Lecture 5: Cyclic codes. BCH codes.

Invited lecturer: Pavel Rybin

p.rybin@skoltech.ru

Teaching Assistant: Stanislav Kruglik

stanislav.kruglik@skolkovotech.ru

February 8, 2018

Outline

Outline

1. Cyclic codes
2. BCH codes
3. Bounded minimum distance decoding

Ideal, principal ideal, principal ideal ring

Here and in what follows by K we denote a commutative ring with 1.

Definition

$J \subseteq K$ is an ideal if $KJ \subset J$, i.e.

$$\forall a \in K, j \in J : aj \in J.$$

Ideal, principal ideal, principal ideal ring

Here and in what follows by K we denote a commutative ring with 1.

Definition

An ideal J is called a principal ideal if it is generated by one element

$$\exists g \in J : \forall j \in J \;\; j = bg, \;\text{ where }\; b \in K$$

Notation

$$J = (g).$$

Definition

The ring in which any ideal is principal is called a principal ideal ring.

$\mathbb{F}[x]$ is a principal ideal ring

Theorem

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a principal ideal ring.

Proof.

Let $J \subseteq \mathbb{F}[x]$ and $g \in J$ be a normalized polynomial of minimal degree.
For any other polynomial $f \in J$

$$f = hg + r, \;\; \deg r < \deg g.$$

As $r = f - hg \in J$, then $r = 0$. □

Quotient ring

Let J be an ideal, then K/J is a quotient ring.

$$[f] + [g] = (f + J) + (g + J) = [f + g]$$

$$[f][g] = (f + J)(g + J) = [fg]$$

Quotient ring, that we need

We need such a quotient ring, which is also a vector space.

$$K/J = \mathbb{F}_q[x]/(x^n - 1) = \langle 1, x, x^2, \ldots, x^{n-1} \rangle.$$

Polynomial code

Definition

A linear code $\mathcal{C} \subseteq \mathbb{F}_q[x]/(x^n - 1)$ is called a polynomial code if $\mathcal{C}$ is an ideal.

- The codewords of polynomial code are polynomials

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \Leftrightarrow (a_0, a_1, \ldots, a_{n-1})$$

- $\mathcal{C}$ is an ideal $\Rightarrow \mathcal{C}$ is a linear code
- $\mathcal{C}$ is a linear code $\not\Rightarrow \mathcal{C}$ is an ideal $\mathcal{C} = \langle 1, x \rangle$ is not an ideal in $\mathbb{F}_2[x]/(x^3 + 1)$

Cyclic code

Definition

The code $\mathcal{C}$ is cyclic if

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \Leftarrow (a_{n-1}, a_0, \ldots, a_{n-2}) \in \mathcal{C}$$

Example

$\mathcal{C} = \{001, 010, 100\}$.

Equivalence of polynomial and cyclic codes

Theorem

Let $\mathcal{C}$ be a linear code in $K = \mathbb{F}_q[x]/(x^n - 1)$. $\mathcal{C}$ is cyclic iff $\mathcal{C}$ is an ideal.

Sufficient condition.

$$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

Note, that

$$xc(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-1}(x^n - 1) = (c_{n-1}, c_0, \ldots, c_{n-2}).$$

$\square$

Equivalence of polynomial and cyclic codes

Necessary condition.

$$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

Note, that

$$xc(x), x^2 c(x), \ldots, x^{n-1} c(x) \in \mathcal{C}.$$

Thus,

$$(\sum_j b_j x^j) c(x) \in \mathcal{C}.$$

$\square$

Generator polynomial

Definition

$g(x)$ is a generator polynomial of $\mathcal{C}$ if $g(x)$ is a normalized polynomial of smallest degree in $\mathcal{C}$.

$$\deg g(x) = n - k \Rightarrow \mathcal{C} = (g) = \{ag : \deg a \leq k - 1\}$$

$a(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$ is an information polynomial,
$c(x) = a(x)g(x)$ is a code polynomial.

Generator polynomial

Theorem

Let $g(x)$ be a generator polynomial of cyclic code $\mathcal{C} \subseteq \mathbb{F}_q[x]/(x^n - 1)$. Then $g(x) | x^n - 1$.

Proof.

Assume $g(x) \not| x^n - 1$, then

$$x^n - 1 = g(x)h(x) + r(x).$$

As we see $r(x) \in \mathcal{C}$ and we come to contradiction. $\square$

Check polynomial

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

- $\deg g(x) = n - k$
- $\deg h(x) = k$
- $g(x)h(x) = 0 \mod x^n - 1$
- $c(x) \in \mathcal{C} \Rightarrow c(x)h(x) = 0 \mod x^n - 1$

Generator matrix

Theorem

$$\mathcal{C} = \langle g(x), xg(x), \ldots, x^{k-1}g(x)\rangle.$$

$$G = G_{k\times n} = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix}$$

Parity check matrix

$$H = H_{(n-k)\times n} = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

$$(\sum_i g_i x^i)(\sum_j h_j x^j) = \sum x^m (\sum_{i+j=m} g_i h_j).$$

$C^\perp \neq (h)$, $C^\perp = (\hat{h})$, where $\hat{h}(x) = x^k h(1/x)$.

Encoding

Non-systematic

$$c(x) = a(x)g(x)$$

Systematic

$$a'(x) = x^{n-k}a(x) = g(x)b(x) + r(x).$$

$$c(x) = a'(x) - r(x) \in \mathcal{C}.$$

Syndrome

$$S(x) = S_{y(x)} = y(x) \mod g(x).$$

Properties

$$S_{xy(x)}(x) = xS_{y(x)} \mod g(x)$$

Burst of errors

Burst of errors is a sequence of L consequent bits with errors (errors at margins are mandatory).

$$e(x) = 000001101101000000, L = 7.$$

Burst of errors

Theorem

Let $\mathcal{C}$ be a cyclic code, then it detects any error burst of length $\leq n - k$.

Proof.

Assume $e(x)$ is not detected. Then $g(x) | x^j b(x)$.
Note, that as $g(x) | x^n - 1$, then $(g(x), x^k) = 1$.
This means, that $g(x) | b(x)$, but $\deg b(x) \leq L - 1 = n - k - 1$.

□

Primitive cyclic codes

For a code over $\mathbb{F}_q$ a length $n = q^m - 1$, where $m \in \mathbb{N}$ is called primitive. A cyclic code of primitive length is called primitive.

- Let $\mathcal{C} = (g)$ and $\beta_1, \ldots, \beta_{n-k}$ are the roots of g, the $\beta_i \in \mathbb{F}_q^m$;
- $c(x) \in \mathcal{C} \Rightarrow c(\beta_i) = 0$
- Any primitive cyclic code can be described by the roots of g.
- Let $\alpha_1, \ldots, \alpha_s$ be the elements of extension field and let $m_j(x)$ be a minimal polynomial of $\alpha_j \in \mathbb{F}_q$.

$$g(x) = LCM(m_1(x), \ldots, m_s(x)).$$

Cyclic Hamming code

$$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$$

$$\alpha^3 = \alpha + 1$$

$$\begin{array}{c|c}
0 & 000 \\
1 & 001 \\
\alpha & 010 \\
\alpha^2 & 100 \\
\alpha^3 & 011 \\
\alpha^4 & 110 \\
\alpha^5 & 111 \\
\alpha^6 & 101
\end{array}$$

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

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}$$

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

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

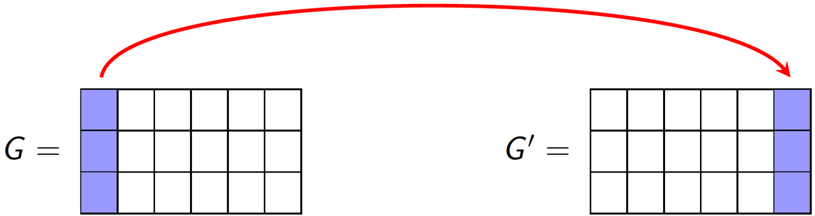
CRC code

Definition

Let $p(x) \in \mathbb{F}_2[x]$ be a primitive polynomial of degree m. CRC code is defined by
$$g(x) = (x+1)p(x).$$

- $n = 2^m - 1$
- $\deg g = m + 1$
- $k = 2^m - m - 2$
- $\mathbf{H} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$
- $d = 4$
- $L = n - k = m + 1.$

Check if the code is cyclic



$$\mathbf{G}'\mathbf{H} = \mathbf{0}.$$

Outline

BCH codes

- R. C. Bose, D. K. Ray-Chaudhury, 1960; A. Hocquenghem, 1959.
- BCH code is a cyclic code over $\mathbb{F}_q$
- Parameters: length n, designed distance d, $b \in \mathbb{N}$
- m – minimal number, such that $n | q^m - 1$

$$\exists \beta \in \mathbb{F}_q^* : |\beta| = n.$$

BCH codes

Definition

BCH code is defined by the roots of generator polynomial

$$\beta^{b}, \beta^{b+1}, \ldots, \beta^{b+d-2}.$$

$$g(x) = LCM(m_b(x), \ldots, m_{b+d-2}(x)).$$

BCH codes

Definition

- $b = 1 \Rightarrow$ narrow sense BCH code;
- $n = q^m - 1 \Rightarrow$ primitive BCH code;
- $m = 1$, $n = q - 1 \Rightarrow$ RS code.

Parity check matrix

$$H = \begin{pmatrix} 1 & \beta^b & (\beta^b)^2 & \dots & (\beta^b)^{n-1} \\ 1 & \beta^{b+1} & (\beta^{b+1})^2 & \dots & (\beta^{b+1})^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \beta^{b+d-2} & (\beta^{b+d-2})^2 & \dots & (\beta^{b+d-2})^{n-1} \end{pmatrix}.$$

Example

$q = 2,\ n = 15,\ t = 2,\ b = 1$

- the code is primitive as $15 = 2^4 - 1$;
- $m = 4$

  $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4 + x + 1)$, $\alpha^4 = \alpha + 1$:

0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1

- $d = 5$
- Roots: $\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$
- $m_\alpha(x) = m_{\alpha^2}(x) = m_{\alpha^4}(x) = x^4 + x + 1$
- $m_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$
- $g(x) = x^8 + x^7 + x^6 + x^4 + 1$

Example

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha^1 & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^1 & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

Example

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1

$$H' = \begin{pmatrix} 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \end{pmatrix}$$

Outline

Notations

Let us consider a situation when t errors $\{e_{j_1}, e_{j_2}, \dots, e_{j_t}\}$.
We introduce a notation of error locator

$$X_i = \alpha^{e_{j_i}}, \;\; i = 1, \dots, t.$$

and error values $Y_i = e_{j_i}$, $i = 1, \dots, t$.
Let $\mathbf{S} = (S_1, S_2, \dots, S_{2t})$. The syndrome can be calculated as follows

$$\begin{aligned} S_1 &= Y_1X_1 + Y_2X_2 + \ldots + Y_tX_t \\ S_2 &= Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_tX_t^2 \\ \ldots & \\ S_{2t} &= Y_1X_1^t + Y_2X_2^t + \ldots + Y_tX_t^t \end{aligned}$$

Polynomials

Syndrome polynomial

$$S(z) = \sum_{j=1}^{2t} S_j z^{j-1}$$

Error locator polynomial

$$\sigma(z) = \prod_{i=1}^{t} (X_i z - 1)$$

Error value polynomial

$$\omega(z) = \sum_{i=1}^{t} Y_i X_i \prod_{l=1, l \neq i}^{t} (X_l z - 1).$$

Additional (unnamed) polynomial

$$\Phi(z) = \sum_{i=1}^{t} Y_i X_i^{2t+1} \prod_{l=1, l \neq i}^{t} (X_l z - 1).$$

Key equation

$$S(z)\sigma(z) = z^{2t}\Phi(z) - \omega(z)$$

To solve the equation use extended Euclidean algorithm. Start with polynomial z^{2t} and $S(z)$, stop when the degree of residue is less or equal $t-1$ for the first time. Use extended Euclidean algorithm to find $\sigma(z)$ and $\omega(z)$

Chien search

We know $\sigma(z)$, find X_i by exhaustive search over all the elements of $\mathbb{F}_q$.

Forney's algorithm

$$Y_i = \frac{\omega(X_i^{-1})}{\sigma_z'(X_i^{-1})} \;\; i = 1, \ldots, t.$$

Thank you for your attention!