Error-correcting codes

Lecture 10. Cyclic codes.
Agenda

- Finite fields
- Cyclic codes
- BCH codes
- RS-codes
- Decoding
• Error correction in data storage devices
• Constituent codes in concatenated systems, e.g. stair-case codes, GLDPC, NB LDPC
• CRC in all standards
Definition

The set $\mathcal{G}$ together with some operation $\ast$ is called group if the following axioms fulfilled

- **Associativity**: for $a, b, c \in \mathcal{G}$, $(a \ast b) \ast c = a \ast (b \ast c)$.
- **Identity element**: there exists $e \in \mathcal{G}$ such that $a \ast e = e \ast a = a$ for any $a \in \mathcal{G}$.
- **Inverse element**: for any $a \in \mathcal{G}$ there exists $b \in \mathcal{G}$ such that $a \ast b = b \ast a = e$.
- If also commutativity axiom: $a \ast b = b \ast a$ for any $a, b \in \mathcal{G}$, then group is called commutative or abelian.

Size of $\mathcal{G}$, i.e. $|\mathcal{G}|$ is called an order of the group.
Example

\( G = \{0, \ldots, p - 1\} = \mathbb{Z}_p \) with + mod \( p \) is a group for any \( p \).
Identity element is 0, inverse element for \( a \in G \) is \( b = -a \pmod{p} = p - a \).

If \( \times \) is used then 1 is the identity element. Inverse \( a \) is \( a^{-1} \).
\( \mathbb{Z}_p \setminus \{0\} \) with \( \times \) mod \( p \) is not necessary a group: For \( p = 4 \) inverse elements does not exist for some elements. \( 3^{-1} = 1 \mod 4 \), but \( 2^{-1} \) does not exist since there is no such \( b \in \mathbb{Z}_4 \) that \( 2 \times b = 1 \).

Definition

If \( H \) and \( G \) are groups with respect to the same group operation and \( H \subset G \) then \( H \) is called **subgroup** of \( G \).
Example

Let $G = \mathbb{Z}_6 = \{0, ..., 5\}$ with addition by modulo 6. Then $H = \mathbb{Z}_4$ is subset of $G$ but not subgroup since $H$ is not a group with $+$ by modulo 6.

Sets $H = \{0, 3\}$ and $H = \{0, 2, 4\}$ are two examples of subgroups of $G$.

Definition

Let $G$ be a group and $H$ is subgroup of $G$. For $g \in G$ and for $g \notin H$ the set $\{g + h, h \in H\}$ is called a coset of $H$ in $G$. Element $g$ is called a coset generator.

Example

Consider the group $G = \mathbb{Z}_6$ with addition by modulo 6 and its subgroup $H = \{0, 3\}$. Cosets of $H$ are $\{0, 3\}$, $\{1, 4\}$, $\{2, 5\}$. 
Lemma
All cosets of $\mathcal{H}$ in $G$ have the same size $|\mathcal{H}|$.

Proof.
Let a cosets size is smaller than $|\mathcal{H}|$. It means that for different $h_1, h_2 \in \mathcal{H}$ we get the same coset element $a \ast h_1 = a \ast h_2$. By applying $a^{-1}$ to both sides we obtain $h_1 = h_2$ which contradicts to the assumption that $h_1 \neq h_2$. 

Lemma
Cosets either do not intersect or coincide.

Proof.
For two cosets $A$ not equal $B$, assume that for some $a \in A$, $b \in B$, $h_1, h_2 \in A$ their common element is $a \ast h_1 = b \ast h_2$. Applying to both side operation with $h \in \mathcal{H}$ one more common element will be found. Repeating for all $h \in \mathcal{H}$ we verify that $A = B$. 

Theorem

Lagrange’s theorem. For a finite group $\mathcal{G}$ and its subgroup $\mathcal{H}$, order of subgroup $|\mathcal{H}|$ divides the order of group $|\mathcal{G}|$.

Example

The group $\mathcal{G} = \mathbb{Z}_6$ with addition by modulo 6 has order 6. Its subgroups $\mathcal{H} = \{0, 3\}$ and $\mathcal{H} = \{0, 2, 4\}$ are of orders 2 and 3, respectively.

Next we consider structures with two operations, addition $+$ and multiplication $\times$. 
Definition
A set \( \mathcal{R} \) with \( \times \), is ring if

- \( R \) is group with \( + \) operation and 0 as identity;
- multiplication is associative: \((a \times b) \times c = a \times (b \times c)\);
- distributivity law holds: \( a \times (b + c) = a \times b + a \times c \).

Example
The group \( \mathbb{Z}_6 \) is the ring with \( + \) and \( \times \) mod 6. 
\( \mathbb{Z}_6 \backslash \{0\} \) is not a group under \( \times \) mod 6.
The group \( \mathbb{Z}_5 \) is the ring with \( + \) and \( \times \) mod 5. 
\( \mathbb{Z}_5 \backslash \{0\} \) is a group under \( \times \) mod 5.
Definition
A set $\mathbb{F}$ is a field if it is ring and $\mathbb{F}\setminus\{0\}$ is a group under multiplication. By $\mathbb{F}_q$ we denote field of $q$ elements.

Theorem
The ring $\mathcal{R} = \mathbb{Z}_q$ is a field $\mathbb{F}_q$ over addition and multiplication by modulo $q$ if $q$ is prime number.

Proof.
It is enough to check if all nonzero elements $a \in \mathbb{F}_q$ have inverses $a^{-1}$. Consider products $a \times b$ for all $b \in \mathbb{F}_q$ except $b = 0$. All $q - 1$ products are different (otherwise from $a \times b = a \times b'$ mod $q$ follows $a \times (b - b') = 0$ mod $q$ which is impossible for prime $q$). Thus, one of products is $a \times b = 1$ and there exists $b = a^{-1}$. \qed
\( \mathbb{Z}_q \) is a field \( \mathbb{F}_q \) for prime \( q \).

**Definition**
The set of polynomials over \( \mathcal{R} \)

\[
a(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, \quad a_n \neq 0.
\]

is called a **polynomial ring** \( \mathcal{R}[x] \).

**Definition**
Polynomial \( a(x) \) of degree \( n \) is called **monic** if \( a_n = 1 \)

**Definition**
Polynomial \( a(x) \in \mathcal{R}[x] \) of degree \( n > 0 \) is called **irreducible** over \( \mathcal{R} \) if it cannot be represented as a product of two or more polynomials from \( \mathcal{R}[x] \).
Similarly to prime fields:

**Theorem**

Let $p(x)$ of degree $n > 0$ be an irreducible polynomial over finite field $\mathbb{F}_q$. Then a polynomial ring of residuals by modulo $p(x)$ is a field $\mathbb{F}_{p(x)}[x]$.

**Definition**

The finite field of $q$ elements denoted as $\text{GF}(q)$ is called **Galois field**. The field size $q$ is either a prime number or a degree of a prime number.
### Galois field example

#### $p(x) = 1 + x^2$

<table>
<thead>
<tr>
<th>Element</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$x$</td>
<td>$x$</td>
</tr>
<tr>
<td>$1 + x$</td>
<td>Not exists</td>
</tr>
</tbody>
</table>

#### $p(x) = 1 + x + x^2$

<table>
<thead>
<tr>
<th>Element</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$x$</td>
<td>$1 + x$</td>
</tr>
<tr>
<td>$1 + x$</td>
<td>$x$</td>
</tr>
</tbody>
</table>
Definition
A group generated by a single element is called a cyclic group.

Definition
Minimal integer $d$ such that $a^d = a$ is called the order of $a$.

Example
In $\mathbb{F}_5$ multiplicative group consists of 4 elements, all of order 4. In particular degrees of 3 are equal to 3, $3^2 = 9 = 4 \mod 5$, $3^3 = 27 = 2 \mod 5$, $3^4 = 81 = 1 \mod 5$.
In $\mathbb{F}_7$ element 6 is of order 2, elements 2 and 4 have order 3, and 3 5 have order 6.
Since the entire multiplicative group consists of \( q - 1 \) elements from Lagrange’s theorem follows

**Theorem**

*Little Fermat’s theorem.* For any \( a \in \mathbb{F}_q \)

\[
a^{q-1} = 1 \mod q. \quad (1)
\]

**Proof.**

For some \( d \leq q - 1 \) which is equal to the order of \( a \) we have \( a^d = 1 \). From Lagrange’s theorem follows that \( t = (q - 1)/d \) is integer. Therefore, \( a^{dt} = a^{q-1} = 1 \).
Theorem

In the multiplicative group of GF(q) there exists an element of order q – 1, not necessarily unique.

Definition

Nonzero element $\alpha \in GF(q)$ of order $q - 1$ is called primitive element of this field.

All elements can be indexed by degrees of $\alpha$. The choice is not unique. We choose a root of $p(x)$.

Definition

If $p(x)$ is minimum degree polynomial having primitive element $\alpha$ as a root, then $p(x)$ is called primitive.
Multiplicative group of Galois field

\[ p(x) = x^3 + x + 1 \text{ over } \mathbb{GF}(2). \]

<table>
<thead>
<tr>
<th>Degree of primitive element</th>
<th>Polynomial form</th>
<th>Binary form</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\alpha^0)</td>
<td>1</td>
<td>001</td>
</tr>
<tr>
<td>(\alpha)</td>
<td>(\alpha)</td>
<td>010</td>
</tr>
<tr>
<td>(\alpha^2)</td>
<td>(\alpha^2)</td>
<td>100</td>
</tr>
<tr>
<td>(\alpha^3)</td>
<td>(\alpha^3 = 1 + \alpha)</td>
<td>011</td>
</tr>
<tr>
<td>(\alpha^4)</td>
<td>(\alpha + \alpha^2)</td>
<td>110</td>
</tr>
<tr>
<td>(\alpha^5)</td>
<td>(\alpha^2 + \alpha^3 = 1 + \alpha + \alpha^2)</td>
<td>111</td>
</tr>
<tr>
<td>(\alpha^6)</td>
<td>(\alpha + \alpha^2 + \alpha^3 = 1 + \alpha^2)</td>
<td>101</td>
</tr>
<tr>
<td>(\alpha^7 = \alpha^0)</td>
<td>(\alpha + \alpha^3 = 1)</td>
<td>001</td>
</tr>
</tbody>
</table>
### GF(2^4)

<table>
<thead>
<tr>
<th>Degree</th>
<th>Polynomials $p(x) = 1 + x + x^4$</th>
<th>Polynomials $p(x) = 1 + x + x^2 + x^3 + x^4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-\infty$</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0</td>
<td>0001</td>
<td>0001</td>
</tr>
<tr>
<td>1</td>
<td>0010</td>
<td>0010</td>
</tr>
<tr>
<td>2</td>
<td>0100</td>
<td>0100</td>
</tr>
<tr>
<td>3</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>4</td>
<td>0011</td>
<td>1111</td>
</tr>
<tr>
<td>5</td>
<td>0110</td>
<td>0001</td>
</tr>
<tr>
<td>6</td>
<td>1100</td>
<td>0010</td>
</tr>
<tr>
<td>7</td>
<td>1011</td>
<td>0100</td>
</tr>
<tr>
<td>8</td>
<td>0101</td>
<td>1000</td>
</tr>
<tr>
<td>9</td>
<td>1010</td>
<td>1111</td>
</tr>
<tr>
<td>10</td>
<td>0111</td>
<td>0001</td>
</tr>
<tr>
<td>11</td>
<td>1110</td>
<td>0010</td>
</tr>
<tr>
<td>12</td>
<td>1111</td>
<td>0100</td>
</tr>
<tr>
<td>13</td>
<td>1101</td>
<td>1000</td>
</tr>
<tr>
<td>14</td>
<td>1001</td>
<td>1111</td>
</tr>
</tbody>
</table>
Definition
For a field $\mathbb{GF}(q)$ a smallest number $p$ such that

\[
1 + 1 + \ldots + 1 = 0. \quad \text{($p$ summands)}
\]

is called characteristic of the field $\mathbb{GF}(q)$.

The following identities hold for a field of characteristic $p$:

\[
px = 0; \\
(x + y)^p = x^p + y^p.
\]
Definition
The minimal polynomial $m(x)$ for $\beta \in \text{GF}(p^m)$ over $\text{GF}(p)$ is the smallest-degree nonzero monic polynomial such that $m(\beta) = 0$.

Example:
In $\text{GF}(16)$ with $p(x) = 1 + x + x^4$ for $\beta = \alpha^0$ $m_0(x) = x + 1$.
For $\beta = \alpha, \alpha^p, \alpha^{2p}, \ldots$ $m_1(x) = x + 1$.

\[
\begin{align*}
m_3(x) &= 1 + x + x^2 + x^3 + x^4\bigg|_{x=\alpha^3} = 0; \\
m_5(x) &= 1 + x + x^2\bigg|_{x=\alpha^5} = 0; \\
m_7(x) &= 1 + x^3 + x^4\bigg|_{x=\alpha^7} = 0; \\
m_7(x)\bigg|_{x=\alpha^7} &= 1 + \alpha^{21} + \alpha^{28} = 1 + \alpha^6 + \alpha^{13} = 0,
\end{align*}
\]
**Table:** Minimal polynomials for elements of GF(2^4) defined by primitive polynomial $p(x) = 1 + x + x^4$

<table>
<thead>
<tr>
<th>Degrees</th>
<th>Minimal polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$m_0(x) = 1 + x$</td>
</tr>
<tr>
<td>1,2,4,8</td>
<td>$m_1(x) = 1 + x + x^4$</td>
</tr>
<tr>
<td>3,6,9,12</td>
<td>$m_3(x) = 1 + x + x^2 + x^3 + x^4$</td>
</tr>
<tr>
<td>5,10</td>
<td>$m_5(x) = 1 + x + x^2$</td>
</tr>
<tr>
<td>7,11,13,14</td>
<td>$m_7(x) = 1 + x^3 + x^4$</td>
</tr>
</tbody>
</table>
From little Fermat’s theorem:

\[ x^{q-1} - 1 = \prod_{a \in GF(q)} (x - a). \]

By grouping multipliers into products equal to minimal polynomials we obtain formula

\[ x^{q-1} - 1 = \text{LCM}\{m_i(x), i = 0, 1, \ldots, q - 1\} \quad (2) \]

where LCM denotes the least common multiple, \( m_i(x) \) is the minimal polynomial for \( \alpha^i \).
Galois fields. Summary

- Finite field is a set closed with respect to addition, multiplication and division.
- The size of the field is either a prime number or a degree of a prime number.
- For prime $p$ the extension field of size $q = p^m$ can be represented as a ring of polynomial residuals by modulo irreducible polynomial.
- Field elements can be indexed by degrees of primitive element.
- Products in $GF(q)$ are convenient to compute by summing up corresponding degrees of primitive elements. Sums are easily computed by symbol-wise summing of binary representations.
Definition
Linear \([n, k]\)-code over \(\mathbb{GF}(q)\) is called cyclic code if a cyclic shift of a codeword is a codeword of the same code.
Two simple examples, are repetition code and single-parity-check code.

Theorem
In the polynomial ring \(\mathbb{R}_{x^{n-1}}[x]\) of polynomial residuals by modulo \(x^n - 1\) over \(\mathbb{GF}(q)\) for any \(a(x)\) the polynomial \(xa(x)\) is a cyclic shift of \(a(x)\).

Proof.
It is enough to proof the statements for monomials. The statement is definitely correct for \(x^i, i = 0, 1, \ldots x^{n-2}\). For \(i = n - 1\) we obtain \(x \ast x^{n-1} = 1 \mod x^n + 1\). \(\square\)
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. These products are codewords.

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.
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 of degree larger than $h$. Write it as $c(x) = g(x)q(x) + r(x)$. Then $r(x)$ is a codeword. Since degree is smaller than $h$, therefore, $r(x) = 0$.

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 $r(x) = q(x)g(x) \mod x^n - 1$. Degree of $r(x)$ smaller than $h$. Therefore, $r(x) = 0$. 
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 *generator polynomial of the cyclic code*. 
Let $n = 7$, $g(x) = 1 + x^2 + x^3$. The dimension $k = 7 - 3 = 4$, if do not exist words of weight less than 3. 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 $[7,4]$ Hamming code.
In general, cyclic \([n, k]\)-code with generator polynomial \(g(x)\) has generator matrix

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

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

$$h(x) = \frac{x^n - 1}{g(x)}. \quad (3)$$

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

$h(x) = (x^n - 1)/g(x)$ is called check polynomial of the cyclic code.
In \( c(x) h(x) = 0 \) all \( n \) coefficients of the polynomial in left hand side are zeros. In particular, the coefficient for \( x^i \) for \( i \geq k \) is

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

These \( r = n - k \) linear equations in matrix form are

\[
H = \begin{pmatrix}
    h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \\
    h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \\
    \vdots & \vdots & \cdots & \cdots & \cdots \\
    h_k & \cdots & h_1 & h_0
\end{pmatrix}.
\]
Polynomial with coefficients $x_k, \ldots, x_0$ is called reciprocal to

**Theorem**

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

$$g^\perp(x) = x^k h(x^{-1}).$$

**Remark:** $G$ and $H$ are in minimum span form. Trellis complexity cannot be reduced without permutations.
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></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>[7,4]</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>[7,3]</td>
<td>$m_1 m_3 = 1 + \ldots + x^6$</td>
<td>$m_0 = 1 + x$</td>
<td>7</td>
</tr>
<tr>
<td>[7,1]</td>
<td>$m_1 m_3 = 1 + \ldots + x^6$</td>
<td>$m_0 = 1 + x$</td>
<td></td>
</tr>
</tbody>
</table>
Theorem
Let \( n = 2^m - 1 \) and \( g(x) = p(x) \) is primitive polynomial. Then such a binary cyclic code is \([n, n - m] \) Hamming code with minimum distance 3.

Proof.
Let
\[
H = \begin{pmatrix}
\alpha^0 & \alpha^1 & \ldots & \alpha^{n-1}
\end{pmatrix}.
\]

Indeed, for binary sequence \( b = (b_1, \ldots, b_n) \) its syndrome \( s = b H^T \) can be equivalently expressed as \( b(x)|_{x = \alpha} \) which is equal to 0 only for those \( b(x) \) which are multiple of \( g(x) \). Since \( \alpha \) is primitive, all columns of \( H \) are different, therefore \( d_{\text{min}} \geq 3 \).
The dual to Hamming code is the simplex $[n = 2^m - 1, m]$-code with $d_{\text{min}} = (n + 1)/2$. As a cyclic codes it is determined by check polynomial $h(x) = p(x)$ where $p(x)$ is a primitive polynomial of degree $m$. Generator polynomial is $g(x) = (x^n - 1)/p(x)$. 
By direct computations we can check that

\[ x^{23} - 1 = (x - 1)g(x)\tilde{g}(x) \]

\[ g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} \]

\[ \tilde{g}(x) = x^{11}g(x^{-1}) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} \]

where \( \tilde{g}(x) \) is reciprocal to \( g(x) \).

[23,12]-code generated by \( g(x) \) is Golay code, \( d = 7 \).

Its dual [23,11]-code generated by \( (x - 1)\tilde{g}(x) \), \( d = 8 \).
Let 
\[ c = (a_0, a_1, ..., a_{n-k-1}, m_0, m_1, ..., m_{k-1}) \] 
and try to find the first \( n - k \) code symbols in such a way that entire \( c \) is a valid codeword. In terms of polynomial representation we require that 
\[ a(x) + x^{n-k}m(x) = 0 \mod g(x) \]
or 
\[ a(x) = -x^{n-k}m(x) \mod g(x) \]
Similarly, at the decoder we need to compute the syndrome for the channel output \( b(x) \): 
\[ s(x) = b(x) \mod g(x). \]
Figure: A circuit for computing syndrome of $b(x)$ as residual by modulo monic polynomial $g(x)$
Figure: A circuit for computing syndrome of $b(x)$ as residual by modulo monic polynomial $g(x) = 1 + x + x^4$
Systematic encoding

\[ m = (0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1) \]

\[ \leftrightarrow m(x) = x + x^2 + x^3 + x^7 + x^{10} \]

Residual of shifted message by modulo \( g(x) \)

\[ a(x) = x^4 m(x) \mod g(X) = x + x^2. \]

Using \( m(x) \) as input of the scheme we obtain the same result in form \( a = (0 \ 1 \ 1 \ 0) \).

The codeword in polynomial form is

\[ c(x) = a(x) + x^4 m(x) = x + x^2 + x^6 + x^7 + x^{11} + x^{14}, \]

\[ c = (a, m) = (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1) \]
\[ b = (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1) \]
Given $c(x)$ and the channel output $b(x)$, error polynomial $e(x) = b(x) - c(x)$. The generator polynomial $g(x) = 1 + x + x^4$.

\[ s = b(x)|_{x=\alpha} = \sum_{i=0}^{n-1} b_i \alpha^i = c(\alpha) + e(\alpha) = e(\alpha) = \sum_{i=0}^{n-1} e_i \alpha^i. \]

In case of single error at position $j$ this equation rewrites as

\[ \alpha^j = s. \]

If $\alpha$ is primitive, the solution is unique.
BCH codes. Example, $n = 15$, two errors

The two different roots could provide two equations. Roots $\alpha^2$, $\alpha^4$, and $\alpha^8$ do not help since.

Minimal polynomial for $\alpha^3$ as

$$m_3(x) = 1 + x + x^2 + x^3 + x^4$$

Let extended generator polynomial be

$$g(x) = m_1(x) m_3(x)$$

$$= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$$

$$= 1 + x^4 + x^6 + x^7 + x^8.$$ 

The parity-check matrix can be chosen as

$$H = \begin{pmatrix}
1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12}
\end{pmatrix}.$$
Two errors can be corrected:

\[ e(x) = x^i + x^j, \quad i \neq j; \]
\[ s_1 = b(\alpha) = \alpha^i + \alpha^j; \]
\[ s_3 = b(\alpha^3) = \alpha^{3i} + \alpha^{3j}; \]

Denote \( X_1 = \alpha^i, X_2 = \alpha^j \). These variables we call error locators.

\[
\begin{align*}
\begin{cases}
X_1 + X_2 = s_1, \\
X_1^3 + X_2^3 = s_3.
\end{cases}
\end{align*}
\]

\[
X_1^2 + X_1X_2 + X_2^2 = s_3/s_1, \quad X_1^2 + X_2^2 = s_1^2
\]

\[
\begin{align*}
\begin{cases}
X_1 + X_2 = s_1, \\
X_1X_2 = s_3/s_1 - s_1^2
\end{cases}
\end{align*}
\] (4)

Use Vieta’s theorem:

\[ x^2 + \sigma_1 x + \sigma_2 = 0, \quad \sigma_1 = X_1 + X_2, \sigma_2 = X_1X_2. \] (5)
Example

For the code above let

\[ b = (1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1) \]

Syndrome components are

\[ s_1 = \alpha^8, \ s_3 = \alpha^4. \]

\[ \sigma_1 = \alpha^{11}; \ \sigma_2 = s^3/s^1 - s^2 = \alpha^{11} \]

By substituting field elements into equation for locators

\[ X_1 = \alpha^2, \ X_2 = \alpha^9 \]

Positions 2 and 9 (starting with 0) are with errors.
Definition
A cyclic code of length \( n \) over \( GF(q) \) is called BCH code with
design distance \( d \) if for some \( b \geq 0 \) the generator polynomial
of the code is

\[
g(x) = \text{LCM}\{m_i(x), \quad i = b, b+1, ..., b+d-2\}
\]

where LCM is an abbreviation for the least common multiple,
\( m_i(x) \) denotes minimal polynomial for \( \alpha^i \), \( \alpha \) denotes a
primitive element of the field.
LCM means that \( g(x) \) is a product of different minimal
polynomials
Theorem

BCH bound. Let \( g(x) \) be the generator polynomial of a BCH code over \( GF(q) \) and \( \alpha \) denotes a primitive element. If for some \( b \geq 0 \) and \( d \geq 2 \)

\[
g(\alpha^i) = 0, \quad i = b, b + 1, \ldots, b + d - 2
\]

then minimum distance of the code is at least \( d \).
BCH codes. Proof

$H = \begin{pmatrix}
1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\
1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \ldots & \alpha^{(n-1)(b+d-2)}
\end{pmatrix}.

Let us prove that sets of $d - 1$. For columns $i_1, \ldots, i_{d-1}$

$\begin{pmatrix}
\alpha^{i_1b} & \alpha^{i_2b} & \ldots & \alpha^{i_{d-1}b} \\
\alpha^{i_1(b+1)} & \alpha^{i_2(b+1)} & \ldots & \alpha^{i_{d-1}(b+1)} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^{i_1(b+d-2)} & \alpha^{i_2(b+d-2)} & \ldots & \alpha^{i_{d-1}(b+d-2)}
\end{pmatrix}.$
Its determinant is equal to

$$\alpha^{(i_1+\ldots+i_{d-1})b} \det \begin{pmatrix}
1 & 1 & \ldots & 1 \\
\alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_{d-1}} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^{i_1(d-2)} & \alpha^{i_2(d-2)} & \ldots & \alpha^{i_{d-1}(d-2)}
\end{pmatrix}.$$

which is determinant of a famous Vandermonde matrix.

$$\det \begin{pmatrix}
1 & 1 & \ldots & 1 \\
a_1 & a_2 & \ldots & a_m \\
\vdots & \vdots & \ddots & \vdots \\
a_1^{m-1} & a_2^{m-1} & \ldots & a_m^{m-1}
\end{pmatrix} = \prod_{j=1}^{m-1} \prod_{i=j+1}^{m} (a_i - a_j),$$

determinant is not zero if all $a^i$ are different
**Theorem**

The dimension of BCH code over $\text{GF}(p)$ of length $n$ and with design distance $d$ the generator polynomial has roots in $\text{GF}(p^m)$ is at least $n - m(d - 1)$.

**Proof.**

The degree of polynomial is $\leq m$, the number of multipliers $\leq d - 1$. Therefore, degree of $g(x)$ is $\leq m(d - 1)$.

For binary BCH codes minimal polynomial $m_{2i}(x)$ is the same as $m_i(x)$, the generator polynomial

$$g(x) = \text{LCM} \{ M_1(x), M_3(x), \ldots, M_{2t-1}(x) \},$$

determines the code with the design distance $d = 2t + 1$.

Therefore, for binary codes

$$k \geq n - mt.$$
Definition

In $\text{GF}(p^m)$ for $\alpha \in \text{GF}(p^m)$ elements $\alpha, \alpha^p, \alpha^{p^2}, \ldots$, are called conjugates of $\alpha$. The set of conjugates is called conjugacy class of $\alpha$ in $\text{GF}(p^m)$. The set of degrees of elements belonging to the same conjugacy class is called a cyclotomic class.

Cyclotomic classes for binary codes of length $n = 15$

\[
\begin{align*}
C_0 &= \{0\}; \\
C_1 &= \{1, 2, 4, 8\}; \\
C_3 &= \{3, 6, 12, 9\}; \\
C_5 &= \{5, 10\}; \\
C_7 &= \{7, 14, 13, 11\}. 
\end{align*}
\]
**Definition**

BCH codes of length of the form \( n = q^m - 1 \) called *primitive*. Lengths of non-primitive codes are divide \( q^m - 1 \) for some \( m \).

<table>
<thead>
<tr>
<th>Degrees of ( \alpha )</th>
<th>Generating polynomial</th>
<th>Dimension ( n - \deg g(x) )</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( M_0(x) = x + 1 )</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>1,2,4,8</td>
<td>( M_1(x) )</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>0,1,2,4,8</td>
<td>( M_0(x)M_1(x) )</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>1,2,3,4,6,9,12</td>
<td>( M_1(x)M_3(x) )</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>1,...,5,6,8,9,10,12</td>
<td>( M_1(x)M_3(x) \times \times M_5(x) )</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>1,2,...,14</td>
<td>( M_1(x)M_3(x) \times \times M_5(x)M_7(x) )</td>
<td>1</td>
<td>15</td>
</tr>
</tbody>
</table>
Non-primitive BCH codes. Example, \( n = 23 \)

From \( 2^{11} - 1 = 23 \times 89 \) choose \( n = 23 \).

\[
C_0 = \{0\}; \\
C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}; \\
C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}.
\]

<table>
<thead>
<tr>
<th>Degrees</th>
<th>Generating polynomial</th>
<th>Dimension ( n - \deg g(x) )</th>
<th>Distance design</th>
<th>Distance true</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( M_0(x) = x + 1 )</td>
<td>22</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1,2,3,4,6,8,...</td>
<td>( M_1(x) )</td>
<td>12</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>...19,20,21,22,...</td>
<td>( M_5(x) )</td>
<td>12</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>0,1,2,3,4,6,...</td>
<td>( M_0(x)M_1(x) )</td>
<td>11</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>1,...,23</td>
<td>( M_1(x)M_5(x) )</td>
<td>1</td>
<td>23</td>
<td>23</td>
</tr>
</tbody>
</table>
Redundancy decrease degrees of minimal polynomials. They are \( \geq 1 \). Degrees are 1 if if roots belong to the same field as the code alphabet, \( \beta \in \text{GF}(q) \) has minimal polynomial is \( x - \beta \), \( n \leq q - 1 \).

**Definition**

BCH code of length \( n = q - 1 \) over \( \text{GF}(q) \) is called the Reed-Solomon code.

The generator polynomial for RS code is

\[
g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \times \cdots \times (x - \alpha^{b+d-2}).
\]

\[d - 1 = n - k,\]
Let $b = 1$, $n = 15$, alphabet $\text{GF}(2^4)$ and

$$
g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)
= \alpha^{10} + \alpha^3 x + \alpha^6 x^2 + \alpha^{13} x^3 + x^4
$$

Parameters of RS code are $[n = 15, k = 11, q = 16]$, $d = 5$. Binary code of length $n = 15$, $d = 5$ has $k = 7$. The RS code as binary code is $[60,44]$. $d = 5$ (for the best code $d = 6$).
Important property:

**Theorem**  
*Any set of $k$ symbols is information set.*

**Proof.**  
Otherwise there exists a codeword with $k$ zeros and minimum distance is less than $n - k + 1$.  

$\blacksquare$
BCH and RS. Summary

- BCH codes are infinite family of cyclic binary and non-binary codes.
- Design distance depends on properties of cyclotomic classes. True distance can be larger than design distance.
- RS codes have maximum achievable distance satisfying to Singleton bound.
- Hard decision decoding with correcting capability guaranteed by design distance has polynomial ($\approx n^2$) complexity.