Tutorial II group 2

26 September 2019 15:57

LINEAR CODES

$C \in \{0,1\}^n$

I. Important parameters (n, M, d)

length of codewords

number of codewords

minimum distance

to calculate d you need to calculate Hamming distance of every pair of codewords $O(n^2)$

II. ENCODE:

$$\boxed{\begin{array}{c} m_0 \longrightarrow c_0 \\ \vdots \\ m_M \longrightarrow c_M \end{array}}$$

III. DECODING

Upon recieving w. You need to find $c \in C$ with minimum Hamming distance

$$\min_{c \in C} H(c, w)$$

DEFINITION:

A code C over alphabet q (q is a power of prime)

is linear if two conditions hold:

I. $\forall x, y \in C \quad x + y \in C$

I. $\forall x, y \in C \quad x+y \in C$

$$x = (x_0, \dots, x_{n-1})$$

$$y = (y_0, \dots, y_{n-1})$$

$$x+y = (x_0+y_0, x_1+y_1, \dots, x_{n-1}+y_{n-1})$$

$$(k \cdot c_0, k \cdot c_1, \dots, k c_{n-1})$$

II. $\forall k \in [0, \dots, q-1] \; \forall c \in C \quad k \cdot c \in C \quad \mathbb{N} \; \mathbb{R} \; \mathbb{C}$

$(+, \cdot)$ are both operations in $\mathbb{F}_q$ (mod q if q is a prime)

$\boxed{\text{Ex 2.1}}$

10100

$C = \{00000, 00110, 10010, 10001, 00101, 10100, 00011, 10111\}$ ← 3 dimensional subspace of $\{0,1\}^n$

10100

Decide whether C is linear.

II. ✓

I.

Code C is a subspace of $[\{0,1\}^n, +, \cdot]$

n-dimensional space contains 2^n vectors

What is the dimension of C?

How large is k-dimensional subspace? 2^k (q^k for alphabet of size q)

for linear codes instead of (n, M, d) we for linear codes instead of (n, M, d) we often write (n, k, d)

k size of code subspace.

C can be characterized by k linearly independent codewords, called a basis $= \{b_0, \dots, b_{k-1}\}$

$\forall c: \quad c = a_0 b_0 + a_1 b_1 + \dots + a_{k-1} b_{k-1}$

$a_i \in \{0, \dots, q-1\}$

$C = \{00000, 00110, 10010, \underline{10001}, 00101, 10100, 00011, 10111\}$

$b_0 = 00110$
$b_1 = 10010$
$b_2 = 10001$

10100

$0 \cdot b_0 + 0 \cdot b_1 + 0 \cdot b_2 = (00000)$

$b_0 + b_1 + b_2 = 00101$

ADVANTAGE I. How to calculate minimum distance d?

$$\boxed{H(c_1, c_2)} = H(c_1 + w, c_2 + w)$$

$$= H(c_1 + c_1, c_2 + c_1)$$

$$= H(\vec{0}, c_2 + c_1)$$

$$c_2 + c_1 \in C$$

FIND the codeword of the smallest weight (number of non-zero entries)

$O(n)$

ENCODING

Generating matrix $G = \begin{bmatrix} b_0 \\ \vdots \\ b_k \end{bmatrix}$ of code C.

Since $M = 2^k$ we can associate each message with $m_i \in \{0,1\}^k$

to encode message m calculate

$$C = m \cdot G$$

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

$m_1 = 001$

$m_5 = 101$

$$c_1 = (001) \cdot G = (\underbrace{0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1}_{=1},\ 0,\ 0,\ 0,\ 1)$$

$$= 10001$$

$$c_5 = (101) \cdot G = (10111)$$

WE DO NOT NEED ENCODING TABLE! STORING G is ENOUGH

NORMAL FORM OF G

$$G = (\mathbb{I}_k \mid A)$$

$k \times k$ identity matrix

$k \times (n-k)$ matrix (checksum matrix)

Algorithm to find normal form of G:

1.) start with an arbitrary G

1.) Start with an arbitrary G

2.) Do following operations until normal form is found:

a.) permutation of rows

b.) multiplication of a row by nonzero scalar

c.) addition of rows

$\mapsto$ change basis

d.) multiplication of columns by non-zero scalar

e.) permutation of columns

$\mapsto$ do change the code for an equivalent one

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

$$= \begin{pmatrix} 1&1&0&0&0 \\ 0&1&0&0&1 \\ 0&0&1&0&1 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1 \\ 0&1&0&0&1 \\ 0&0&1&0&1 \end{pmatrix} = (\mathbb{I}_3 \mid A)$$

Codes with G in normal form are called systemic

$$(a\ b\ c) \cdot G = \underbrace{a\ b\ c}_{\text{data part}}\ \underbrace{0\ (a+b+c)}_{\text{Checksum}}$$

DECODING

Standard array decoding

$\text{Coset } u = \{ u + c \mid c \in C \}$

$\forall\, u, v \in \{0,1\}^n$ coset u and coset v are either identical or disjoint.

Coset leader is an element of a coset with the smallest weight.

$\boxed{\text{Ex 2.7}}$ $C = \{00000, 10110, 01011, 11101\}$

u	$C+u$			
00000	00000	10110	01011	11101
00001	00001	10111	01010	11100
00010	00010	10100	01001	11111
00100	00100	10010	01111	11001
01000	01000	11110	00011	10101
10000	10000	00110	11011	01101
00011	00011	10101	01000	11110
11110	11110	01000	10101	00011
10101	10101	00011	11110	01000
11000	11000	01110	10011	00101
01100	01100	11010	00111	10001

Decoding procedure:

1.) obtain w

2.) Find w in standard array

3.) Call coset leader of a coset w belongs to l_w.

4.) decode w as $\underline{\underline{w + l_w}}$

Example

$W = 11110$ in array $l_w = 01000$

So I decode as $\underline{10110}$

SYNDROME DECODING

Dual CODE $C^\perp$ of C

Scalar product

$$\vec{x} \cdot \vec{y} = (x_0 \cdot y_0 + x_1 \cdot y_1 + \dots + x_{n-1} \cdot y_{n-1})$$

$\vec{x}$ and $\vec{y}$ are perpendicular

if $\vec{x} \cdot \vec{y} = 0$

$$C^\perp = \{ w \mid w \in \{0,1\}^n : w \circ c = 0, \forall c \in C \}$$

if dimension of C is k

then dimension of $C^\perp$ is $n-k$

$$G = (I_k \mid A)$$

$$G = (I_k | A)$$

$$H = (-A^T | I_{n-k}) \rightarrow \text{Generator matrix of } C^\perp$$

Example

$$G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right) \quad A^T = \begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$$

$\rightarrow A$

$$H = \underbrace{\left(\begin{array}{ccc|cc} 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right)}_{(-A^T \,|\, I_2)}$$

$$\forall c \in C$$

$$c \cdot H^T = \overbrace{0\,0\,0}^{n-k}$$

$$(0\,1\,0\,0\,1) \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \left(\underbrace{[(0\,1\,0\,0\,1) \cdot (0\,0\,0\,1\,0)]}_{0}, \underbrace{[(0\,1\,0\,0\,1) \cdot (1\,1\,1\,0\,1)]}_{0} \right)$$

error in the channel is characterized by an error vector $e \in \{0,1\}^n$

$$\underline{(c+e)} \cdot \underline{H}^T = \underbrace{c \cdot H^T}_{= 0} + \underbrace{e H^T}_{\text{syndrome}}$$

There is a one to one correspondence between

There is a one to one correspondence between errors and cosets [Cosets are $\{c+e\}$]

Ex 2.8

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

b

$A^T \quad I \quad A$

$$= \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

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

e	$e \cdot H^T$	
0000000	000	
0000001	001	
0000010	100	
000$\boxed{1}$00	011	
⋮		
1000000	101	

$w \cdot H^T$ 011

Hamming codes

$(7,4,3)$- hamming

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

$$H^T = \begin{pmatrix} 001 \\ 010 \\ 011 \\ 100 \\ 101 \end{pmatrix} \begin{array}{l} \leftarrow \text{'1'} \\ \leftarrow \text{'2'} \\ \leftarrow \text{'3'} \\ \vdots \\ \end{array}$$

$$\begin{array}{ccccccc} (1 & 0 & 1 & 0 & 1 & 0 & 1) \\ \uparrow & \uparrow & \uparrow & & & & \uparrow \\ '1' & '2' & '3' & & & & '7' \end{array} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{array}{l} \vdots \\ \\ \\ \leftarrow '7' \end{array}$$

for error vector with '1' in k-th position

syndrome is 'k'.

Example:

$$(0010000) \cdot H^T = (011) =$$