4. Groups & Coding Theory

DATE:

Coding of Binary Information & Error Detection

In binary message we use only two symbols 0 & 1. It is called the set of alphabets & is denoted by $B = \{0, 1\}$. The basic unit of information is called a message.

A message is a finite sequence of characters from a finite alphabet.

From the set B of alphabets we construct the basic unit of information (a word) of length m (say) that contain m 1's & 0's.

e.g ① 11101 is the information called a word of length 5.

② 101101 ⟶ length 6.

The set $B = \{0, 1\}$ form a group under binary operation +. So B can be $(Z_2, +)$ with addition modulo 2.

+	0	1
0	0	1
1	1	0

$B^2 = B \times B$, $B^3 = B \times B \times B$ ....

$B^m = B \times B \times$ .... m times.

The set B^2 is a group under the binary operation $\oplus$ defined as

$(x_1, x_2) \oplus (y_1, y_2) = (x_1 \oplus y_1, x_2 + y_2)$

DATE:

e.g. $(1,0) \oplus (1,1) = (1+1, 0+1)$

$= (0,1)$

In general the above fact B^m

$$(x_1, x_2 \cdots x_m) \oplus (y_1, y_2 \cdots y_m) = (x_1+y_1, x_2+y_2 \cdots x_m+y_m)$$

So $(B^m, \oplus)$ is group with identity element denoted $\overline{0} = (0, 0 \cdots 0)$ m times & every element is its own inverse.

The set B^m has 2^m elements.

e.g.

B^2 has 4 element $\{00, 01, 10, 11\}$

B^3 has $2^3 = 8$ elements

$\{000, 010, 100, 001, 110, 011, 101, 111\}$

similarly B^4 has $2^4 = 16$ elements.

Weight of code word:- Let, $x \in B^n$.
The number of 1's in x is called the wt. of x. It is denoted by $|x|$

$|x|$ = no. of 1's in x.

e.g.

① $x = 110011100011 \in B^{12}$

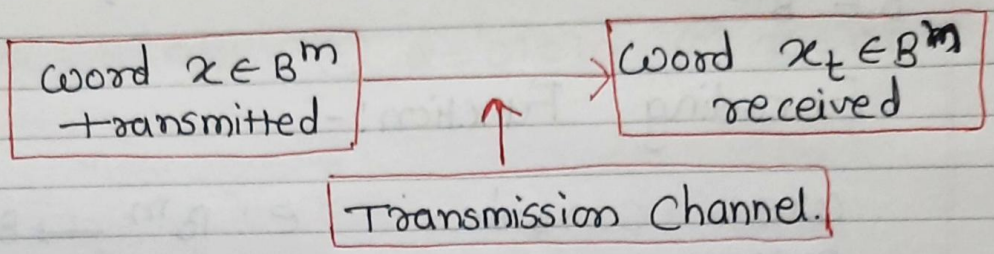
$|x| = 7$

② $x = 111$ then $|x| = 3$

③ $x = 101011$ then $|x| = 4$.

DATE:

* How to send or transmit word from one pt. to ~~anti~~ another point through a ~~transmission~~ channel?



when $x = x_t$ there is no error & both x & x_t belongs to B^m.

A word x transmitted is different than word received x_t i.e. $x \neq x_t$.

To fulfill this task we define an encoding function denoted by e. on the set of words that is B^m.

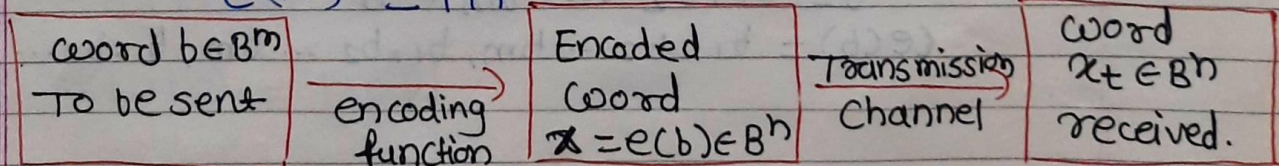
$$e : B^m \rightarrow B^n, \quad n > m$$

is one-one function $\forall$ $b \in B^m$ as $b \rightarrow e(b)$

The element $e(b) \in B^n$ is called a code word. The encoding function is known as (m, n) encoding function.

e.g. $e : B^2 \rightarrow B^3$ Here $m = 2$, $n = 3$.

$e(00) = 001$
$e(01) = 010$
$e(10) = 100$
$e(11) = 111$



DATE:

Code word:- A code word is an image of a word $b \in B^m$ under an encoding function e. It is denoted by $e(b)$ for any $b \in B^m$.

Encoding Function:-

We consider $e: B^m \longrightarrow B^n$

message length $= m$, code word length $= n$

$n - m$ = Parity bit added.

We can use these parity bits to detect error. or extra bit attached is known as a parity bit.

I] Encoding Function $(m, m+1)$

$e: B^m \longrightarrow B^{m+1}$, $b = m_{i-1}$

$e(b) =$

$b = b_1, b_2 \cdots b_m \in B^m$

$e(b) = b_1, b_2 \cdots b_m, b_{m+1}$

where $b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd.} \end{cases}$

II] Encoding Function $(m, 3m)$

$e: B^m \longrightarrow B^{3m}$

$b = b_1, b_2 \cdots b_m \in B^m$

$e(b) = b_1, b_2 \cdots b_m, b_1, b_2 \cdots b_m, b_1, b_2 \cdots b_m$

$|b| = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd} \end{cases}$ DATE:

Examples:-

$e: B^m \to B^{m+1}$

① write codewords for encoding fun^n $e: B^5 \to B^6$

ⓐ $x = 11100$ ⓑ $x = 01010$ ⓒ $x = 00110$

→

	Message (x)	Codeword (x_t)
ⓐ	$b = 11100$, $\|b\| = 3 = \text{odd}$	11100 **1**
ⓑ	$b = 01010$, $\|b\| = 2 = \text{even}$	01010 **0**
ⓒ	$b = 00110$, $\|b\| = 2 = \text{even}$.	00110 **0**

② Define encoding fun^n $e: B^3 \to B^4$ ($e: B^m \to B^{m+1}$) write the code words.

→ message length $= 3 = m$. $2^m = 2^3 = 8$

$\{000, 100, 010, 001, 101, 110, 011, 111\}$

$e(000) = 0000$ ← identity $e(011) = 011$**0**

$e(100) = 100$**1** $e(111) = 111$**1**

$e(010) = 010$**1**

$e(001) = 001$**1**

$e(101) = 101$**0**

$e(110) = 110$**0**

DATE:

H.W.

* Solve $e: B^2 \rightarrow B^3$ write all Codewords.

③ write all codewords for $m=3$ encoding fun^n $e: B^3 \rightarrow B^9$. $e: B^m \rightarrow B^{3m}$

Message (x)	Codeword (xt)
000	000000000
001	001001001
010	010010010
100	100100100
101	101101101
110	110110110
011	011011011
111	111111111

* Solve $e: B^2 \rightarrow B^6$ find all Codewords.

* Solve $e: B^3 \rightarrow B^4$ determine whether an error will be detected

ⓐ 0100 yes ⓑ 1100 no ⓒ 0010 yes ⓓ 1001 no

* Solve $e: B^6 \rightarrow B^7$ determine whether an error will be detected.

ⓐ 1101010 ⓑ 1010011 ⓒ 0011111 ⓓ 1001101

* Using (m, 3m) encoding fun^n. Determine whether an error will be detected.

① m=3 ⓐ 110111110 Here m=110 6th Position → Yes error will be detected

ⓑ 110010101 Here 110 1st & 3rd Position. → yes error will be detected.

DATE:

② $m = 4$

ⓐ 011010011111 ⓒ 010010110010

ⓑ 110110010110 ⓓ 001001111001

* Find the wt. of the following words.

ⓐ 1011 ⓑ 0110 ⓒ 1110 ⓓ 011101 ⓔ 11111

Hamming Distance:-

Let, $x, y \in B^m$ The Hamming distance $\delta(x,y)$ between x & y is the weight $|x \oplus y|$ of $x \oplus y$.

Hamming distance bet^n two codewords is denoted $\delta(x,y)$

e.g. ① $x = 1101$, $y = 0110$

$$x = 1101$$
$$y = 0110$$
$$x \oplus y = 1011 \qquad |x \oplus y| = 3$$

②
$$x = 11110100000$$
$$y = 11001011000$$
$$x \oplus y = 00111111100 \qquad |x \oplus y| = 6.$$

Note:- let $x, y, z \in B^m$ then.

1] $\delta(x,y) = \delta(y,x)$ 2] $\delta(x,y) \geq 0$ (non-negetivity Prop.)

3] $\delta(x,y) = 0$ iff $x = y$

4] $\delta(x,y) \leq \delta(x,z) + \delta(z,y)$ (Triangle inequality Prop)

DATE:

Ex. Consider a (2,5) encoding fun^n e defined

$e(00) = 00000 = x$
$e(10) = 00111 = y$
$e(01) = 01110 = z$
$e(11) = 11111 = \omega$.

$\delta(x,y) = 3$, $\delta(x,z) = 3$, $\delta(x,\omega) = 5$
$\delta(y,z) = 2$ $\delta(y,\omega) = 2$, $\delta(z,\omega) = 2$

*Solve :-

① $x = 1100010$ $y = 1010001$

② $x = 0100110$ $y = 0110010$

③ $x = 1101010$ $y = 0010011$

④ $x = 1101$ $y = 1000$.

Minimum distance of an encoding function :-
It is the minimum of the distance betⁿ all distinct pairs of code words
$\min\{\delta(e(x), e(y)) / x, y \in B^m\}$

Imp Theorem :- An (m,n) encoding fun^n $e : B^m \to B^n$ can detect K or ℓ less no. of errors iff it's minimum distance is at least K+1.

DATE:

Examples:-

1] Consider (2,6) encoding fun^n
$e(00) = 000000$, $e(10) = 101010$
$e(01) = 011110$, $e(11) = 110000$

i] Find min distance of e.

ii] How many error will e detect?

⊕	000000	101010	011110	110000
000000	000000	101010	011110	110000
101010	101010	000000	110100	011010
011110	011110	110100	000000	101110
110000	110000	011010	101110	000000

e = min. distance = 2 = $d(x,y)$
Now encoding fun^n $e: B^m \to B^n$ can detect k or less errors iff its min. distance is at least k+1.
Here since minimum distance is 2.
we have $2 \geq k+1$ or $k \leq 1$
so the code will detect ~~two~~ one or less no. of error.

Imp
Theorem:- Let, $e: B^m \to B^n$ be a group code The minimum distance of e is the minimum wt. of a non-zero code word.

2] Define $e: B^2 \to B^5$, (2,5) encoding fun^n.

$e(00) = 00000$, $e(10) = (10101)$
$e(01) = 01110$, $e(11) = 11011$.

1] find min. distance 2] How many error will 'e' detect?

→ The min. distance of $e = 3$ (By above thm)
(min. wt. of non-zero code word)

e will detect k or less no of errors. iff
it's min. distance is at least $k+1$.
Since min. distance $= e = 3$.

we have $3 \leq k+1$ or $k \leq 2$.

∴ So the code will detect two or less errors.

H.W.

① $e: B^3 \to B^6$, (3,6) encoding function. Find min. distance & errors will 'e' detect.

$e(000) = 000000$
$e(001) = 001100$
$e(010) = 010011$
$e(011) = 011111$
$e(100) = 100101$
$e(101) = 101001$
$e(110) = 110110$
$e(111) = 111010$

DATE:

Group code:- An (m,n) encoding function $e: B^m \to B^n$ is called a group code if

$$e(B^m) = \{e(b) / b \in B^m\} = \text{range}(e)$$

is a subgroup of B^n.

A non-empty subset H of a group G is a subgroup if a) Every element in H has inverse in H.
b) For any $x, y \in H$, $x \cdot y \in H$.

We know that in B^n every element is inverse itself. So, to prove that e is a group code it is enough to prove the set has identity element & $x \oplus y \in e(B^m)$

* Show that (2,6) encoding fun^n $e: B^2 \to B^6$ defined by

$e(00) = 000000$, $e(10) = 101010$

$e(01) = 011110$ $e(11) = 111000$

is a group code.

→ $e(00)$ is an identity element that belongs to $e(B^2)$

Now write operation table for $\oplus$ to ensure that $x, y \in e(B^2)$, $x \oplus y \in e(B^2)$

[we Prepare table in above example write again]

From the above table we see that the binary operation $\oplus$ is closed in $e(B^2)$ Hence $e(B^2)$ is subgroup of B^6. Hence e is a group code.

Generation of Group Code:-

Let, $B = \{0, 1\}$ is a Boolean algebra

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

$0+0=0$, $1+0=1$, $1+1=0$

$0 \cdot 0 = 0$ $1 \cdot 0 = 0$, $1 \cdot 1 = 1$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+1+0 & 0+1+0 \\ 0+1+0 & 0+1+1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Parity Check Matrix:-

Let, $m < n$, $r = n - m$ ↑ these are extra bits called Parity bits.

An $n \times r$ Boolean matrix H.

m = message length n = codeword length.

$$e(b) = [b_1\ b_2 \cdots b_m]\, H$$

$$= b\, H.$$

H is Parity check matrix of order $n \times r$

DATE:

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots 1 \end{bmatrix} \} \; r \text{ rows.}$$

Parity check equations are

$$x_1 = h_{11} b_1 + h_{21} b_2 + \cdots + h_{m1} b_m$$
$$x_2 = h_{12} b_1 + h_{22} b_2 + \cdots + h_{m2} b_m$$
$$\vdots$$
$$x_r = h_{1r} b_1 + h_{2r} b_2 + \cdots + h_{mr} b_m.$$

These Parity bits & Parity check equations are used to detect & correct error in the codewords.

* Find all codewords using (2,5) group code with $e: B^2 \rightarrow B^5$ & Parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \} \text{ identity matrix.}$$

→ $m = 2$, $n = 5$, $r = n - m = 5 - 2 = 3$ = Parity bits

Message $= 2^2 = 4 = \{00, 01, 10, 11\}$

DATE:

$e(b) = (b_1\ b_2\ x_1\ x_2\ x_3)$

$e(b) = [b_1\ b_2]\ H$

$$e(00) = [0\ 0]\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix} = [0\ 0\ 0]$$

$\therefore e(00) = 00000$

$$e(01) = [0\ 1]\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix} = [0\ 1\ 1]$$

$e(01) = 01011$

$$e(10) = [1\ 0]\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix} = [1\ 1\ 0]$$

$e(10) = 10110$

$$e(11) = [1\ 1]\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix} = [1\ 0\ 1]$$

$e(11) = 11101$

These are required codewords.

DATE:

* Generate codewords of group code $e_H : B^3 \to B^6$ with Parity check matrix / generator matrix.

$$H = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

→

Message length = m = 3
Codeword length = n = 6
$r = n - m = 6 - 3 = 3$ parity bits.

Message = {000, 100, 010, 001, 101, 011, 110, 111}

$e(b) = (b_1 b_2 b_3 \; x_1 x_2 x_3)$

$e(b) = [b_1 \; b_2 \; b_3] H$

$$e(000) = [0\,0\,0] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [0\;0\;0]$$

$e(000) = 000000$

$$e(001) = [0\,0\,1] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [1\;1\;1]$$

$e(001) = 001111$

$$e(100) = [1\,0\,0] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [1\;1\;0]$$

$e(100) = 100110$

$$e(010) = [0\ 1\ 0]\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [1\ 0\ 1]$$

$$e(010) = 010101$$

$$e(101) = [1\ 0\ 1]\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [0\ 0\ 1]$$

$$e(101) = 101001$$

$$e(011) = [0\ 1\ 1]\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [0\ 1\ 0]$$

$$e(011) = 011010$$

$$e(110) = [1\ 1\ 0]\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [0\ 1\ 1]$$

$$e(110) = 110011$$

$$e(111) = [1\ 1\ 1]\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [1\ 0\ 0]$$

$$e(111) = 111000$$

∴ These are required code words.

DATE:

Determine group code fun^n.

H.W.

1] $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $e_H : B^3 \rightarrow B^6$

2] $H = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right]$ $e_H : B^2 \rightarrow B^4$

3] $H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $e_H : B^2 \rightarrow B^5$