Lecture 4: MacWilliams identities. Reed–Solomon codes.

Invited lecturer: Pavel Rybin

p.rybin@skoltech.ru

Teaching Assistant: Stanislav Kruglik

stanislav.kruglik@skolkovotech.ru

February 5, 2018

Outline

Outline

Weight spectrum and enumerator

Definition

Let $\mathcal{C}$ be a linear (n, k, d) code. A vector $A(\mathcal{C}) = [A_0, A_1, \dots, A_n]$, where

$$A_W = |\{c \in \mathcal{C} : ||c|| = W\}|.$$

is called a weight spectrum of $\mathcal{C}$.

Definition

Let $A(\mathcal{C}) = [A_0, A_1, \dots, A_n]$ be a weight spectrum of a code $\mathcal{C}$, then

$$W_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{c \in \mathcal{C}} x^{n-||c||} y^{||c||}$$

is called a weight enumerator of $\mathcal{C}$.

Example

Example

$\mathcal{C} = \{000, 011, 101, 110\}$

$$W_{\mathcal{C}}(x, y) = x^3 + 3xy^2$$

.

MacWilliams identities

Theorem (F. J. MacWilliams, 1963))

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + y, x - y).$$

Hadamard transform

Definition (Dot product)

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$:

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 \oplus \ldots x_n y_n.$$

Definition (Hadamard transform)

Let f be an arbitrarily function defined on $\mathbb{F}_2^n$. Then

$$\hat{f}(\mathbf{x}) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} (-1)^{\mathbf{a} \cdot \mathbf{x}} f(\mathbf{a}).$$

is called a Hadamard transform of f.

Lemma

$$\sum_{\mathbf{x} \in \mathcal{C}^{\perp}} f(\mathbf{x}) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{x} \in \mathcal{C}} \hat{f}(\mathbf{x})$$

Proof of lemma

$$\sum_{\mathbf{x}\in\mathcal{C}} \hat{f}(\mathbf{x}) = \sum_{\mathbf{x}\in\mathcal{C}} \sum_{\mathbf{a}\in\mathbb{F}_2^n} (-1)^{\mathbf{a}\cdot\mathbf{x}} f(\mathbf{a}) =$$

$$= \sum_{\mathbf{a}\in\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} f(\mathbf{a}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} =$$

$$= \sum_{\mathbf{a}\in\mathcal{C}^\perp} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} + \sum_{\mathbf{a}\notin\mathcal{C}^\perp} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}}$$

1. $\forall\, \mathbf{a} \in \mathcal{C}^\perp, \mathbf{x} \in \mathcal{C}: \quad \mathbf{a}\cdot\mathbf{x} = 0 \;\Rightarrow$

$$\sum_{\mathbf{a}\in\mathcal{C}^\perp} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} = \sum_{\mathbf{a}\in\mathcal{C}^\perp} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} 1 = |\mathcal{C}| \sum_{\mathbf{a}\in\mathcal{C}^\perp} f(\mathbf{a})$$

2. $\forall\, \mathbf{a} \notin \mathcal{C}^\perp$: «$\mathbf{a}\cdot\mathbf{x} = 0$» и «$\mathbf{a}\cdot\mathbf{x} = 1$» occur equal times in the second sum $\Rightarrow \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} = 0 \;\Rightarrow$

$$\sum_{\mathbf{a}\notin\mathcal{C}^\perp} f(\mathbf{a}) \sum_{\mathbf{x}\in\mathcal{C}} (-1)^{\mathbf{a}\cdot\mathbf{x}} = 0 \qquad \square$$

Proof of theorem

Consider

$$f(\mathbf{b}) = x^{n-\|\mathbf{b}\|} y^{\|\mathbf{b}\|}$$

Apply Hadamard transform

$$\hat{f}(\mathbf{a}) = \sum_{\mathbf{b}\in\mathbb{F}_2^n} (-1)^{\mathbf{a}\cdot\mathbf{b}} f(\mathbf{b}) = \sum_{\mathbf{b}\in\mathbb{F}_2^n} (-1)^{\mathbf{a}\cdot\mathbf{b}} x^{n-\|\mathbf{b}\|} y^{\|\mathbf{b}\|} =$$

(Note, that $y^{\|\mathbf{b}\|} = y^{b_1} \dots y^{b_n}$ и $x^{n-\|\mathbf{b}\|} = x^{1-b_1} \dots x^{1-b_n}$)

$$= \sum_{\mathbf{b}\in\mathbb{F}_2^n} (-1)^{a_1 b_1 + \ldots + a_n b_n} \prod_{i=1}^{n} x^{1-b_i} y^{b_i} =$$

$$= \sum_{b_1=0}^{1} \sum_{b_2=0}^{1} \cdots \sum_{b_n=0}^{1} \prod_{i=1}^{n} (-1)^{a_i b_i} x^{1-b_i} y^{b_i} =$$

$$= \prod_{i=1}^{n} \sum_{w=0}^{1} (-1)^{a_i w} x^{1-w} y^{w} =$$

Proof of theorem

$$\hat{f}(\mathbf{a}) = \ldots = \prod_{i=1}^{n} \sum_{w=0}^{1} (-1)^{a_i w} x^{1-w} y^{w} =$$

$$= (x+y)^{n-\|\mathbf{a}\|}(x-y)^{\|\mathbf{a}\|},$$

as

$$\sum_{w=0}^{1} (-1)^{a_i w} x^{1-w} y^{w} = \begin{cases} x+y, & \text{если } a_i = 0, \\ x-y, & \text{если } a_i = 1. \end{cases}$$

According to lemma
$$\frac{1}{|\mathcal{C}|} \sum_{\mathbf{a}\in\mathcal{C}} \hat{f}(\mathbf{a}) = \sum_{\mathbf{a}\in\mathcal{C}^{\perp}} f(\mathbf{a}),$$

thus
$$\frac{1}{|\mathcal{C}|} \sum_{\mathbf{a}\in\mathcal{C}} (x+y)^{n-\|\mathbf{a}\|}(x-y)^{\|\mathbf{a}\|} = \sum_{\mathbf{a}\in\mathcal{C}^{\perp}} x^{n-\|\mathbf{a}\|} y^{\|\mathbf{a}\|}. \qquad \square$$

Example

Example

Let $\mathbf{H} = [11\ldots1]$ be a parity check matrix of single parity check (SPC) code with length n. Find its enumerator.
Note, that the dual code is a repetition code with

$$W_{\mathcal{C}^\perp}(x,y) = x^n + y^n,$$

thus we have

$$W_{\mathcal{C}}(x,y) = \frac{1}{|\mathcal{C}^\perp|}\left[(x+y)^n + (x-y)^n\right] = \frac{1}{2}\left[(x+y)^n + (x-y)^n\right].$$

Outline

MDS code

Definition

An (n, k, d) code is called Maximum Distance Separable (MDS) code if

$$d = n - k + 1.$$

This means, that the code meets the Singleton bound.

Properties of MDS codes

Proposition

A q-ary $[n, k]$ linear code is an MDS code precisely if the parity check matrix $\mathbf{H}$ has every set of $n - k$ columns linearly independent.

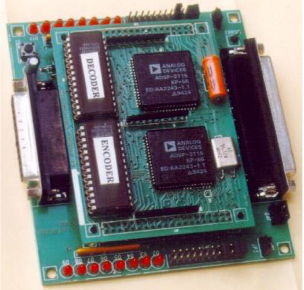
Proposition

The code $\mathcal{C}^{\perp}$ dual to $\mathcal{C}$ is a linear MDS code if $\mathcal{C}$ itself is a linear MDS code.

Outline

The best algebraic codes

Millions of error-correcting codes are decoded **every minute**, with efficient algorithms implemented in custom VLSI circuits.



At least 50% of these VLSI circuits **decode Reed-Solomon codes.**

I.S. Reed and G. Solomon, Polynomial codes over certain finite fields, *Journal Society Indust. Appl. Math.* **8**, pp. 300-304, June 1960.

RS codes are used in ...

RS codes: generator matrix view

Let $\mathbb{F}_q$ be the finite field of order q and let $\mathbb{F}_q[x]$ denote the ring of polynomials over $\mathbb{F}_q$ in the variable x. Given a set $\mathcal{B}$ of n pairwise different field elements

$$\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

from $\mathbb{F}_q$.

The Reed-Solomon code $RS(n,k)$, $1 \leq k \leq n$, is defined as follows

$$RS(n,k) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \deg f(x) < k\}.$$

The Reed-Solomon code is a linear code over $\mathbb{F}_q$. It has length $n \leq q$, dimension k and $d = n - k + 1$.

RS codes: distance and generator matrix

The polynomial of degree $\leq k-1$ cannot have more than $k-1$ roots (zeroes), thus

$$d = n - k + 1.$$

Generator matrix

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{k-1} & {\alpha_2}^{k-1} & \dots & {\alpha_n}^{k-1} \end{bmatrix}$$

Encoding

$$c = f\mathbf{G},$$

where $f = (f_0, f_1, \dots, f_{k-1})$ – vector of coefficients of $f(x)$.

RS codes: parity check matrix view

Generator polynomial:

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1}).$$

Encoding:

$$c(x) = f(x)g(x).$$

Parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{d-1} & \dots & \alpha^{(d-1)(n-1)} \end{bmatrix}$$

What is the connection in between two points of view?

Discrete Fourier Transform

$$F = [\alpha^{ij}]_{i=0,\dots,n-1}^{j=0,\dots,n-1} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ 1 & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{bmatrix}$$

Discrete Fourier Transform

Information:

$$f = [f_0 f_1 \dots f_{k-1} 0 \dots 0]$$

Apply DFT to obtain a codeword

$$c = Ff$$

$$\begin{aligned}
c(\alpha^{-k}) &= c(\alpha^{n-k}) = c(\alpha^{d-1}) = 0 \\
c(\alpha^{-k-1}) &= c(\alpha^{n-k-1}) = c(\alpha^{d-2}) = 0 \\
\vdots &= \vdots \\
c(\alpha^{-(n-1)}) &= c(\alpha) = 0
\end{aligned}$$

Outline

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

$$\begin{aligned}
S_1 &= Y_1 X_1 + Y_2 X_2 + \ldots + Y_t X_t \\
S_1 &= Y_1 X_1^2 + Y_2 X_2^2 + \ldots + Y_t X_t^2 \\
\ldots & \\
S_1 &= Y_1 X_1^t + Y_2 X_2^t + \ldots + Y_t X_t^t
\end{aligned}$$

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

Problem 1

- Consider a $(7, 5)$ Rid-Solomon code over field $\mathbb{F}_2^8$ which gerating element is equal to the root of $\phi(x) = x^3 + x^2 + 1$
- After transmission of codevector over noisy channel weigh one error was added and we received $Y = V + E = [\alpha^5, \alpha^2, \alpha^4, 0, 0, \alpha, \alpha^6]$ Correct error and find information vector

Thank you for your attention!