Lecture 6: Methods for combining codes

Invited lecturer: Pavel Rybin

p.rybin@skoltech.ru

Teaching Assistant: Stanislav Kruglik

stanislav.kruglik@skolkovotech.ru

February 9, 2018

Outline

Outline

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

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

Bounded minimum distance decoding. Notations

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

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

and error values $Y_i = e_{j_i}$, $i = 1, \ldots, t$.
Let $\mathbf{S} = (S_1, S_2, \ldots, S_{2t})$. 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

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

Outline

Asymptotic regime, $n \to \infty$

$\frac{d}{n} \to \delta$ (relative minimum distance), $\frac{k}{n} \to R$ (code rate).

Definition

A code family $\{\mathcal{C}_n\}$ is said to be *asymptotically good* if there exist constants $R, \delta > 0$:

- $\frac{k_n}{n} \geq R > 0$;
- $\frac{d_n}{n} \geq \delta > 0$;

Are the codes we already know asymptotically good?

1. $(n = 2^m - 1, k = 2^m - m - 1, d = 3)_2$ Hamming codes
   - $R = \frac{2^m - m - 1}{2^m - 1} \to 1$;
   - $\delta = \frac{3}{2^m - 1} \to 0$.
2. $(n = 2^m, k, d)_2$ $RM(m, s)$ code
   - $k = \sum\limits_{i=0}^{s} \binom{m}{i} = V_s$;
   - $d = 2^{m-s}$;
   - $R = \frac{V_r}{2^m}$
   - $\delta = 2^{-s}$.

Statement

Hamming and RM codes are asymptotically bad.

Are the codes we already know asymptotically good?

BCH codes:

- $t = \text{const}$. Hamming bound

$$n - k \geq t \log n + O(1).$$

BCH code

$$n - k \leq t \log n + O(1).$$

BCH codes are good!

- t grows with n

Theorem

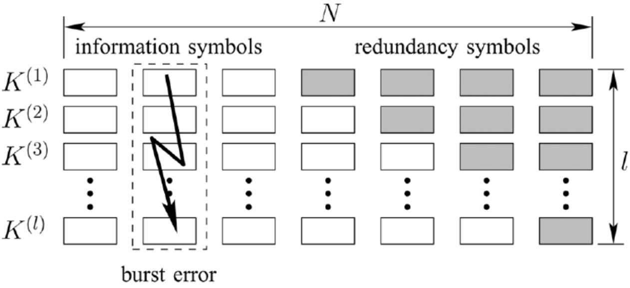
Let $n \to \infty$ and $\delta > 0$, then the rate of BCH code $R \to 0$.

BCH codes are asymptotically bad.

Solution: combine existing codes and construct new asymptotically good codes!

Outline

Interleaved codes

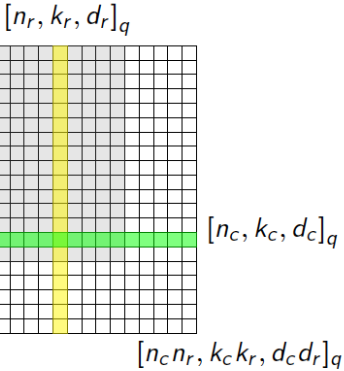


$$R = \frac{\sum R_i}{\ell}.$$

Outline

Construction

A codeword of a product code is a matrix whose rows are codewords of the first component code and whose columns are codewords of the second component code.

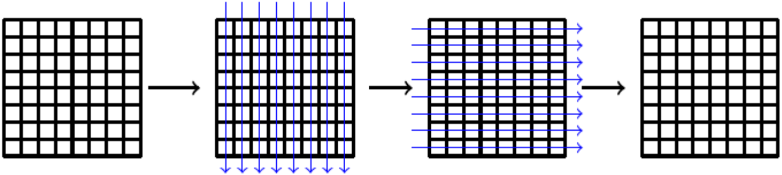


Parameters

Consider a product code $\mathcal{C}$ constructed from row code $\mathcal{C}_r$ and column code $\mathcal{C}_c$, then

$$\begin{aligned} n(\mathcal{C}) &= n_r n_c \\ R(\mathcal{C}) &= R(\mathcal{C}_r)R(\mathcal{C}_c) \\ d(\mathcal{C}) &\geq d(\mathcal{C}_r)d(\mathcal{C}_c) \end{aligned}$$

Iterative decoder



Generator matrix

Statement

Let G_r and G_c be generator matrices of a row code $\mathcal{C}_r$ and a column code $\mathcal{C}_c$, then

$$G = G_r \otimes G_c.$$

Recall the Kronecker product definition. Let $\mathbf{X} = [x_{i,j}]$ be of size $m_x \times n_x$, $\mathbf{Y} = [y_{i,j}]$ be of size $m_y \times n_y$, then

$$X \otimes Y = \begin{bmatrix} x_{1,1}Y & x_{1,2}Y & \dots & x_{1,n_x}Y \\ x_{2,1}Y & x_{2,2}Y & \dots & x_{2,n_x}Y \\ \vdots & \vdots & \ddots & \vdots \\ x_{m_x,1}Y & x_{m_x,2}Y & \dots & x_{m_x,n_x}Y \end{bmatrix}$$

Product of cyclic codes

Statement

Let $\mathcal{C}_r$ and $\mathcal{C}_c$ be cyclic codes with $(n_r, n_c) = 1$, then $\mathcal{C} = \mathcal{C}_r \otimes \mathcal{C}_c$ is also cyclic.

Outline

Problem 1

Generator polynom of $(15, 5)$ cyclic code over $\mathbb{F}(2)$ has form $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Write its' generator and parity-check matrix.

Problem 2

Let generator plolynom of cyclic code over $\mathbb{F}(2)$ has a form $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. Find the lenght of such code.

Problem 3

- Constuct field $\mathbb{F}_2^{16}$ over modulo of $\phi(x) = 1 + x + x^4$
- Find the generator matrix of $(15, 7)$-BCH code which can correct two errors
- Decode vector $y = (001100101100000)$

Thank you for your attention!