined as \( h(x) = \frac{x^n-1}{g(x)} \) is called **check polynomial** of the cyclic code.
c(x)h(x) = 0 all coefficients of the polynomial in left hand side of equation are zeros. In particular, the coefficient for \(x^i\) for \(i \geq k\) is

\[
\sum_{j=0}^{i} h_j c_{i-j} = 0, \quad i = k, k + 1, ..., n - 1.
\]

These \(r = n - k\) linear equations can be written in matrix form \(Hc = 0\),

\[
H = \begin{pmatrix}
h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \\
h_k & h_{k-1} & \cdots & h_1 & h_0 \\
& \ddots & \ddots & \ddots & \ddots \\
& & \ddots & \ddots & \ddots & \ddots \\
& & & \ddots & \ddots & \ddots \\
& & & & \ddots & \ddots & \ddots \\
& & & & & \ddots & \ddots & \ddots \\
h_k & \cdots & h_1 & h_0
\end{pmatrix}.
\]
Thus, unlike the case of generator polynomial, coefficients $h_i$ in rows of $H$ run in descending order. The corresponding polynomial $x^k h(x^{-1})$ is called \textit{reciprocal} polynomial to $h(x)$.

The obtained result can be formulated as a theorem.

\textbf{Theorem}

\textit{The dual code to a cyclic $[n, k]$-code with check polynomial $h(x)$ is the cyclic code with generator polynomial}

$$g^\perp(x) = x^k h(x^{-1}).$$
Cyclic codes. The set of length 7 cyclic codes

Example

Let $n = 7$,

$$x^7 + 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3) = m_0(x)m_1(x)m_3(x).$$

<table>
<thead>
<tr>
<th>$[n, k]$</th>
<th>$g(x)$</th>
<th>$h(x)$</th>
<th>$d_{\text{min}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[7,6]$</td>
<td>$m_0 = 1 + x$</td>
<td>$m_1 m_3 = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$</td>
<td>2</td>
</tr>
<tr>
<td>$[7,4]$</td>
<td>$m_1 = 1 + x + x^3$</td>
<td>$m_0 m_1 = 1 + x + x^2 + x^4$</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>$m_3 = 1 + x^2 + x^3$</td>
<td>$m_0 m_3 = 1 + x^2 + x^3 + x^4$</td>
<td></td>
</tr>
<tr>
<td>$[7,3]$</td>
<td>$m_0 m_1 = 1 + \ldots + x^4$</td>
<td>$m_3 = 1 + x^2 + x^3$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$m_0 m_3 = 1 + \ldots + x^4$</td>
<td>$m_1 = 1 + x + x^3$</td>
<td>4</td>
</tr>
<tr>
<td>$[7,1]$</td>
<td>$m_1 m_3 = 1 + \ldots + x^6$</td>
<td>$m_0 = 1 + x$</td>
<td>7</td>
</tr>
</tbody>
</table>
Theorem

Cyclic Hamming codes. Let $n = 2^m - 1$ and choose a degree $m$ binary primitive polynomial $p(x)$ as a generator polynomial $g(x)$. Such a binary cyclic code is $[n, n - m]$ Hamming code with minimum distance 3.
Proof.
Denote by $\alpha$ a primitive element of $\text{GF}(2^m)$ i.e. a root of $p(x)$ and let $H = (\alpha^0 \ \alpha^1 \ \ldots \ \alpha^{n-1})$.
Since any codeword is multiple of $g(x) = p(x)$, then $c(x)|_{x=\alpha} = c(\alpha) = 0$.
For any $b(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}$,

$$s = b H^T = b_0 \alpha^0 + b_1 \alpha^1 + \ldots + b_{n-1} \alpha^{n-1} = b(\alpha) = 0$$

iff $b(x)$ is multiple of $g(x) = p(x)$.
Since $\alpha$ is primitive element, all powers of $\alpha$ are different, that is, all columns of $H$ are different and $d_{\text{min}} \geq 3$.  

\[\square\]
Since $x^n - 1$ has root 1, then $x + 1$ is always divisor of $x^n - 1$ and can be chosen as $g(x)$. For any $m(x)$, $c(x) = m(x)(x + 1)$ has an even number of summands, that is, we obtain $[n, n - 1]$ single parity-check code. Its dual code is $[n, 1]$ repetition code. It is also cyclic.

The extended Hamming code has generator polynomial $g(x) = p(x)(x + 1)$. 
The dual to Hamming code is the simplex 
\([n = 2^m - 1, m]\)-code with \(d_{\text{min}} = (n + 1)/2\). 
As a cyclic code it is determined by check polynomial
\(h(x) = p(x)\), where \(p(x)\) is a primitive polynomial of degree \(m\). Its generator polynomial is
\(g(x) = (x^n - 1)/p(x)\).
Generator of maximal length sequences

\[
\begin{aligned}
& m_t + m_{t+1} + \ldots + m_{t+m-2} + m_{t+m-1} \\
& \times p_0 \quad \times p_1 \quad -p_2 \quad \ldots \quad -p_{m-1}
\end{aligned}
\]

Example

Generator of maximal length sequences
\((p(x) = 1 + x + x^4)\) or encoder of \([15, 4]\) code

\[
\begin{aligned}
& m_t + m_{t+1} + m_{t+2} + m_{t+3} \\
& \times p_0 \quad \times p_1
\end{aligned}
\]
<table>
<thead>
<tr>
<th>Step</th>
<th>State</th>
<th>Output symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0011</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1101</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1010</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0101</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1110</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0111</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1111</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1011</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1001</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0100</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0010</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0001</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1100</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>0110</td>
<td>0</td>
</tr>
</tbody>
</table>