Group Code

Def: If $B = \{0,1\}$, then $B^n = \{(x_1, x_2, \cdots x_n) \mid x_i \in B\}$ is a group under the binary operation of addition modulo 2 (denoted by $\oplus$, say).

Elements of B^n are strings of length 'n'. (binary strings)

Prove that $(B^n, \oplus)$ is an abelian group.

Def: (Weight of a binary string:)

Let $x \in B^n$. Then the number of 1's in the string 'x', is called the weight of x and denoted by $|x|$ or $w(x)$

Eg: $x = 1010110$

So $|x| = 4$

Def: [Hamming distance] (of equal lengths)

If x and y are two binary strings, then the distance b/w x and y is the number of positions at which they differ. Denoted by $H(x,y)$ or $d(x,y)$.

$$d(x,y) = \left|\{i : x_i \neq y_i \text{ for } x, y \in B^n\}\right|$$

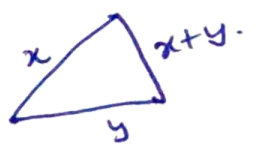
Eg: Let $x = 1011$, $y = 0101$

$d(x,y) = 3$.

In B^n, $d(x,y) = w(x \oplus y)$

$x \oplus y = 1110$ in the eg.

$\Rightarrow w(x \oplus y) = 3 = d(x,y)$.



$d(x,y) = d(0, y+x)$

$= w(y+x)$

0, if $y+x \in C$

$\Rightarrow d(C) = w(C)$

translation invariant.

Minimum distance

The minimum distance of a set $A \subseteq B^n$, is the minimum of the Hamming distances between all pairs of ~~the~~ set.

Eg: Let $C = \{ e_0 = (0000), e_1 = (0101), e_2 = (1010), e_3 = (1111) \}$

Then minimum distance of C, denoted as $d(C)$, is

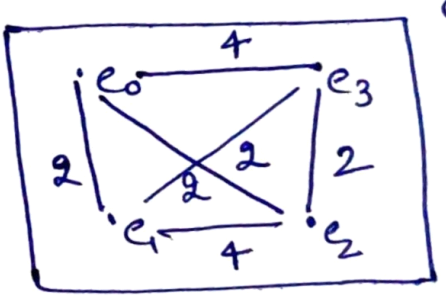
$$\min \{ d(e_i, e_j) : i \neq j \}.$$

ie $$\min \{ d(e_0,e_1), d(e_0,e_2), d(e_0,e_3), d(e_1,e_2), d(e_1,e_3), d(e_2,e_3) \}$$

ie $$\min \{ 2, 2, 4, 4, 2, 2 \} = 2.$$

$\therefore$ $$d(C) = 2.$$

C



Encoding function: A function $e: B^m \longrightarrow B^n$, which is one-one, is called (m,n)-encoding function, where $n > m$.

If $x = (x_1, x_2, \ldots x_m) \in B^m$ is the original word (message), then $e(x)$ is called the codeword.

Group Code:

An (m,n)-encoding function $e: B^m \longrightarrow B^n$ is called a group code if the range of e i.e. $e(B^m) = \{e(x) : x \in B^m\}$, is a subgroup of B^n.

Eg: Consider $(3,6)$-encoding function $e: B^3 \longrightarrow B^6$ defined by:

$x \in B^3$	$e(x) \in B^6$
000	000000
001	001100
010	010011
011	011111
100	100101
101	101001
110	110110
111	111010

Then e is a group code

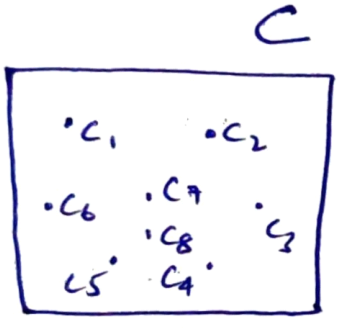
Eg: Let $e: B^2 \longrightarrow B^5$ given as:

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

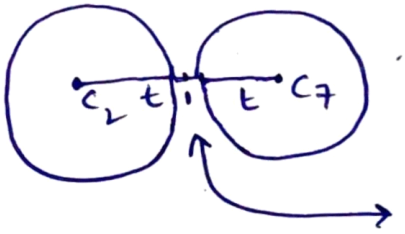
Show that e is a group code

Hint: Make the Composition table to prove the result.

Error detection and error Correction



(i)



(ii)

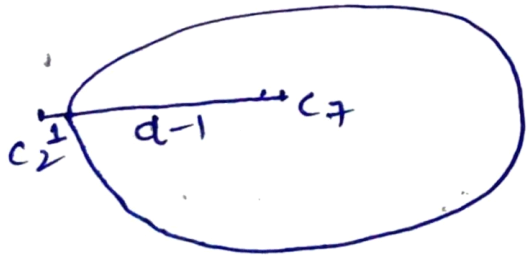
$2t+1$

$\Downarrow$

t - correction capacity

Here $2t+1 = \min$ dis

Say $\min_{i \neq j} \{ d(c_i, c_j) \} = d(c_2, c_7)$



(iii)

$\Rightarrow$ $d-1$ is detection capacity.

Here d = min distance.

Eg

Find the error detection capacity of the following codes:

(i) $e: B^2 \to B^6$:

$e(00) = 000000 = e_0$, $e(01) = 011110 = e_1$

$e(11) = 111000 = e_2$ $e(10) = 101010 = e_3$

Since $e(B^2) = \{e_0, e_1, e_2, e_3\} \subseteq B^6$ is not a subgroup of B^6. [$\because e_1 + e_2 \notin e(B^2)$]

$\therefore$ $w(C)$ may not be equal to $d(C)$ where $C = e(B^2)$.

Here $d(e_0, e_1) = 4$; $d(e_0, e_2) = 3$; $d(e_0, e_3) = 3$

$d(e_1, e_2) = w(e_1 + e_2) = w(100110) = 3$

$d(e_1, e_3) = w(e_1 + e_3) = w(110100) = 3$

$d(e_2, e_3) = w(e_2 + e_3) = w(010010) = 2$

$\therefore$ The minimum distance is 2 = d

$\therefore$ The error detection capacity is: $d - 1 = 1$.

Note that if $e(B^2)$ will be a subgroup of B^6 : in that case $w(e_i + e_j) = d(e_i, e_j)$ and $e_i + e_j \in e(B^2)$ [Closure prop]

$\Rightarrow$ $\min d(e_i, e_j) = w(e_k)$ for some $e_k \in e(B^2)$

$\therefore$ We can Calculate the weights of all codewords, and the Choose min weight to determine min distance.

$e: B^m \longrightarrow B^n$. Then a matrix G_1 of order $m \times n$ is called a generator matrix if

$$e(x) = xG_1 \quad \text{for } x \in B^m.$$

($e(x)$: $1 \times n$; x: $1 \times m$; G_1: $m \times n$; xG_1: $1 \times n$)

Standard form of generator matrix:

We choose a matrix G_1 of order $m \times n$ for $e: B^m \longrightarrow B^n$ as:

$$G_1 = [I_m \mid A]$$

where A is any matrix of order $m \times (n-m)$.

(G_1: $m \times n$; A: $m \times (n-m)$)

ie if $m = (x_1, x_2, \ldots x_m)$ is the message, then

$$e(m) = mG_1 = m[I_m \mid A]$$

$$= (x_1 \ldots x_m)[I_m \mid A]$$

$$= (x_1, x_2, \ldots x_m, a_1, a_2, \ldots a_{n-m})$$

$(x_1, x_2, \ldots x_m)$: message; $(a_1, a_2, \ldots a_{n-m})$: for some $a_1, a_2, \ldots a_{n-m}$.

Def: Parity check matrix:

A matrix H is called a parity check matrix for $e: B^m \longrightarrow B^n$ if $e(B^m)$ is the kernel of H^T.

ie $x \in e(B^m) \iff xH^T = 0$.

Two ways to define Code:

1) Using generator matrix:

if $x \in B^m$ is a message,
then xG is a Codeword
ie

$$C = \{ xG : \quad x \in B^m \}.$$

Code

2) Using parity check matrix:

if $x \in B^n$ is a word, then
$x \in B^n$ is a Codeword if $xH^T = 0$
ie

$$C = \{ x \in B^n : \quad xH^T = 0 \}$$

H
↓
$(n-m) \times n$

If $G = [I_m | A]$ is a standard form,
$m \times n$
then $H = [A^T | I_{n-m}]$ is the corresponding parity check matrix for the same Code,
G is generator matrix of.

X ——— X

Let $e: B^2 \to B^5$ is a code whose generator matrix is. $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

Then find the full code using both methods.

Sol: $B^2 = \{00, 01, 10, 11\}$

∴ Let C represents the code.

Then $C = \{xG : x \in B^2\}$

i.e

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

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

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

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

∴ $C = \{00000, 01011, 10111, 11100\}$. → (1)

Alternatively:

$C = \{x \in B^n : xH^T = 0\}$, Here $n = 5$

Let $x \in C$. Then $x = (x_1, x_2, x_3, x_4, x_5) \in B^5$

and $xH^T = 0$,

where $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 5}$

$n = 5$
$m = 2$
$n - m = 3$

$$\therefore \quad [x_1\ x_2\ x_3\ x_4\ x_5] \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 0$$

$$[x_1+x_3,\ x_1+x_2+x_4,\ x_1+x_2+x_5] = [0\ 0\ 0]$$

$\Rightarrow$

$$(*) \longleftarrow \begin{cases} x_1+x_3 = 0 \\ x_1+x_2+x_4 = 0 \\ x_1+x_2+x_5 = 0 \end{cases} \quad \begin{matrix} \text{No of Eqs} = 3 \\ \text{No of Var} = 5 \\ \text{No of Free var} = 5-3 \\ \qquad\qquad = 2 \end{matrix}$$

Choose x_1, x_2 as free variables.

$\therefore$ $(x_1, x_2, x_1, x_1+x_2, x_1+x_2)$ is sol for (*).

i.e. $(x_1, x_2, x_1, x_1+x_2, x_1+x_2)$ is a codeword for all $x_1, x_2 \in \{0,1\}$

i.e. $\{(0\ 0\ 0\ 0\ 0),$
$(0\ 1\ 0\ 1\ 1),$
$(1\ 0\ 1\ 1\ 1),$
$(1\ 1\ 1\ 0\ 0)\} = C$, same as (1).

Hence the result.

X ——————— X.

Parity check matrix decoding: [For one error detection and correction]

Let rows of transpose of the parity check matrix H are distinct and non-zero.

Suppose that the transmitted codeword 'w' was received with only one error.

Suppose error is there at the i^{th} position.

Denote the vector that has '1' at i^{th} position and '0' elsewhere by e_i.

Rewrite the received word = $w + e_i$

$$\therefore (w + e_i)H^T = wH^T + e_iH^T$$
$$= 0 + e_iH^T$$

↓

will give i^{th} row of H^T.

∴ Multiplication of received word with H^T will give i^{th} row of H^T if error is occured in the i^{th} position.

Example: Try by yourselves.

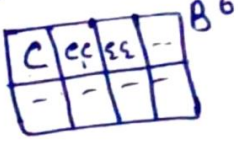
Coset decoding:

Consider a group-code: $e: B^3 \longrightarrow B^6$ as:

{ 000000, 100110, 010101, 001011, 110011, 101101, 011110, 111000 }

Make an array:

First row → $C \in B^6$.
Second row → $100000 + C$ (coset)
and so on



Coset leaders

000000	100110	010101	001011	110011	101101	011110	111000
100000	000110	110101	101011	010011	001101	111110	011000
010000	110110	000101	011011	100011	111101	001110	101000
001000	101110	011101	000011	111011	100101	010110	110000
000100	100010	010001	001111	110111	101001	011010	111100
000010	100100	010111	001001	110001	101111	011100	111010
000001	100111	010110	001010	110010	101100	011111	111001
100001	000111	110100	101010	010010	001100	111111	011001

Min weight

$W+C = V+C$; where V is coset leader of coset $W+C$
Coset leader has min weight.
$(2^6 = 64)$

If the word 101001 is received. This will be decoded as: 101101.

Coset decoding follows Nearest Neighbourhood decoding:

Pf: For any coset $V+C = W+C$
(V: coset leader; W: any element in that coset.)

$\Rightarrow W = V+C$: $C \leq C$
and W be treated as C. (why?)

for any other c': $d(c', w) = wt(c'-w) \geq wt(v)$ [$\because c'-w \in C$, $w+C = v+C$ and $v \in v+C$]
$\geq wt(w-c) = d(w,c)$

$\therefore d(w,c)$ is minimum.

Def: Syndrome:

For any word $x \in B^n$, we define syndrome of x as: $Syn(x) = xH^T$.

ie if x is a codeword $\Leftrightarrow$ $syn(x) = 0$

If $x \in w + C$ (for some coset)

$\Rightarrow x + C = w + C$

Also let v be coset leader of that coset

Then $x + C = v + C$

$\Rightarrow x - v \in C \Rightarrow x = v + c$ for some $c \in C$

$\therefore xH^T = (v+c)H^T = vH^T$

$\therefore \forall x$: $\boxed{syn(x) = Syn(v)}$ for some coset leader v.

$\therefore$ We decode the word 'x' (Received) as: $'x + v'$.

x: Received word.

v: error string

Let $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ be parity check matrix for a code.

(Example for coset/Syndrome decoding:)

v_0	00000	01011	10111	11100
v_1	10000	11011	00111	01100
v_2	01000	00011	11111	10100
v_3	00100	01111	10011	11000
v_4	00010	01001	10101	11110
v_5	00001	01010	10110	11101
v_6	10001	11010	00110	01101
	11000	10011	01111	00100
v_7	10010	11001	00101	01110

If by mistake $2^5 = 32$

Coset leaders = $\{v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$

Their Syndromes = $\{$ $\}$

v_4

$$[0\,0\,0\,1\,0] \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$$

If you receive $w = 11110$ as received word.

$$\Rightarrow [1\,1\,1\,1\,0]H = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} = \text{Syn}(v_4)$$

$\therefore$ 11110 lies in a coset whose coset leader is $v_4 = (00010)$.

$\therefore$ Correct Codeword is: $w + v = 11100$