Lecture 9: Methods for combining codes.

Course instructor: Alexey Frolov

al.frolov@skoltech.ru

Teaching Assistant: Stanislav Kruglik

stanislav.kruglik@skolkovotech.ru

February 17, 2017

Outline

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:

- $t =$ 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

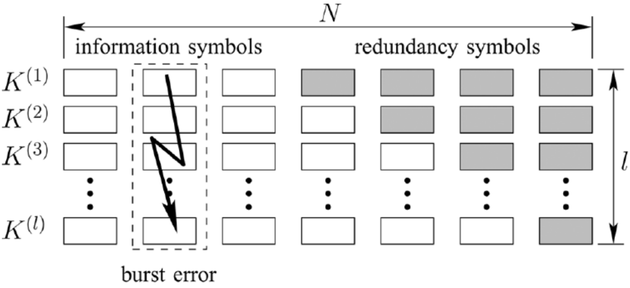
Let $n \to \infty$ and $\delta > 0$, then the rate of BCH code $R \to 0$.

BCH codes are asymptotically bad.

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

Outline

Interleaved codes

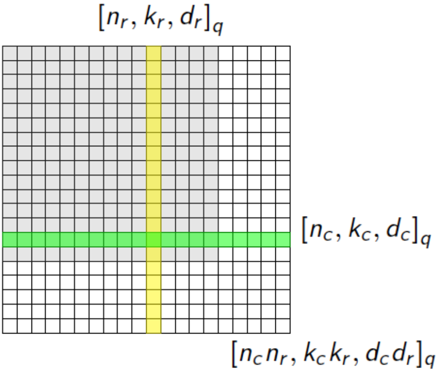


$$R = \frac{\sum R_i}{\ell}.$$

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.

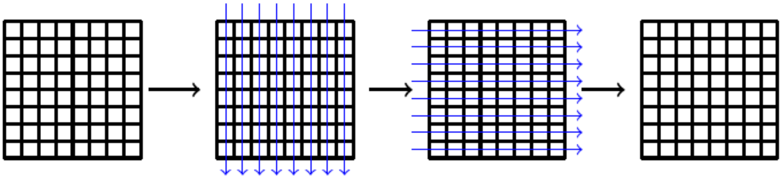


Parameters

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

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

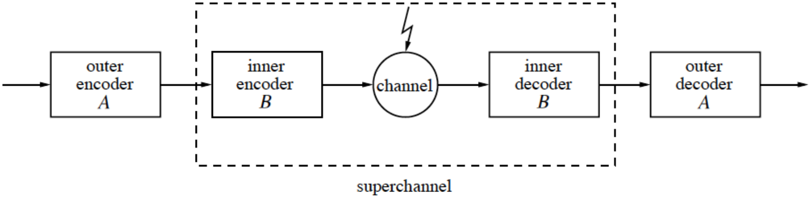
Product of cyclic codes

Statement

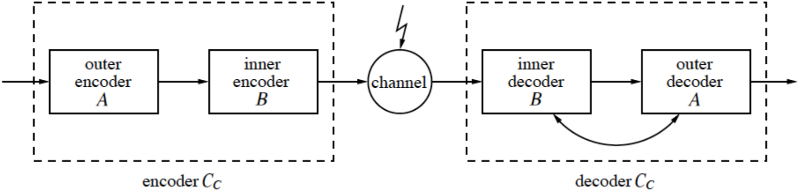
Let $\mathcal{C}_r$ and $\mathcal{C}_c$ be cyclic codes with $(n_r, n_c) = 1$, then $\mathcal{C} = \mathcal{C}_r \otimes \mathcal{C}_c$ is also cyclic.

Outline

Forney's view



Concatenation according to Blokh and Zyablov



Construction

Inner and outer codes:

- Outer (n_a, k_a) code A over $\mathbb{F}_{q^{k_b}}$.
- Inner (n_b, k_b) code B over $\mathbb{F}_q$.

Parameters of $A \diamond B$:

$$\begin{aligned} N &= n_a n_b \text{ (symbols from } \mathbb{F}_q) \\ R &= R_a R_b \\ D &\geq d_a d_b \end{aligned}$$

Zyablov bound

Theorem

Let $R \in (0,1)$, then it is possible to construct a code of rate R and distance

$$\delta(R) = \max_{R \le r \le 1} \left(1 - \frac{R}{r}\right) h^{-1}(1-r),$$

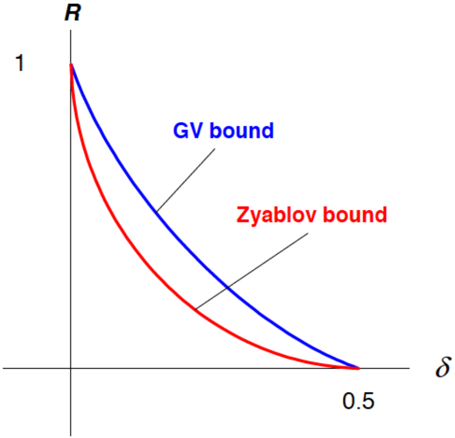
where h^{-1} is the inverse of entropy function.

Proof.

Outer code: $[n_a, k_a]$ RS code over $\mathbb{F}_Q$, $Q = q^{k_b}$, $n_a = Q - 1$.

Inner code: $[n_b, k_b]$ code over $\mathbb{F}_q$, which meets the VG bound. $\square$

Zyablov bound



Decoder

Decoder all the inner codes, then decode the outer code.

With this decoder we can decode up to $\frac{d_a d_b}{4}$ errors.

How to improve the number of correctable errors? We want to decode up to $D/2$.

Generalized minimum distance decoder

Forget for a while about concatenated codes. Assume we are give a code $\mathcal{C}$ of length n. We send a codeword $\mathbf{x}$ and received a sequence $\mathbf{y}$ with errors. Assume are also provided with the reliabilities α_i, $i = 1, \ldots, n$.

$$f(\mathbf{x}, \mathbf{y}, \alpha) = \sum_{i=1}^{n} \alpha_i \phi(x_i, y_i),$$

where $\phi(x_i, y_i) = +1$ if $x_i = y_i$ and $\phi(x_i, y_i) = -1$ otherwise.

Generalized minimum distance decoder

$$d(\mathbf{x}, \mathbf{y}, \alpha) = n - f(\mathbf{x}, \mathbf{y}, \alpha).$$

Theorem

Forney
Assume we are given an (n, k, d) code $\mathcal{C}$. If there exists a codeword c, such that $d(c, \mathbf{y}, \alpha) < d$, then c will be recovered from one of the decoding trials.

In a trial i, $i = 0, \dots, d-1$, we erase i least reliable symbols.

GMD for concatenated codes

Let us decode all the inner codes. How to introduce the reliabilities for outer code?

Let us consider the first inner code. $\mathbf{y}$ is the sequence to be decoded, $\hat{\mathbf{x}}$ is the decoding result.

$$\begin{aligned} \alpha_1 &= 0, \text{ (decoding failure)} \\ \alpha_1 &= n_b - d(\mathbf{y}, \hat{\mathbf{x}}), \text{ (otherwise)} \end{aligned}$$

This method allows to decode up to $D/2$.

Outline

Generalized concatenated codes

The main difference:

- ℓ outer codes A_i, $i = 1, \ldots, \ell$;
- ℓ nested inner codes

$$B_1 \subset B_2 \subset \ldots \subset B_\ell.$$

Distance estimate

$$D \geq \min_{1 \leq i \leq \ell} d_b^{(i)} d_a^{(i)}.$$

Thank you for your attention!