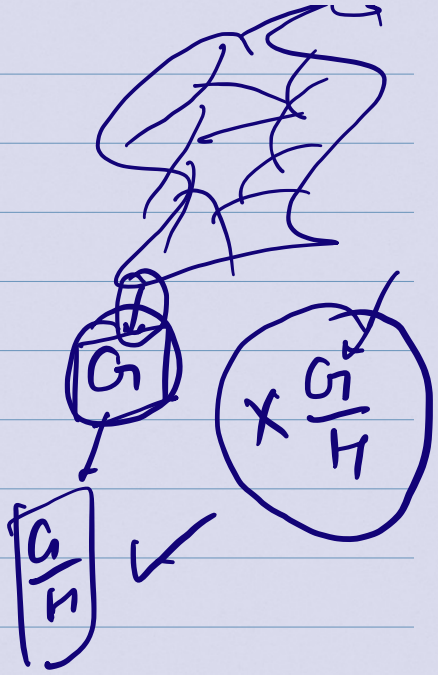
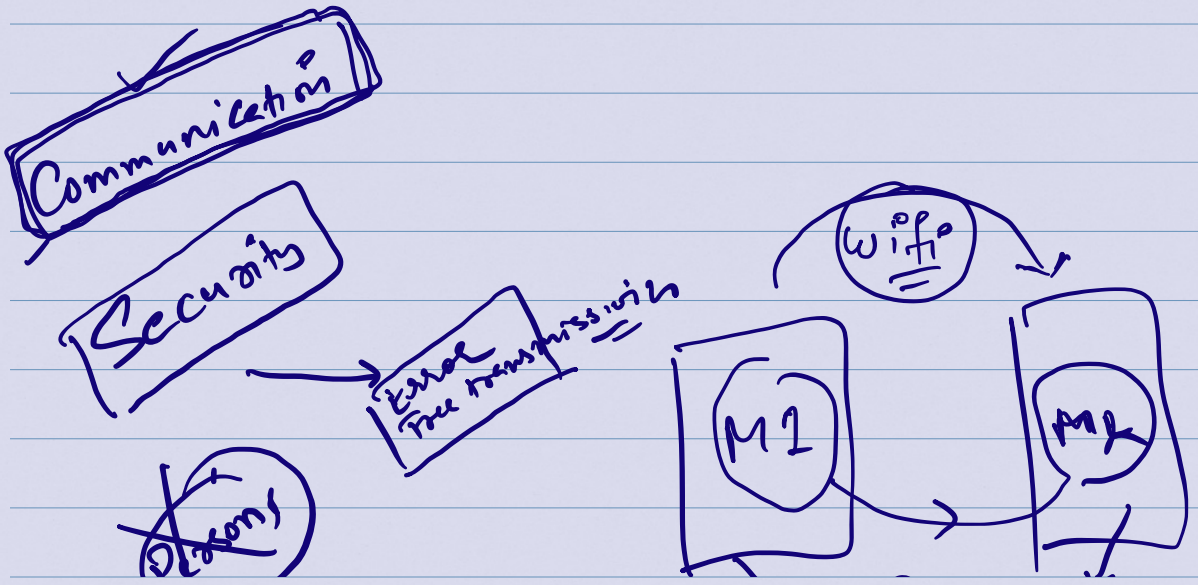
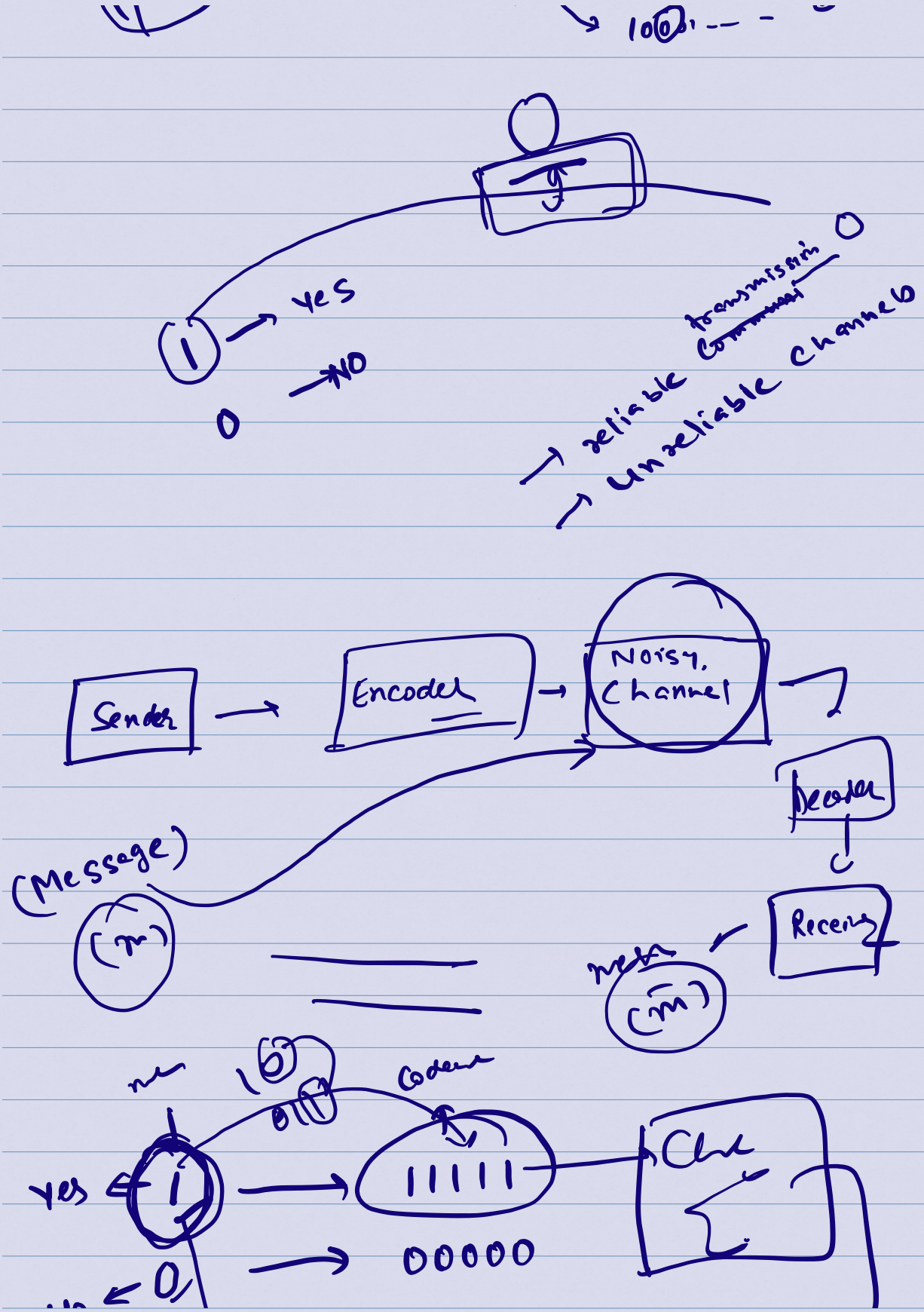


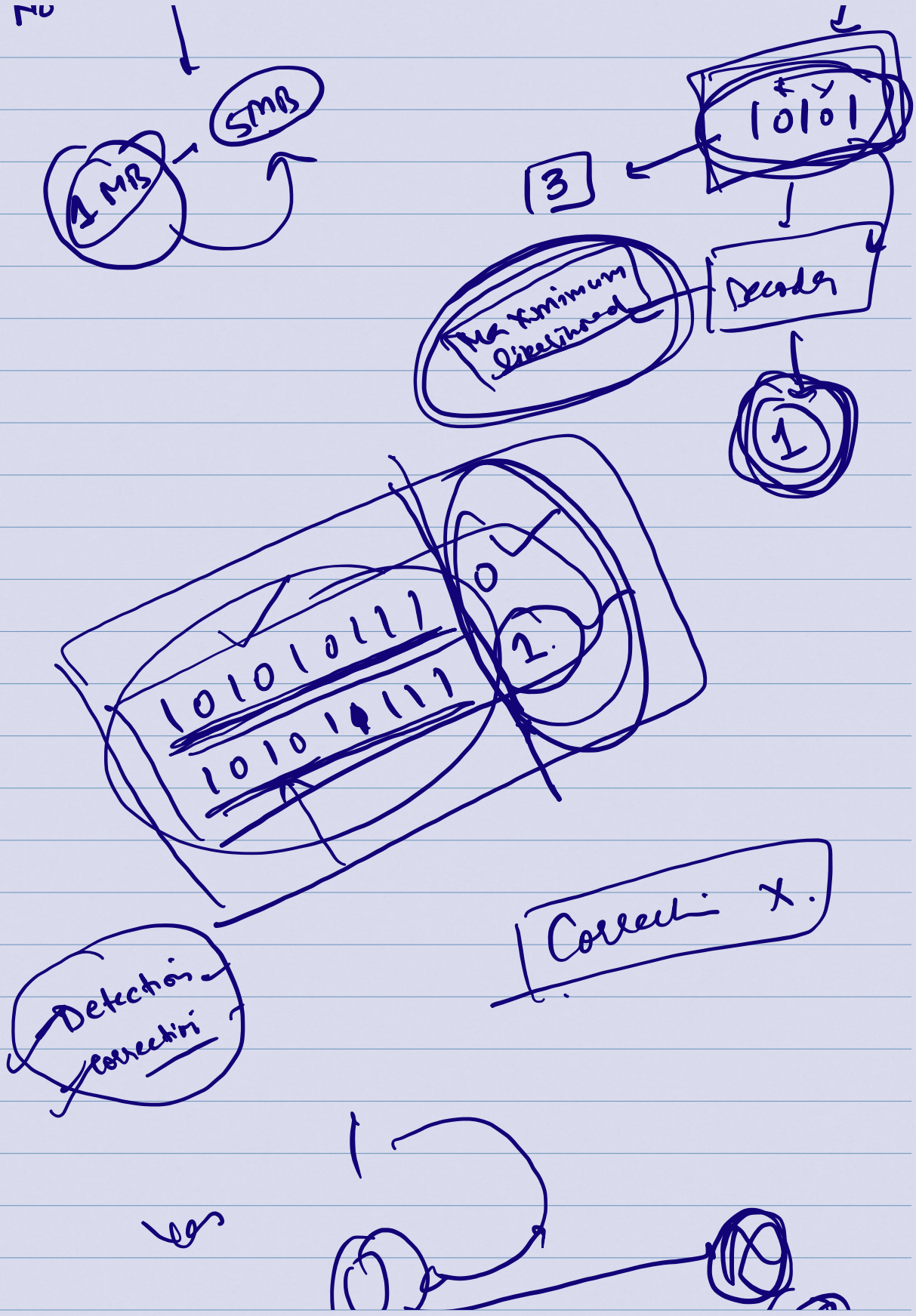
Error Correction

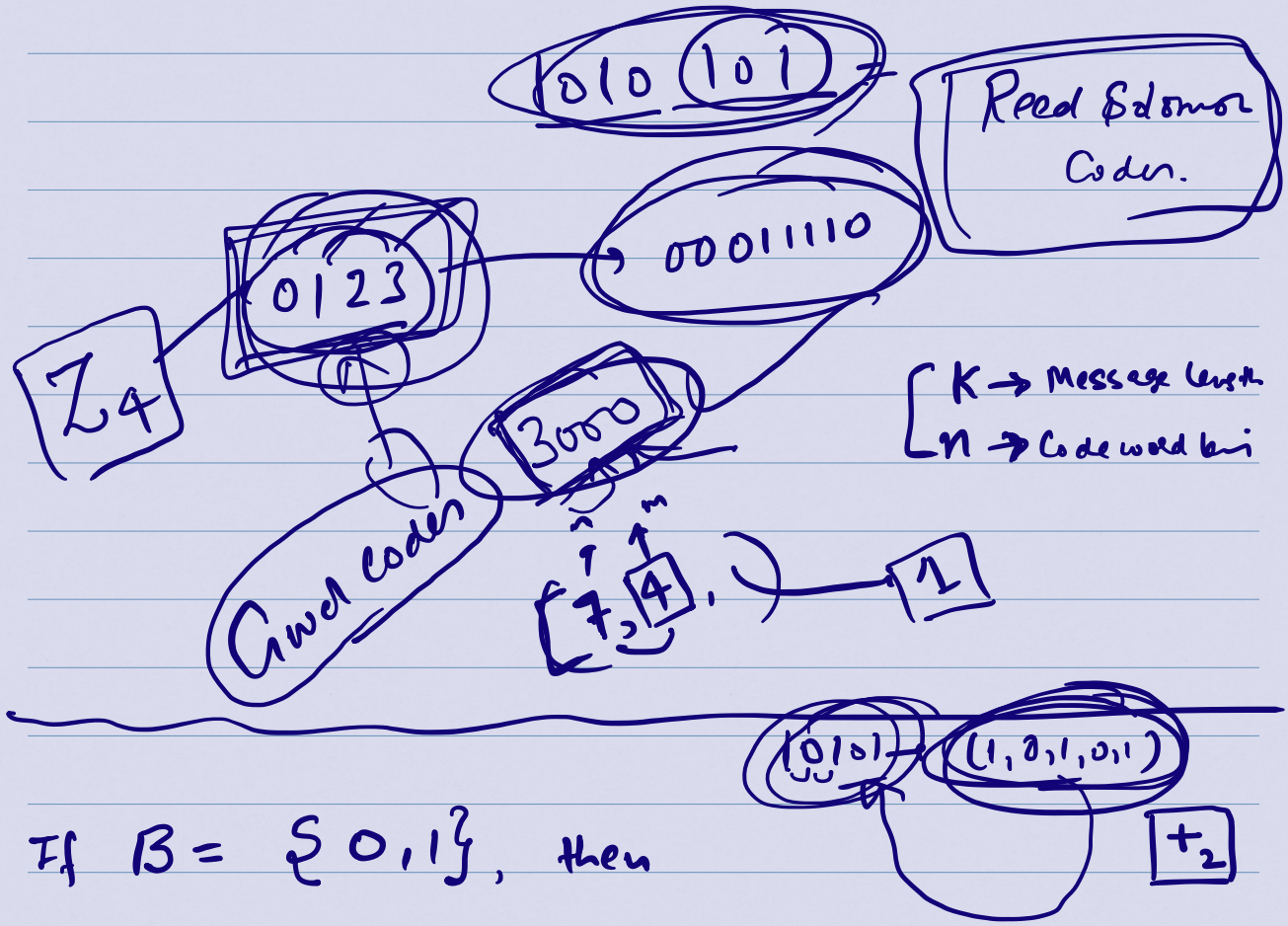
OR

Error Correcting Codes.




yes
NO
transmission
reliable
unreliable channel
Sender
Encoder
Noisy Channel
Decoder
(Message)
Receiv
Code
yes
00000
Che


1 MB
SMB
3
10101
Maximum likelihood
Decoder
1
0
2.
10101011
10101111
Detection
Correction
Correct X.



If $B = \{0, 1\}$, then

$$B^n = \{ x_1 x_2 \cdots x_n \mid x_i \in B : i = 1, \cdots n. \}$$

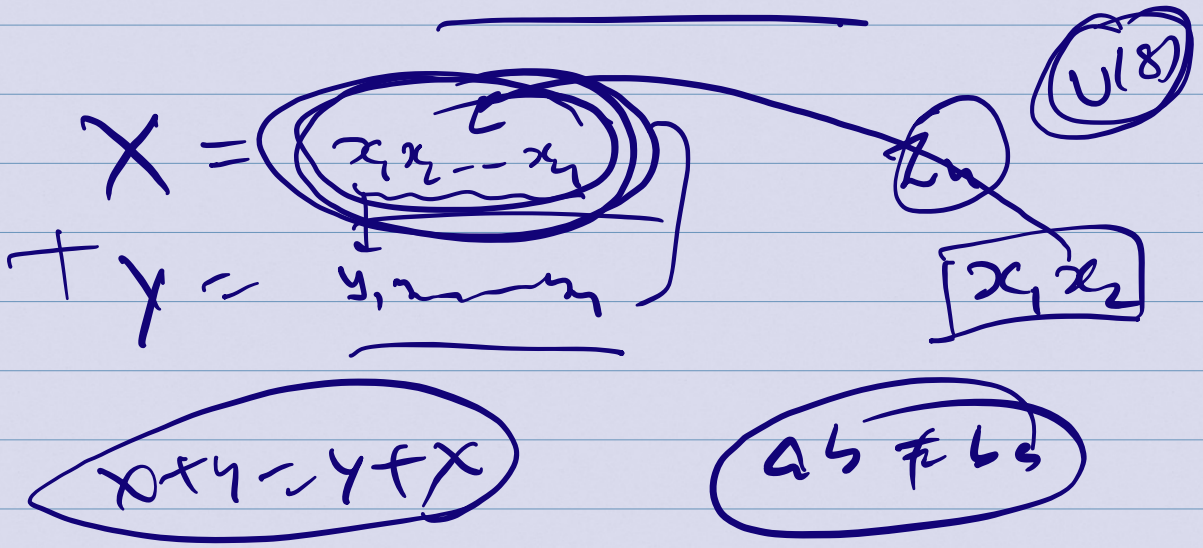
Z_4
$+_4$

is a group under the binary operation of addition modulo 2 (denoted by $\oplus$)

$\vec{a} \cdot \vec{b} = |a||b| \cos\theta$

Prove that $(B^n, \oplus)$ is

an abelian group.



$A \times B = \{(a,b) :$

$B = \{0,1\}$

Group code

$\oplus \rightarrow +_2$

$(B^n, \oplus)$

abelian group

Binary string of length n.

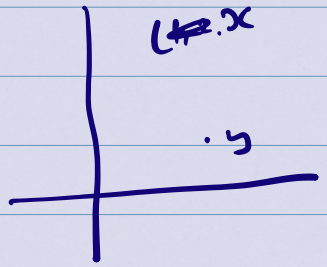
Def: [Weight of a binary string]

Let $x \in B^n$. Then the no of 1's in the string 'x' is called the weight of x and denoted by $w(x)$, or $|x|$.

eg: $x = 01101$ $\quad n = 6$

$\Rightarrow |x|$ or $w(x) = 4$

$w(x) = d(0, x)$



Def: [Distance]

If $x, y \in B^n$ are two binary strings then distance b/w x and y is the no of positions at which they differ. denoted as $d(x, y)$.

$$d(x, y) = \left| \{ i : x_i \neq y_i \text{ for } x, y \in B^n, \; i = 1, 2, \ldots, n \} \right|$$

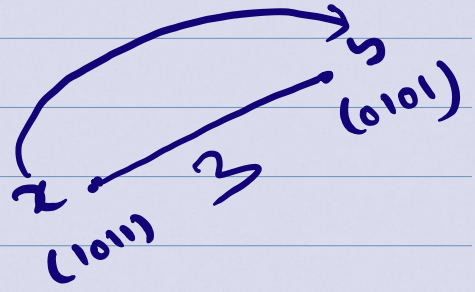
$x = 1011$

$y = 0101$

$d(x,y) = 3$

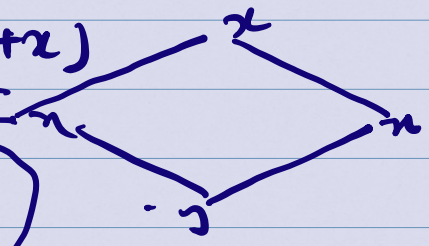
$x + y = 1110$

$w(x+y) = 3.$

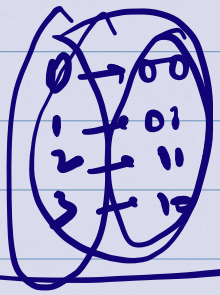


$$d(x,y) = d(x+x, y+x)$$

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



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



$(x_1 x_2 - x_n), (y_1 \cdots y_n)$

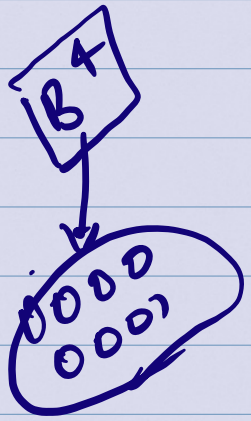
$(x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$

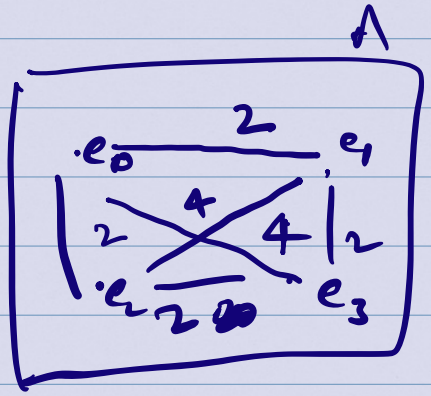
Minimum Distance:

The minimum distance of a set $A \subseteq B^n$ is the minimum of all the distances b/w all pairs.

$$d[A] = \min_{i \neq j} \{ d(x_i, x_j) : i \neq j \}$$

let $A = \{ 0000 = e_0, 0101 = e_1, 1010 = e_2, 1111 = e_3 \} \subseteq B^4$

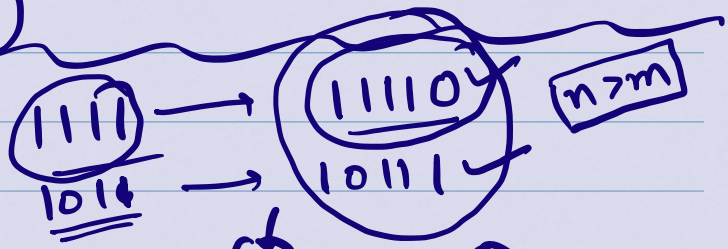




$d(A) = \min\{2,2,2,2,4,4\}$

$= 2$

Encoding function:

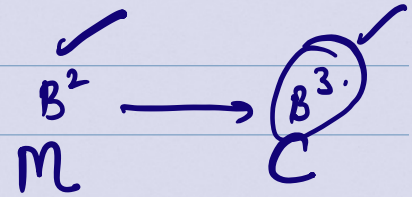


A function $e : B^m \longrightarrow B^n$

Which is a 1-1 function is called (m,n)-encoding function

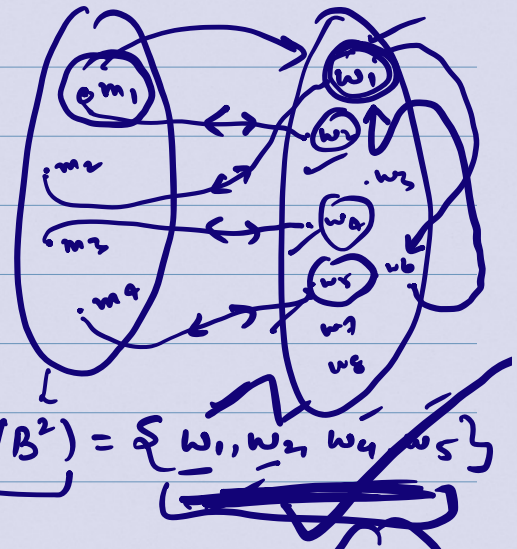
$\Rightarrow$ If x is the original msg

" $(x_1 x_2 \ldots x_m) \in B^m$



$\Rightarrow$ $e(x)$ is called the codeword.

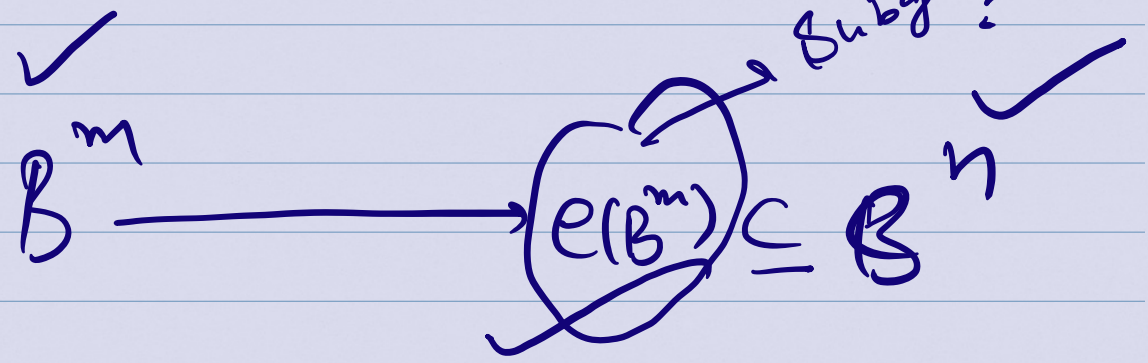
Code := (Set) Collection of codewords.



$e(B^2) = \{w_1, w_2, w_4, w_5\}$

Group Code:

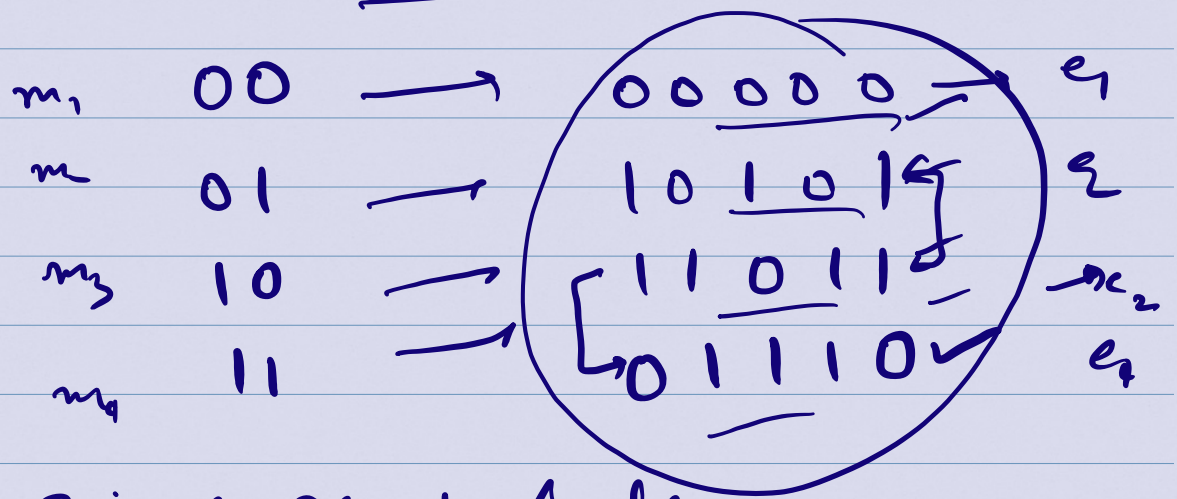
An (m,n)-encoding function $e: B^m \to B^n$ is called a group code if the range of e, i.e $e(B^m) = \{e(x) : x \in B^m\}$ is a subgroup of B^n



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

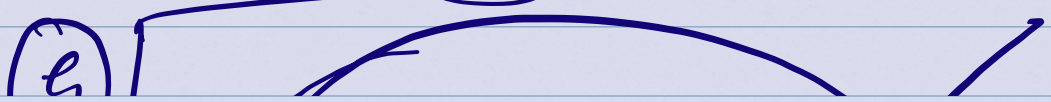
~~This is a group code~~

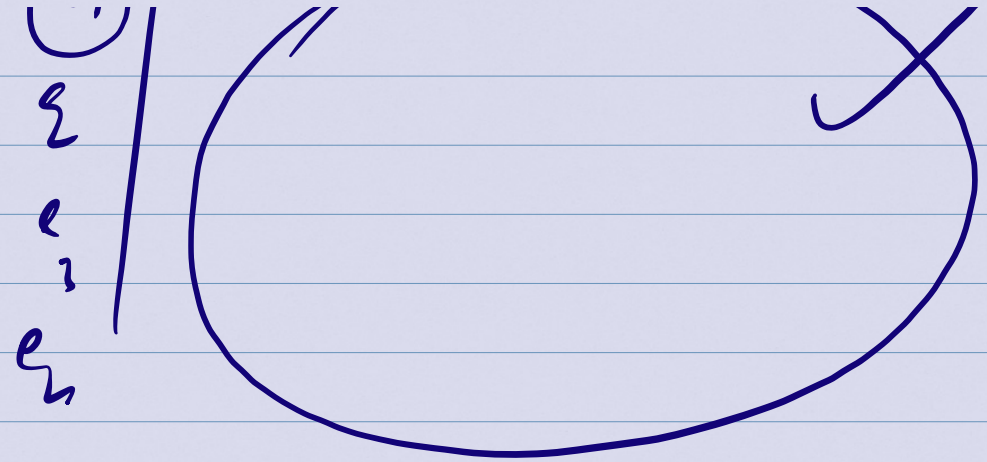
$e: B^2 \to B^5$



e is a group code

e_1 e_2 e_3 e_4





Subgroup Condition

$x, y \in H$

$\Rightarrow xy \in H$

X

$C = \{e_0, e_1, e_2, e_3\}$

$e: B^m \to B^n$

$m=2$

$m=5$

$m_0 \; 00 \to 00000_{e_0}$

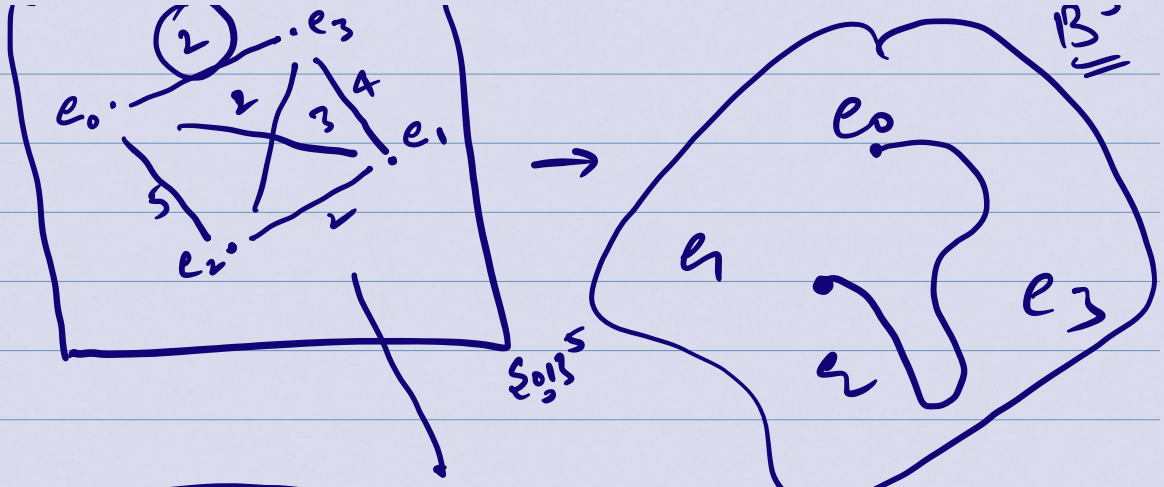
$m_1 \; 10 \to 10101_{e_1}$

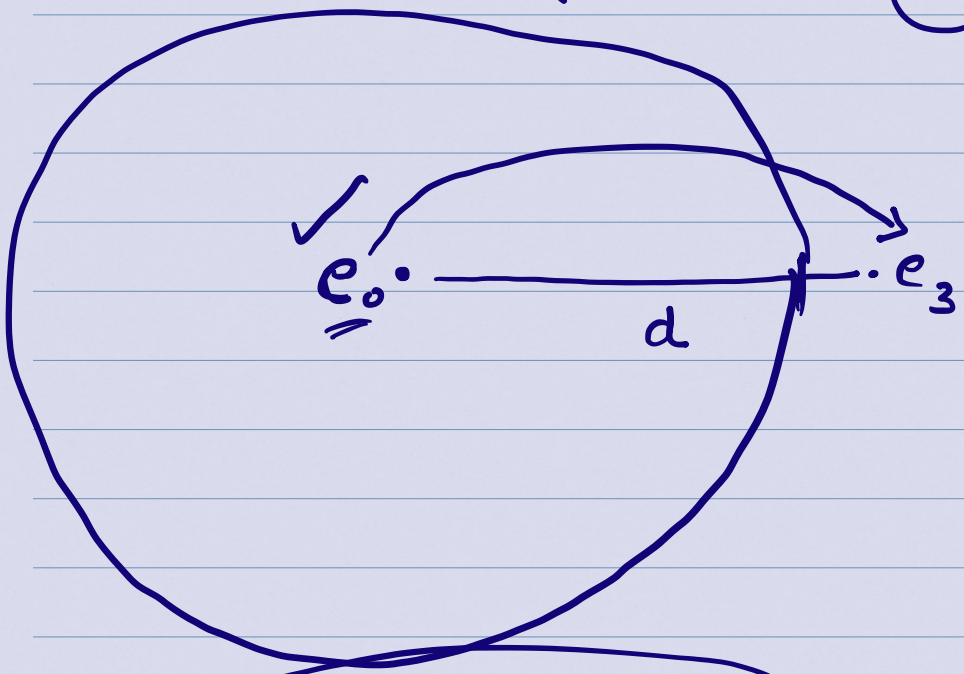
$m_2 \; 11 \to 11011_{e_2}$

$m_3 \; 01 \to 01110_{e_3}$

$e(m_0) = e_0$

$e(m_1) = e_1$

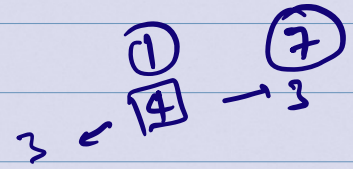


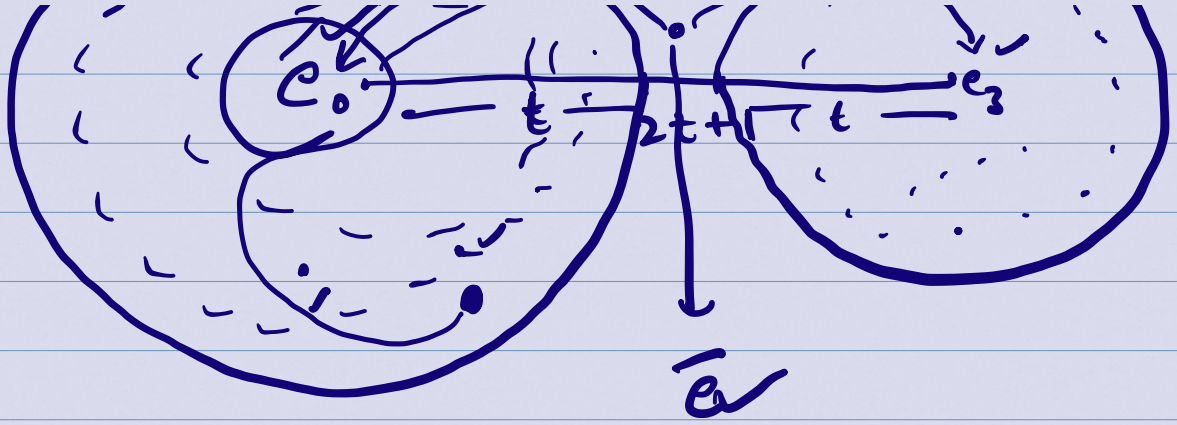


min distance = d

⇒ detect in capacity = d-1

e_4





Min distance = $2t+1$

$\Rightarrow$ Error Correction Capacity = t

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

$x, y \in C$

$00 \rightarrow 00000_{c_0}$
$10 \rightarrow 10101_{c_1}$
$11 \rightarrow 11011_{c_2}$
$01 \rightarrow 01110_{c_3}$

$d(c_0,c_1) = 3$
$d(c_0,c_2) = 4$
$d(c_0,c_3) = 3$
$d(c_1,c_2) = 3$
$d(c_2,c_3) = 3$

3

$w(c_0) = 0$
$w(c_1) = 3$
$w(c_2) = 4$
$w(c_3) = 3$

3

Find the error detection capacity of the Code.

$$e: B^2 \longrightarrow B^6$$

$$\begin{bmatrix} e(00) = 000000 = e_0 \\ e(01) = 011110 = e_1 \\ e(11) = 111000 = e_2 \\ e(10) = 101010 = e_3 \end{bmatrix} \quad \begin{matrix} w(e_0) = 0 \\ w(e_1) = 4 \\ w(e_2) = 3 \\ w(e_3) = 3. \end{matrix}$$

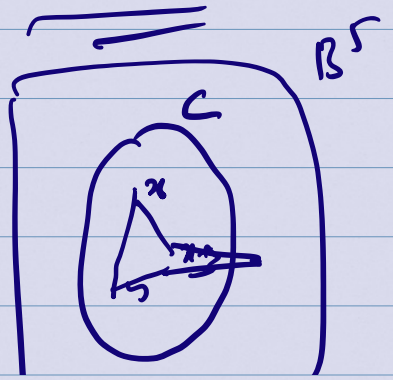
$$e_1 + e_2 = 100110 \notin C$$

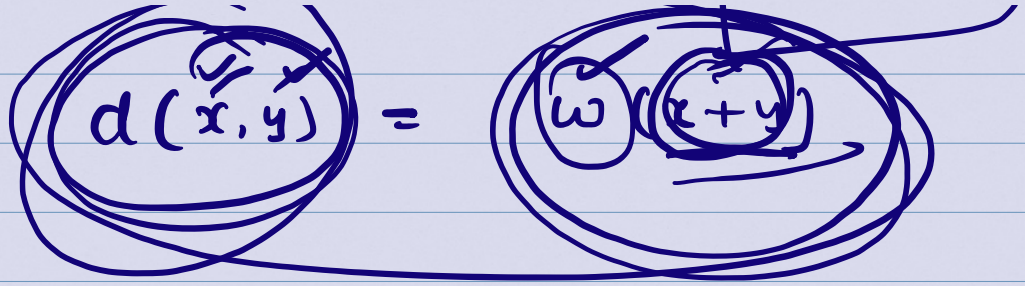
$$d(e_0, e_1) = 4 \;,\; d(e_0, e_2) = 3 \;,\; d(e_0, e_3) = 3$$

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

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

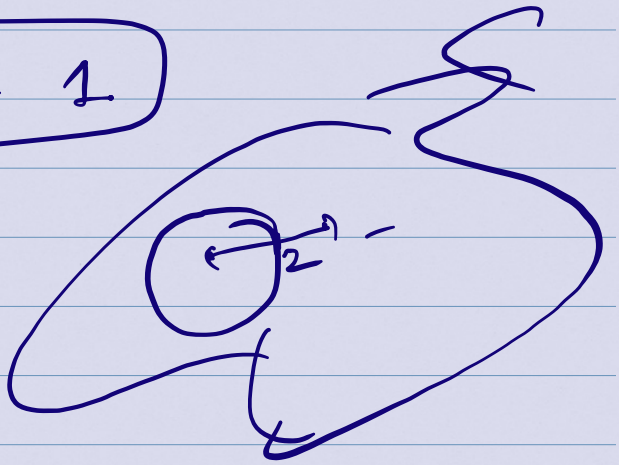
$$d(e_2, e_3) = w(e_2 + e_3) = w(010010) = 2$$





Min distance = 2

Detection Capacity = 1

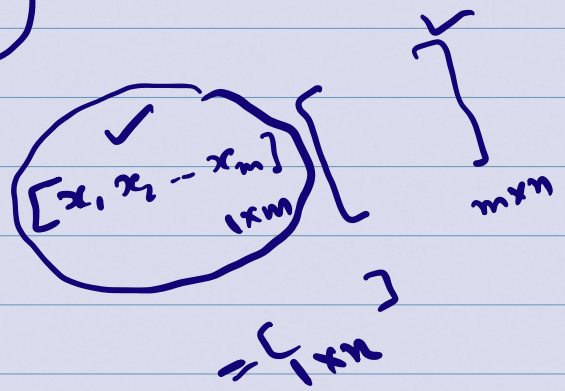


Generator matrix

Let $C : B^m \longrightarrow B^n$. Then a matrix G

of order $m \times n$ is called a generator matrix.

if $e(x) = xG$.



Standard form of generator matrix:

We choose the matrix G of order $m \times n$ for $e: B^m \to B^n$ $[e(x) = xG]$

$$G = [I_m \mid A]_{m \times n}$$

$I_m \to$ identity matrix of order m

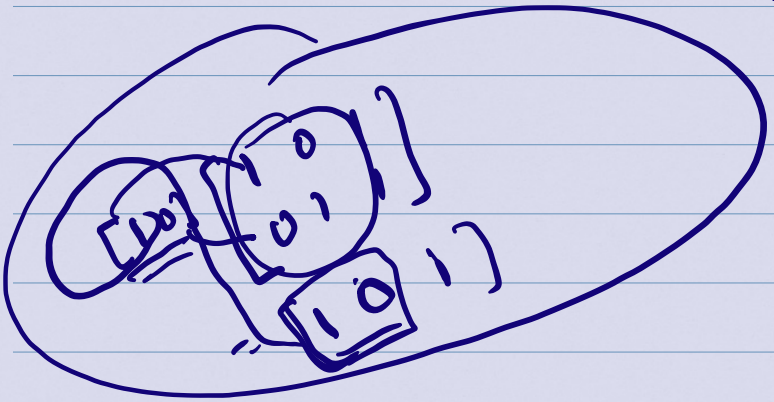
where A is any matrix of order $m \times (n-m)$

Now if $m = (x_1, x_2 \cdots x_m)$ is a message, then

$$(x_1 \cdots x_m)\, G = (x_1 \cdots x_m)[I_m \mid A]$$

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

Same as message



Def:

Parity Check matrix:

A matrix H is called the parity check matrix for $e: B^m \to B^n$ if

$e(B^m)$ is the Kernel of H^T.

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

Two ways are there to define Code

(G)x

① Using generator matrix :

$$C = \{ \underset{1\times n}{x} \underset{m\times n}{G} : \quad x \in B^m \}$$

② Using parity check matrix :

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

($H \to (n-m)\times n$)

Connection b/w G and H. (if given in standard form)

If $G = [I_m \mid A]$ ($I_m \to m\times m$, $A \to m\times(n-m)$)

$$H = [A^T \mid I_{n-m}]$$

Let $e: B^2 \to B^5$ is a code whose generator matrix is:

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

$$\left[\underbrace{0\ 1}_{I_2} \mid \underbrace{0\ 1\ 1}_{A}\right]$$

Then find the full code using both methods.

- $x \in B^2 = \{00, 01, 10, 11\}$

$C = xG$.