Tutorial 2 ENG

22 September 2021 13:59

LINEAR CODES

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

number of codewords

(n, M, d)

length of codewords

minimum distance of codewords

I Parameters

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

II ENCODING

$m_0 \rightarrow c_0$

$m_1 \rightarrow c_1$

$\vdots$

$m_{M-1} \rightarrow c_{M-1}$

III DECODING

Upon receiving w, you need to find $c \in C$ with minimum Hamming distance $\min_{c \in C} H(w,c)$

... distance $\min_{c \in C} \#(w,c)$

ALL OF THE TASKS ABOVE ARE MUCH MORE EFFICIENT WITH LINEAR CODES.

DEFINITION:

A code C over alphabet q (q is a power of a prime) is a linear code if two conditions hold:

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

$x = (x_0, x_1, \dots, x_{n-1})$

$y = (y_0, y_1, \dots, y_{n-1})$

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

II. $\forall k \in \{0, \dots, q-1\}, \forall c \quad k \cdot c = (k \cdot c_0, k \cdot c_1, \dots, k \cdot c_{n-1}) \in C$

$(+, \cdot)$ are both operations $\mathbb{F}_q$ ($\mod q$, for q prime)

Finite field of size q

EX 2.1

10100

10100

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

10100

10100

00110

$\binom{7}{2} = \frac{7!}{5!\,2} = \frac{7 \cdot 6}{2} = 21$

II. $\forall k \in \{0,1\}$

I.

I. + II. $\Rightarrow$ A Linear code C is a subspace of $(\{0,1\}^n, +, \cdot)$ (scalar product)

d_n

What is the dimension of C?

k-dimensional subspace of d_n has 2^k vectors (q^k for alphabet size q).

(n, M, d) is often expressed as (n, ξ, d).

$M = q^\xi$

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

$\forall c \in C \quad c = a_0 \cdot b_0 + a_1 \cdot b_1 + \dots + a_{\xi-1} b_{\xi-1}$ $\not\vdash$

$a_i \in \{0, \dots, q-1\}$ $\rightsquigarrow$ q^ξ linear combinations

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

$b_0 = 00110$

$b_1 = 10010$ $\rightarrow$ 10100

$b_2 = 10001$ $\rightarrow$ 00011

$\rightarrow$ 10111 $\rightarrow$ 00101

$0 \cdot b_0 + 0 \cdot b_1 + 0 \cdot b_2 = 00000$ → All zero codeword is in every linear code ✓

$(a_0 b_0 + a_1 b_1 + a_2 b_2) + (a_0' b_0 + a_1' b_1 + a_2' b_2)$ ∈

$(a_0 + a_0') b_0 + (a_1 + a_1') b_1 + (a_2 + a_2') b_2$

ADVANTAGE I.

$H(c_1, c_2) = H(c_1 + w, c_2 + w) \quad \forall w \in \{0, \dots, q-1\}^n$

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

$H(0, c_2 + c_1)$

$H(0, c)$ $\quad c \in C$

⇒ To find d find the smallest Hamming weight (number of 1's) among $c \in C$. $(O(M))$

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

Hence C is a $(5, 3, 2)$-code.

ENCODING

Generating matrix $G = \begin{bmatrix} b_0 \\ \vdots \\ b_{k-1} \end{bmatrix}$ $k \times n$ of code C

containing basis vectors as rows

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

To encode $m \in \{0,1\}^k$

$$C = m \cdot G$$

$$C = \{00000, 00110, 10010, 10001, 00101, 01000, 00011, 10111\}$$

$$G = \begin{pmatrix} 00110 \\ 10010 \\ 10001 \end{pmatrix} \sim$$

$m_1 = 001$ $\quad G = m_1 \cdot G = 001 \cdot G$

$= [0\cdot 0 + 0\cdot 1 + 1\cdot 1, 0001]$

$= 1$

list of $a_0 a_1 a_2$ in the linear combinations

$m_5 = 101$ $\quad m_5 \cdot G = 10111$

WE DO NOT NEED AN ENCODING TABLE. STORING G IS ENOUGH

NORMAL FORM OF G

$$G = (\mathbb{1}_k \mid A)$$

k × k identity matrix k × (n−k) matrix [check sum matrix]

Algorithm to find normal form of G:

1.) Start with arbitrary G

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

a.) permutation of rows
b.) multiplication of rows by a non-zero scalar → change the basis of the same code
c.) addition of rows

d.) multiplication of columns by non-zero scalar
e.) permutation of columns (P) → change linear code to an equivalent linear code

$$G = \begin{pmatrix} 0&0&1&1&0 \\ 1&0&0&1&0 \\ 1&0&0&0&1 \end{pmatrix} \simeq \begin{pmatrix} 1&0&0&1&0 \\ 0&0&1&1&0 \\ 0&0&1&0&1 \end{pmatrix} \simeq \begin{pmatrix} 1&0&0&1&0 \\ 0&0&0&1&1 \\ 0&0&1&0&1 \end{pmatrix} \simeq \begin{pmatrix} 1&1&0&0&0 \\ 0&1&0&\bullet&1 \\ 0&0&1&0&1 \end{pmatrix} G^{+}$$

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

Codes with G in normal form are called **systemic**.

$(abc) \cdot G' = \underbrace{abc}_{\text{checksum}} \circ (a+b+c)$

DECODING

Standard array decoding

Coset $u = \{u + c \mid c \in C\}$ $u \in \{0,1\}^5$

$\forall u, v \in \{0,1\}^7$ coset u and coset v are either identical or disjoint

Coset leader is a vector of a coset with the smallest weight

EX2.7 $C = \{00000, 10110, 01011, 11101\}$ $(5, 2, 3)$

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
11000	11000	01110	10011	00101
01100	01100	11010	00111	10001

24

Standard array

Decoding procedure

1.) receive w

2.) find w in standard array

3.) identify coset leader (lw) of w

4) decode as $w + lw$

$w = 11110 \Rightarrow lw = 01000$

decode us 10110

Syndrome decoding

Dual code $C^\perp$ of C

Scalar product

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

$\vec{x}$ and $\vec{v}$ are perpendicular if $\vec{x} \cdot \vec{y} = 0$

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

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

$G = (\mathbb{I}_k \mid A)$ → generator matrix of C

$H = (-A^T \mid \mathbb{I}_{n-k})$ → generator matrix of $C^\perp$

$\forall c \in C$

$c \cdot H^T = \overbrace{000}^{n-k} \longmapsto !$

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

$H = \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array} \right)$

$01001 \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \{ \overbrace{(01001) \cdot (00010)}^{\in C^\perp} , \overbrace{(01001) \cdot (11101)}^{\in C^\perp} \}$

$01001 \in C$

$= 0 \quad = 0$

error in the channel is characterized by an error vector

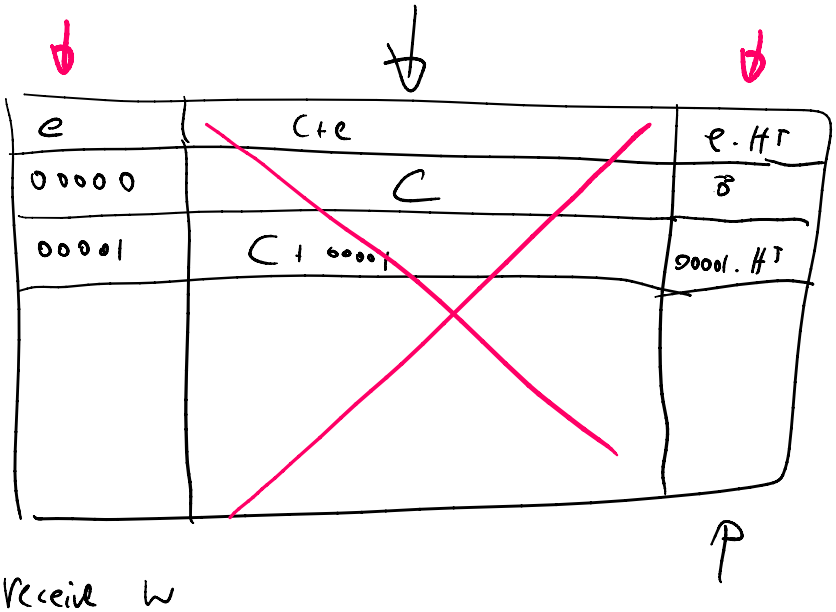
$e \in \{0,1\}^n$

$w = (c+e)$

$$w \cdot H^T = (c+e) \cdot H^T = c \cdot H^T + e \cdot H^T = 0 + eH^T$$

eH^T ↓ Syndrome

THERE is ONE to ONE correspondence between Syndromes and Cosets { Cosets are $(c+e)$ }



1.) Receive w

2.) Calculate the syndrome $w \cdot H^T = e \cdot H^T$

3.) find eH^T in (reduced) standard array

4.) find corresponding error e

5.) decode as $w+e$