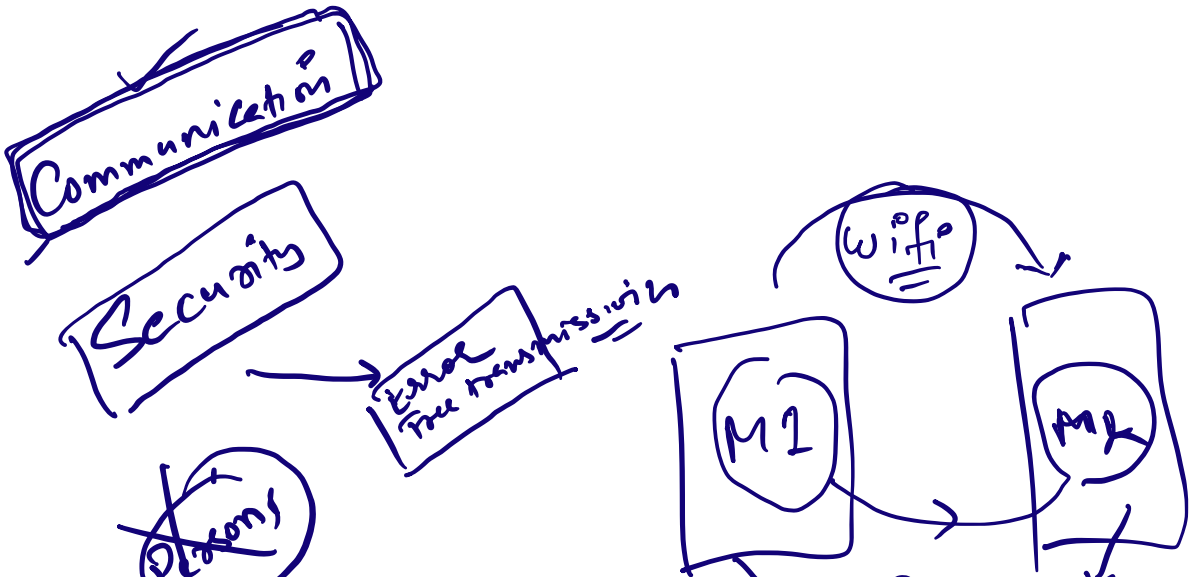
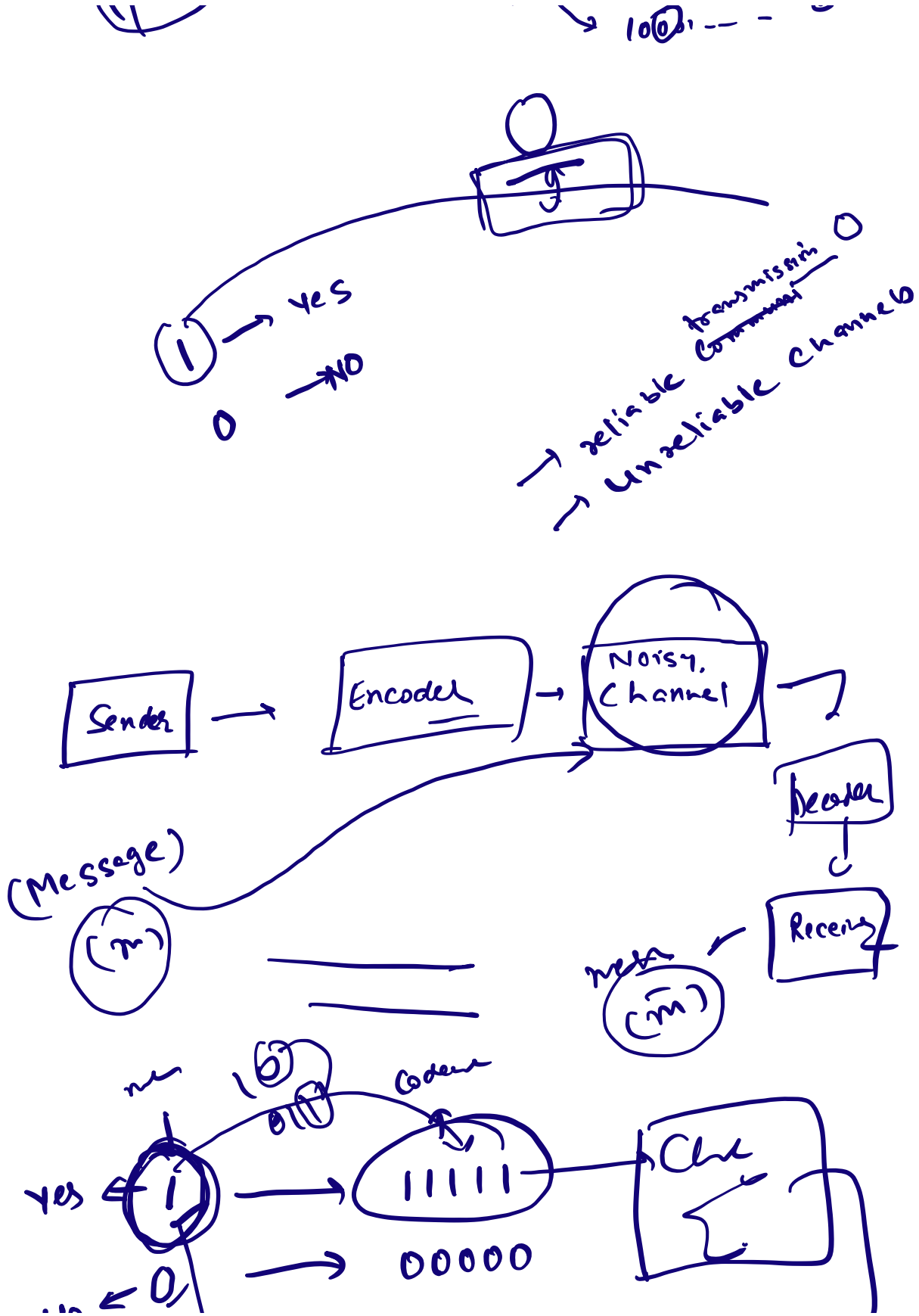
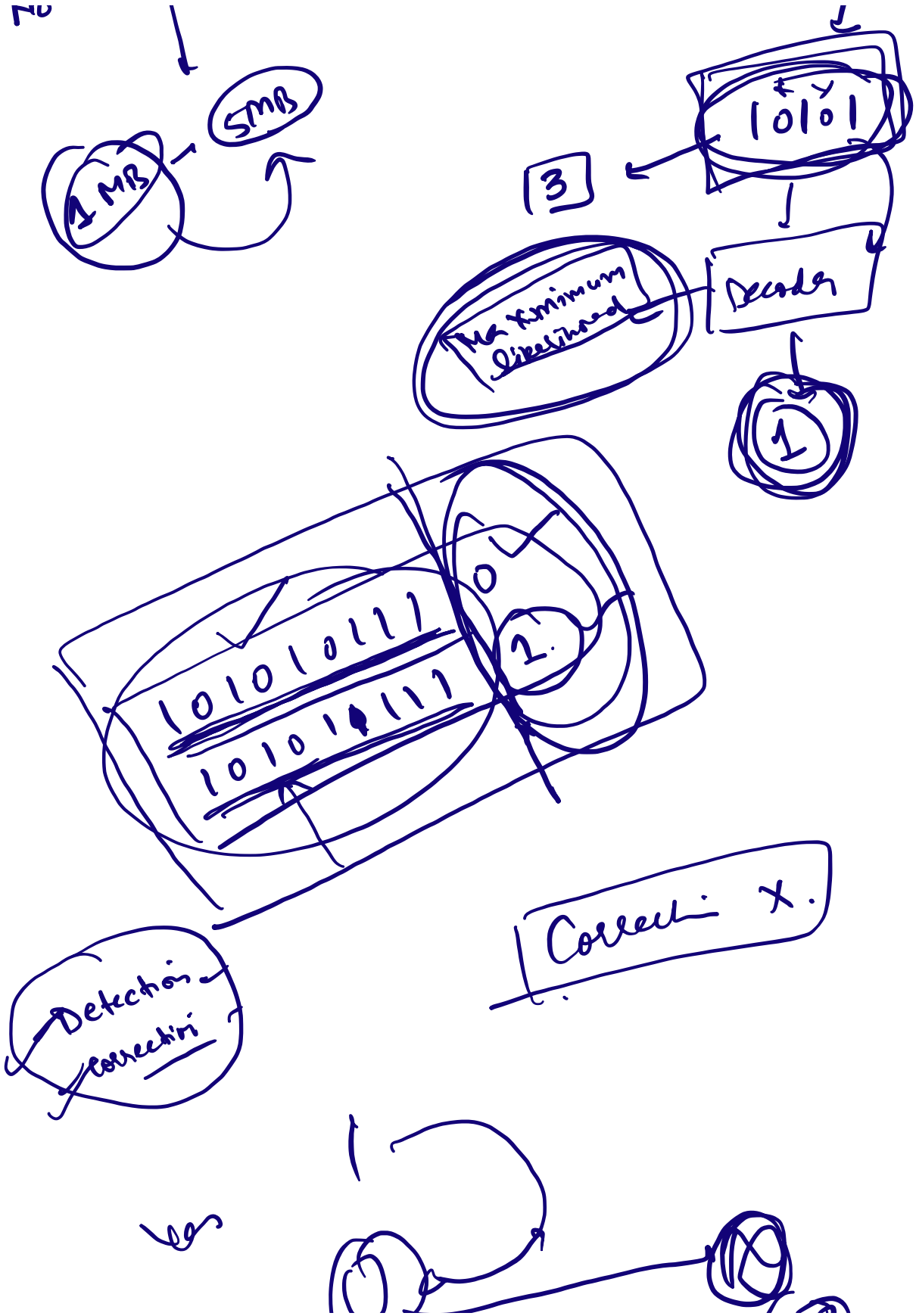
Error Correction

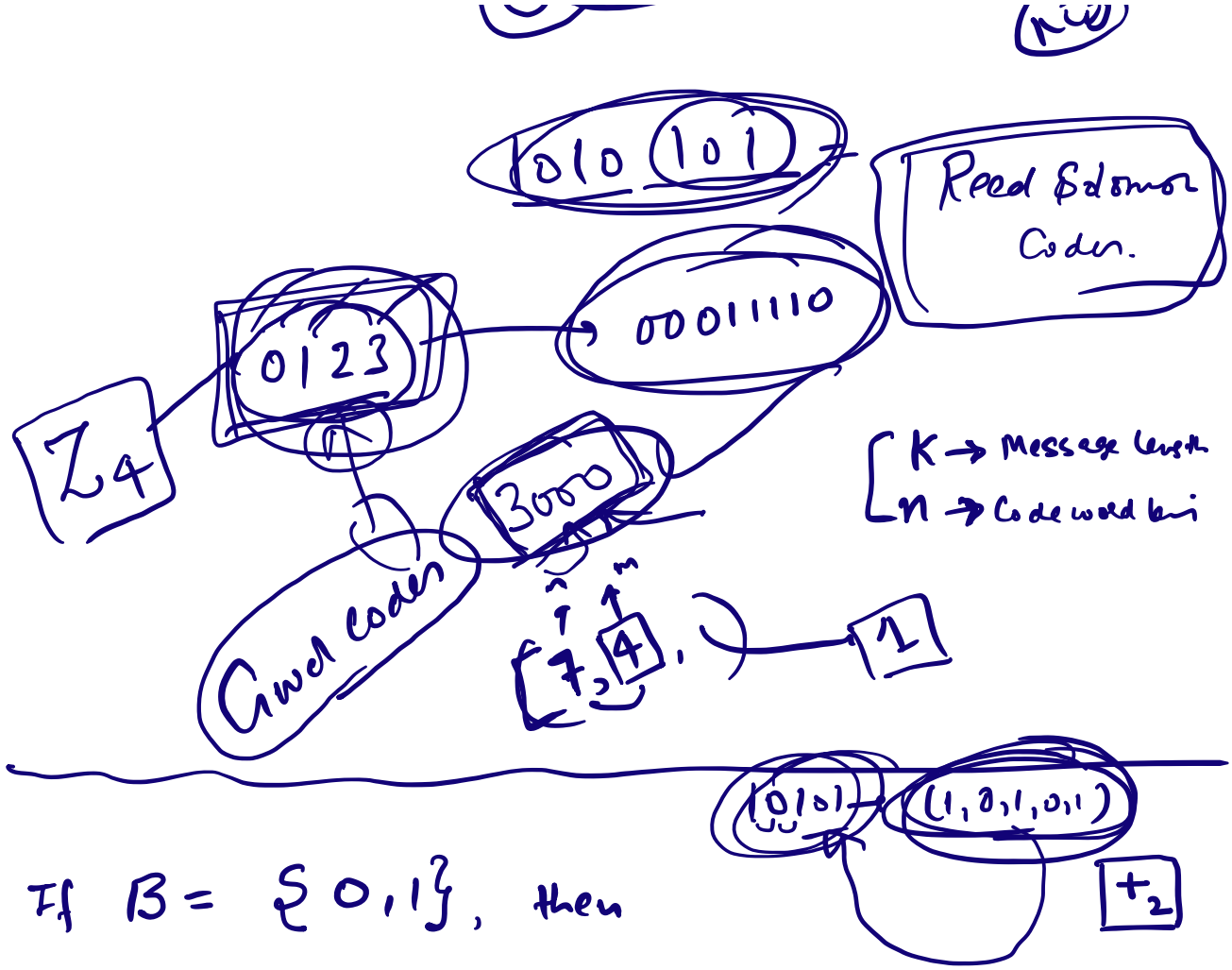
OR

Error Correcting Codes.




yes
NO
transmission
reliable
unreliable channels
Sender
Encoder
Noisy Channel
Decoder
(Message)
Receiver
yes
00000


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



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

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

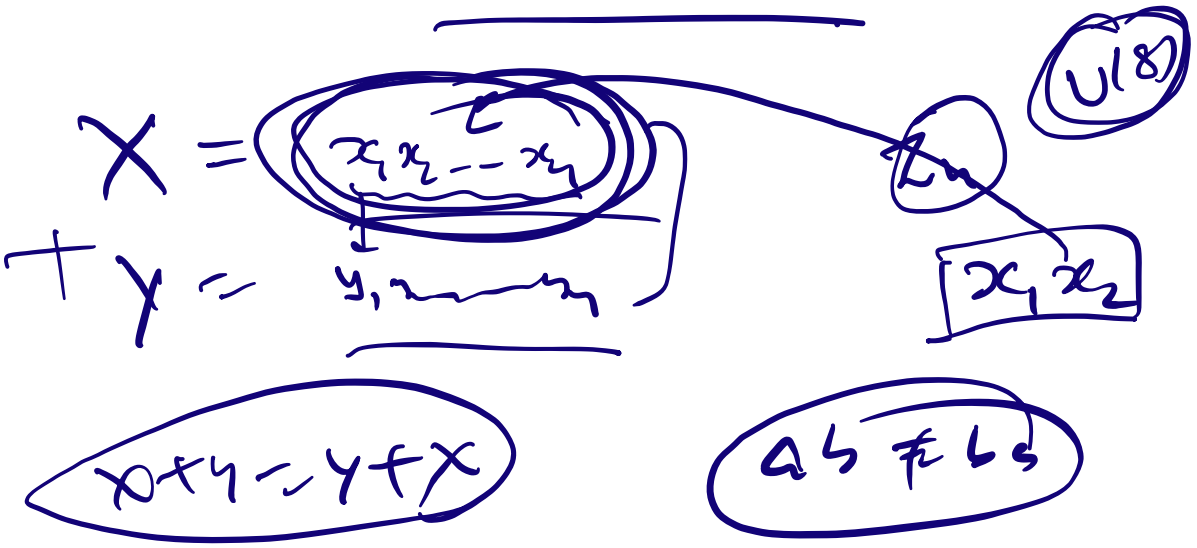
(Z_4) ($+_4$)

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.



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

Group code

$B = \{0,1\}$

$\oplus \rightarrow +_2$

$(B^n, \oplus)$

abelian group

Binary string of length n.

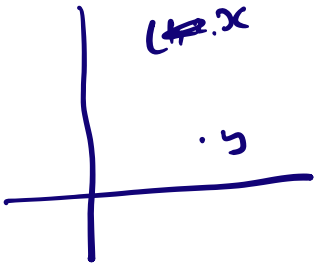
Def: [Weight of a binary string]

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 $d(x, y)$.

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

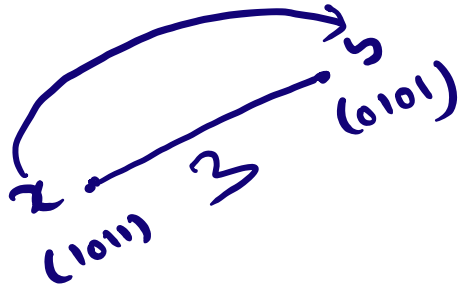
$x = |101|$

$y = 0101$

$d(x,y) = 3$

$x+y = 1110$

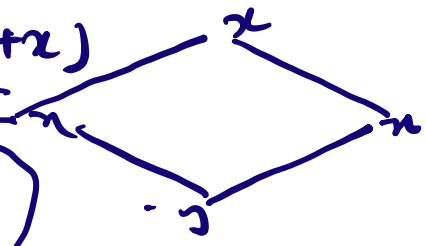
$w(x+y) = 3.$

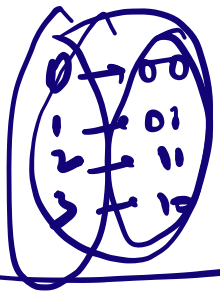


$$d(x,y) = d(x+x, y+x)$$

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

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





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

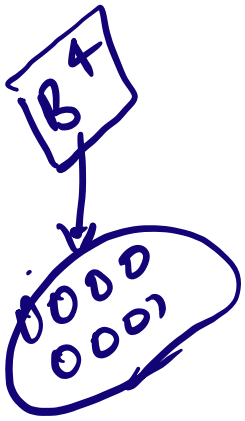
$(x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$

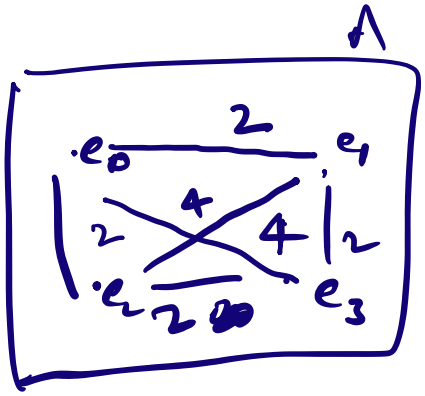
Minimum Distance:

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

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

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





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

$= 2$

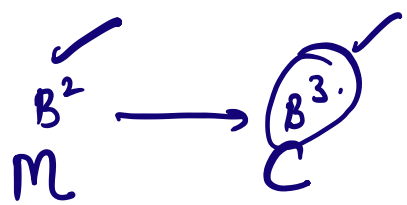
Encoding function:

A function $e : B^{(m)} \longrightarrow B^{(n)}$

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

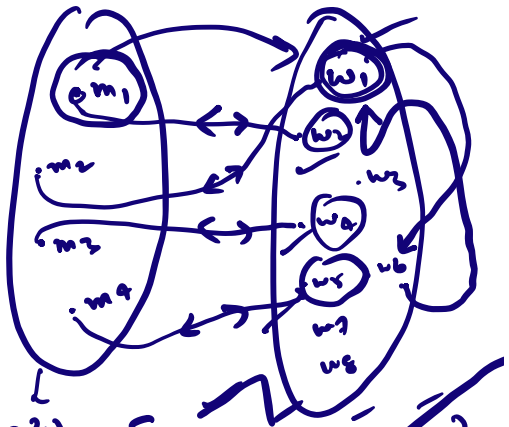
$\Rightarrow$ If x is the original msg

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



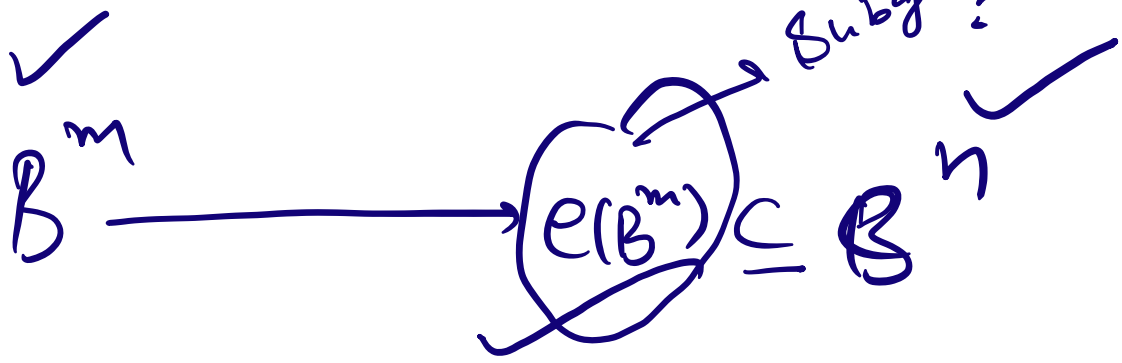
$\Rightarrow$ $e(x)$ is called the codeword.

Code := Collection (Set) of codewords.

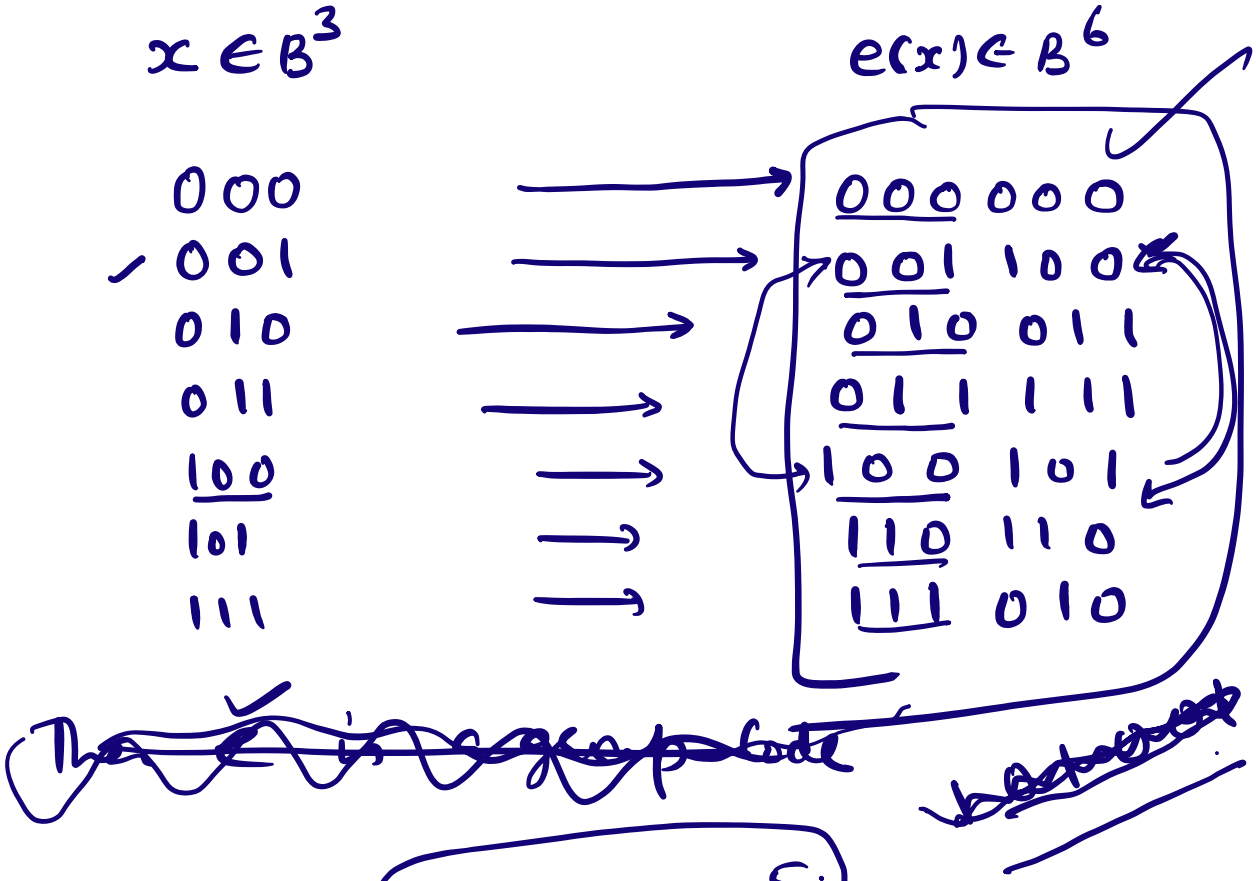


Group code:

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

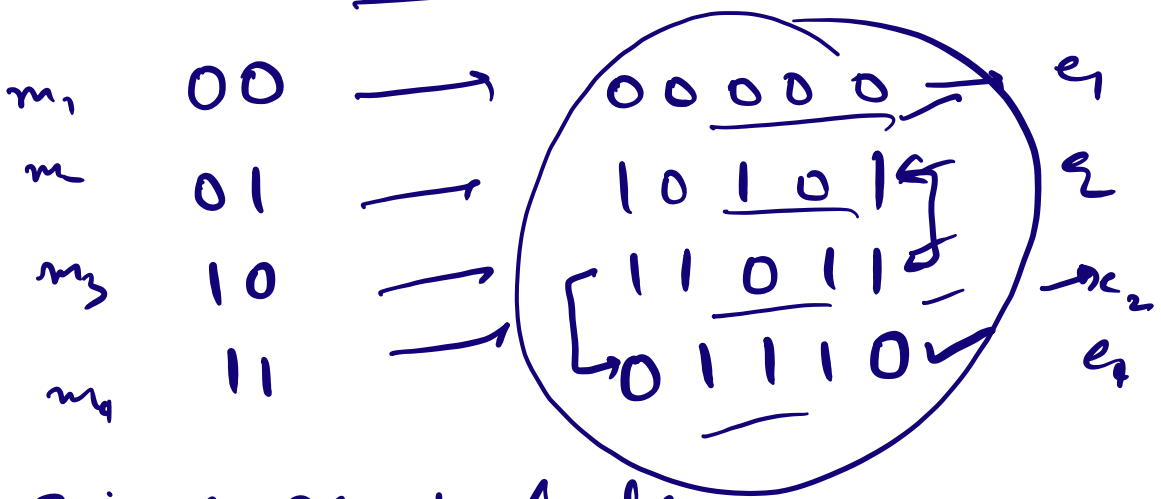


Eg: Consider (3,6)-encoding function: $e: B^3 \to B^6$ defined as:

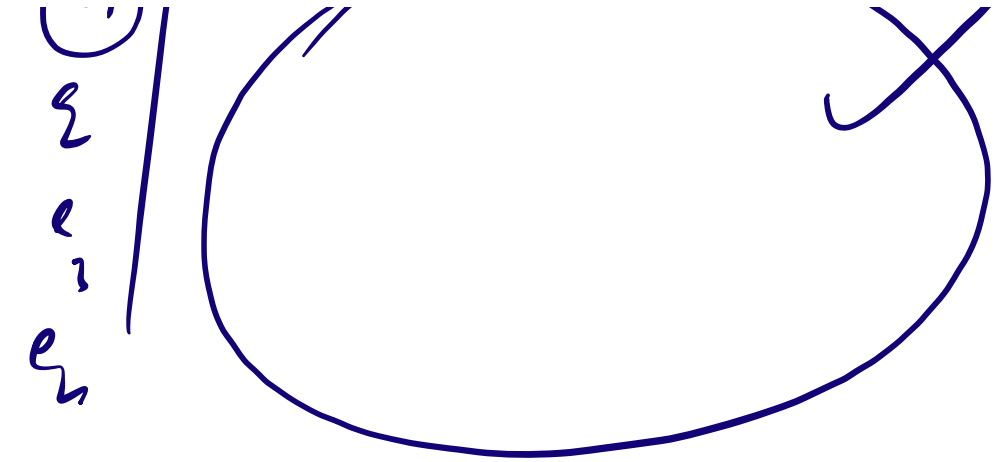


~~The ... code~~

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



e in a group code



Subgroup Condition

$x, y \in H$

$\Rightarrow xy \in H$

x ✓

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

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

$m=2$

$m=5$

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

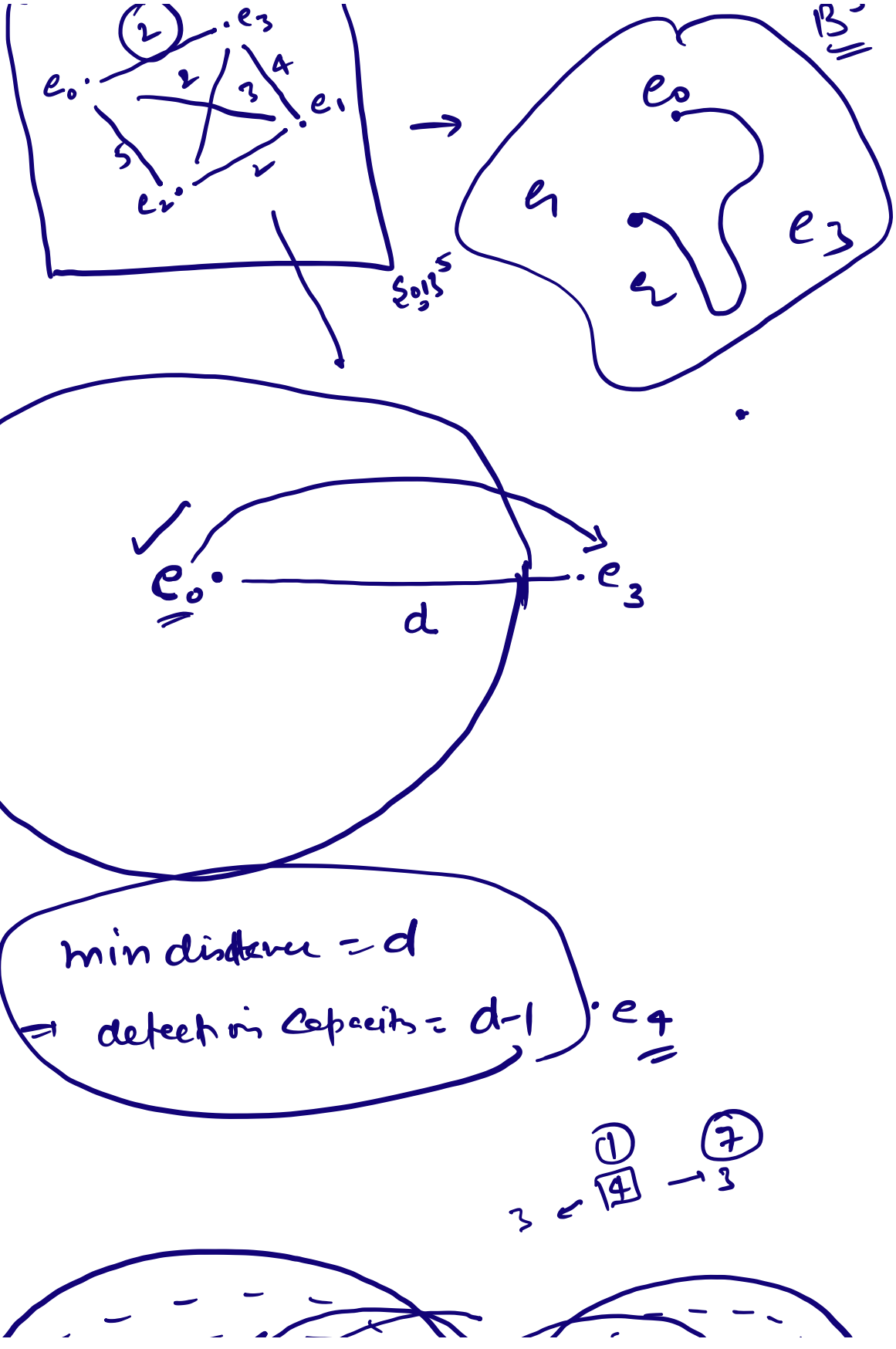
$m_1 \to 10 \to 10101_{e_1}$

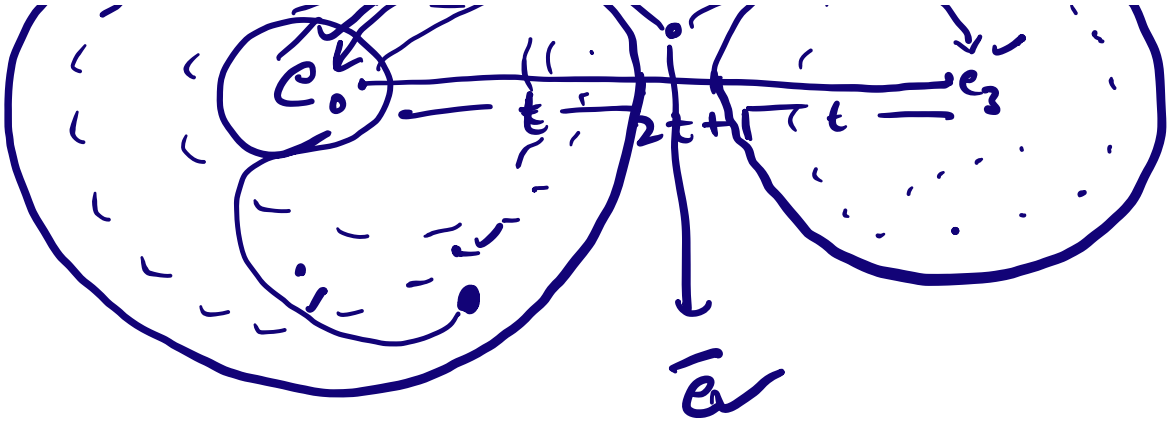
$m_2 \to 11 \to 11011_{e_2}$

$m_3 \to 01 \to 01111_{e_3}$

$e(m_0) = e_0$

$e(m_1) = e_1$


e0
e1
e2
e3
2
2
3
4
5
1
{0,1,3}^5
B
e0
e1
e2
e3
e0
d
e3
min distance = d
⇒ detect in capacity = d-1
e4
1
4
7
3
3



$\bar{c}$

Min distance = $2t+1$

$\Rightarrow$ Error Correction Capacity = t

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

$x, y \in C$

00 →	00000_{c_0}
10 →	10101_{c_1}
11 →	11011_{c_2}
01 →	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.

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

$e(00) = 000000 = e_0$, $w(e_0) = 0$

$e(01) = 011110 = e_1$, $w(e_1) = 4$

$e(11) = 111000 = e_2$, $w(e_2) = 3$

$e(10) = 101010 = e_3$, $w(e_3) = 3$.

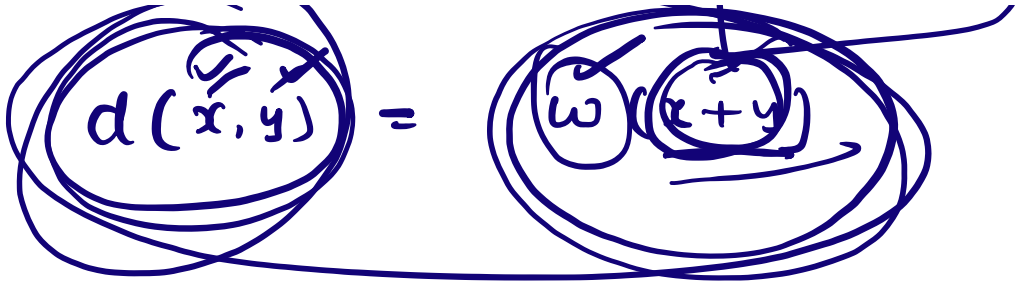
$e_1 + e_2 = 100110 \notin C$

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

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

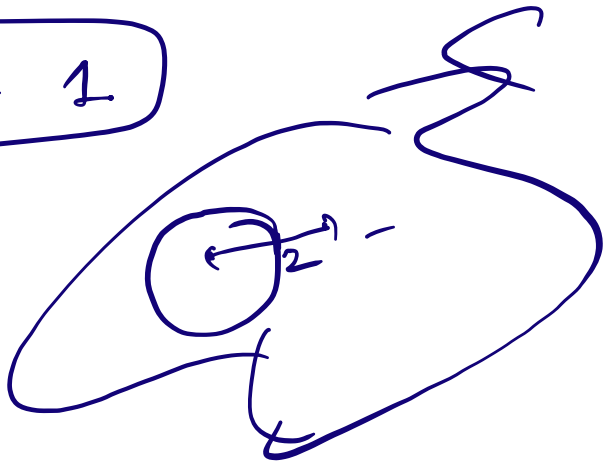
$d(e_1, e_3) = w(e_1 + e_3) = w(110100) = 3$

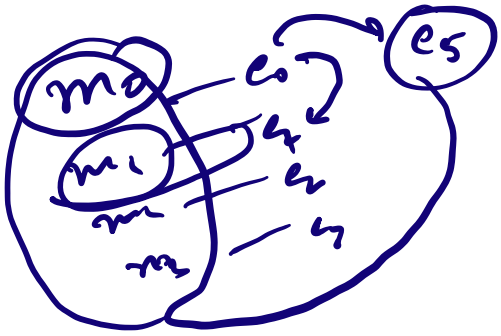
$d(e_2, e_3) = w(e_2 + e_3) = w(010010) = 2$



Min distance = 2

Detection Capacity = 1



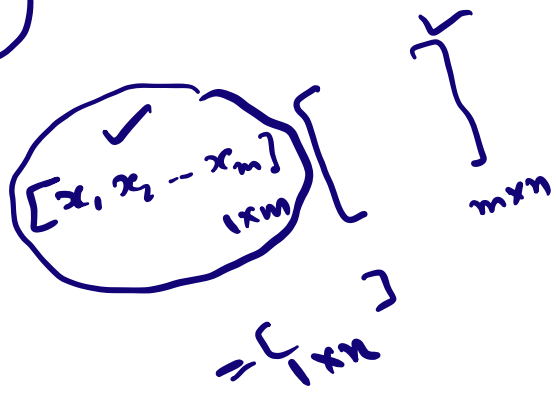


Generator matrix

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

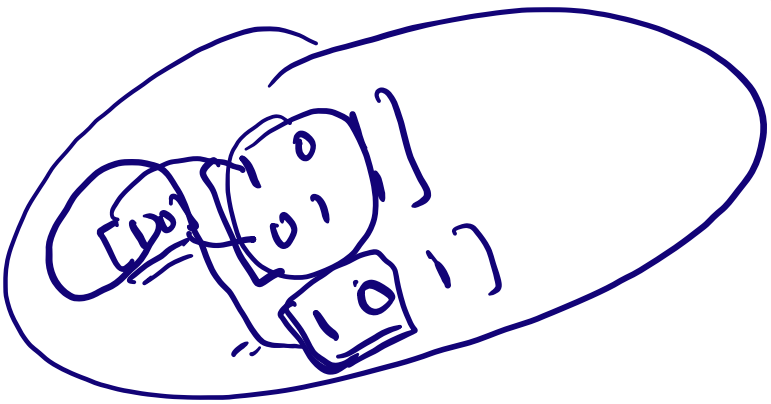
where A is any matrix of order $m \times (n-m)$

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 :

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

② Using parity check matrix :

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

Connection b/w G and H. ($H \to (n-m)\times n$)

(if given in standard form)

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

$$\updownarrow$$

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

Let $e: B^2 \to B^5$ is a Code (Group) whose generator matrix is:

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

$$\checkmark \quad \left[\begin{array}{cc|ccc} 0 & 1 & 0 & 1 & 1 \\ & I_2 & & A & \end{array}\right] \quad (2 \times 5)$$

Then find the full code using both methods.

a $x \in B^2 = \{00, 01, 10, 11\}$ $\quad (f)^2 = 16$

$c = xG$.

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

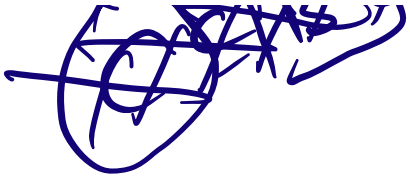
$= [0\,0\,0\,0\,0]$

$[0\,1]G = [0\,1\,0\,1\,1]$

$[1\,0]G = [1\,0\,1\,1\,1]$

$[1\,1]G = [1\,1\,1\,0\,0]$

$C = \{00000, 01011, 10111, 11100\}$



Code

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

$e(x) = xG$.

$[x_1\ x_2]\,G$.

$[0\ 1\ 0]$

$$\begin{matrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{matrix}$$

$[0\ 1\ 1\ 0\ 0]$

$C = \{00000,\ 01011,\ 10111,\ 11100\}$

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

$G \to (2) \times (5)$

Alternatively

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

What is

$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ (2 × 5)

I_2 $\quad$ A

H ?

$G = [I_k \mid A]$

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

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

Let $x \in B^5$ such that x is a codeword.

Then $\quad x H^T = 0$

$x = (x_1\ x_2\ x_3\ x_4\ x_5)$

$$x H^T = (x_1\ x_2\ x_3\ x_4\ x_5) \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$

$$\left\{ \begin{array}{l} x_1 + x_3 = 0 \\ x_1 + x_2 + x_4 = 0 \\ x_1 + x_2 + x_5 = 0 \end{array} \right\}$$ parity check equations

No of eq = 3

No of var = 5.

No of var free var:

$= 5 - 3$

$= 2$

x_4, x_5 as free

$x_3 = x_1$
$x_4 = x_1 + x_2$
$x_5 = x_1 + x_2$

$x_1 = s$
$x_2 = t$

$(x_1 x_2 x_3 x_4 x_5) = (x_1, x_2, x_1, x_1+x_2, x_1+x_2)$

$\therefore$ $(x_1, x_2, x_1, x_1+x_2, x_1+x_2)$ is a codeword

$\forall\ x_1, x_2 \in \{0,1\}$

$x_1 x_2$

B4

$(0,0,0,0,0)$

$(1,0,1,1,1)$

$(0,1,0,1,1)$

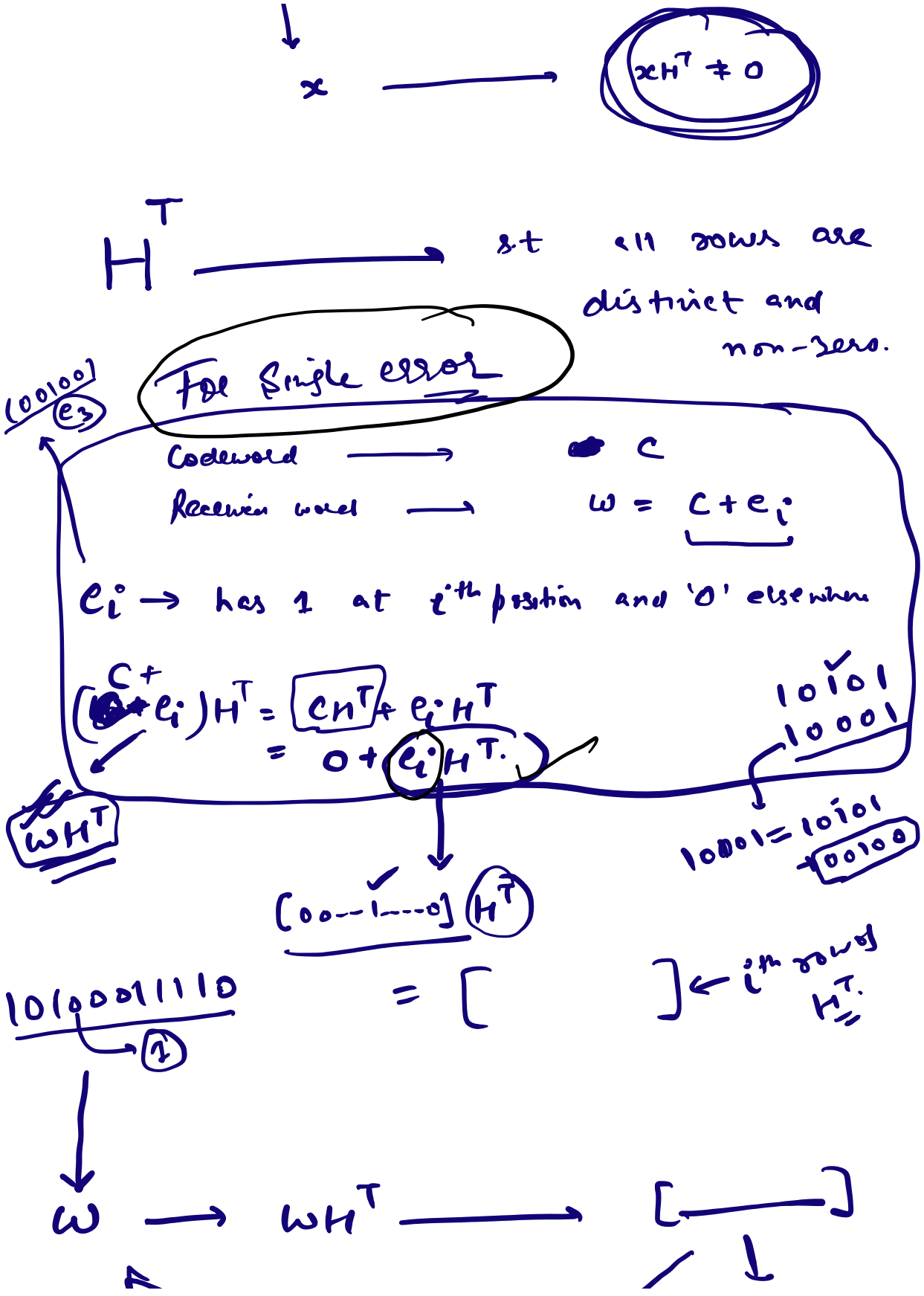
$(1,1,1,0,0)$

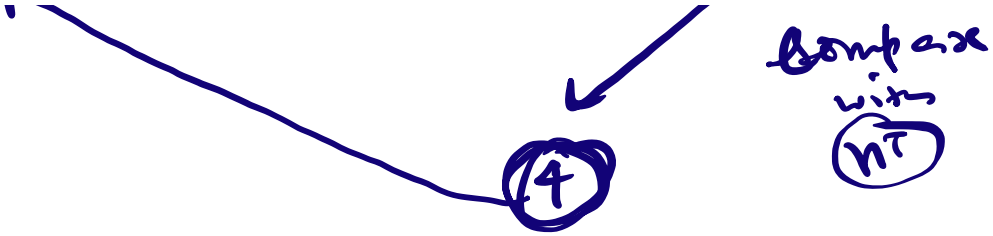
$C = \{00000, 01011, 10111, 11100\}$

C

C

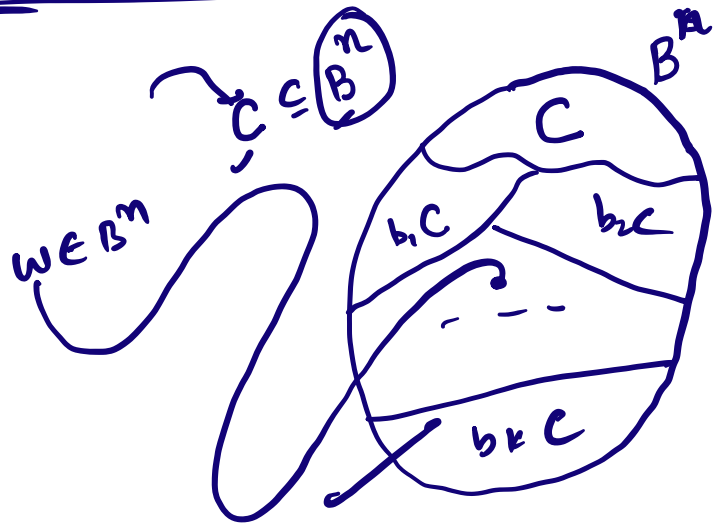
$\mathbb{R}$

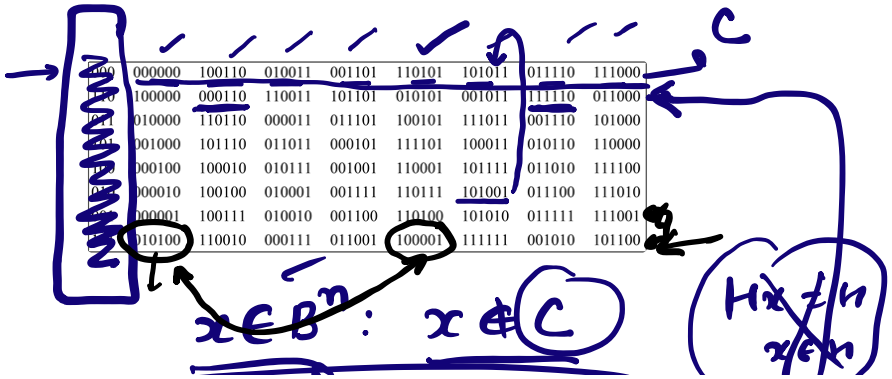

x
$xH^T \neq 0$
H^T
s.t all rows are distinct and non-zero.
For Single error
00100
e_3
Codeword → c
Received word → $w = c + e_i$
e_i → has 1 at i^{th} position and '0' elsewhere
$(c + e_i)H^T = cH^T + e_i H^T$
$= 0 + e_i H^T$
wH^T
10101
10001
10001 = 10101
00100
[00--1---0] H^T
10100011110
1
= [ ] ← i^{th} row of H^T
w → wH^T → [ ]



Example: Try by yourselves

Coset Decoding





$(000110) + C$

$x + H = H \iff x \in H$

Ex:

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

$C = \{ 00000, 01011, 10111, 11100 \}$

00 01 10 11

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

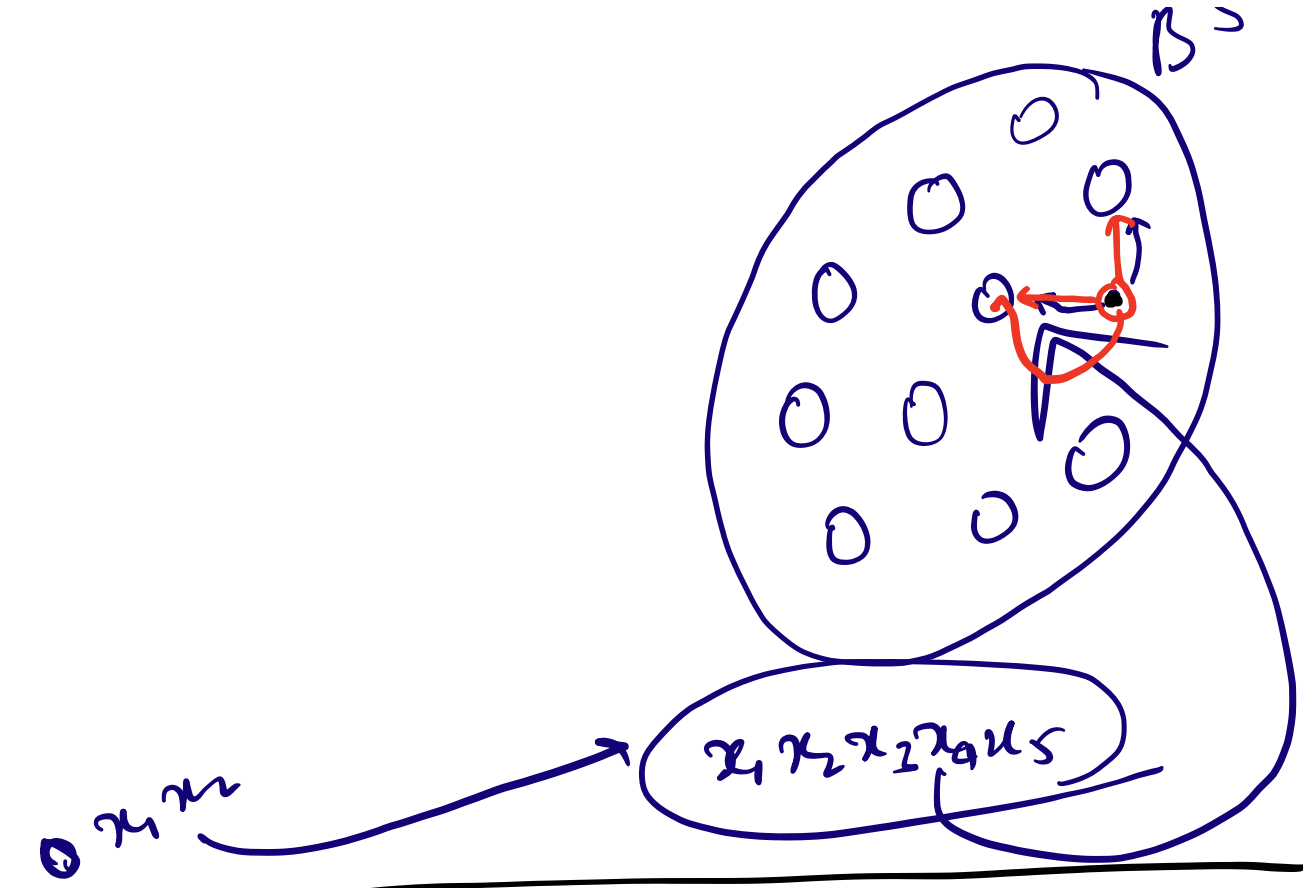
$(10000) + C$

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

$2^5 = 32$

Coset leaders

10011 11000 00100 01111



Coset decoding is actually Nearest Neighbourhood decodi.

$[v + C = w + C]$

Coset leader.

$w = v + c' : \quad c \in C.$

$d(C, w)$ = min weight

$d(c', w) = wt(c' - w) \geq wt(v)$

$\geq wt(w - c)$

$\geq d(w, c)$

Syndrome decoding

$x \in B^n$: defined Syndrome of x as:

$$Syn(x) = x H^T$$

$Syn(x) = 0 \iff x$ is a Codeword.

$x \in w + C$ ($v + C$ coset leader)

$c_1 \in C$.

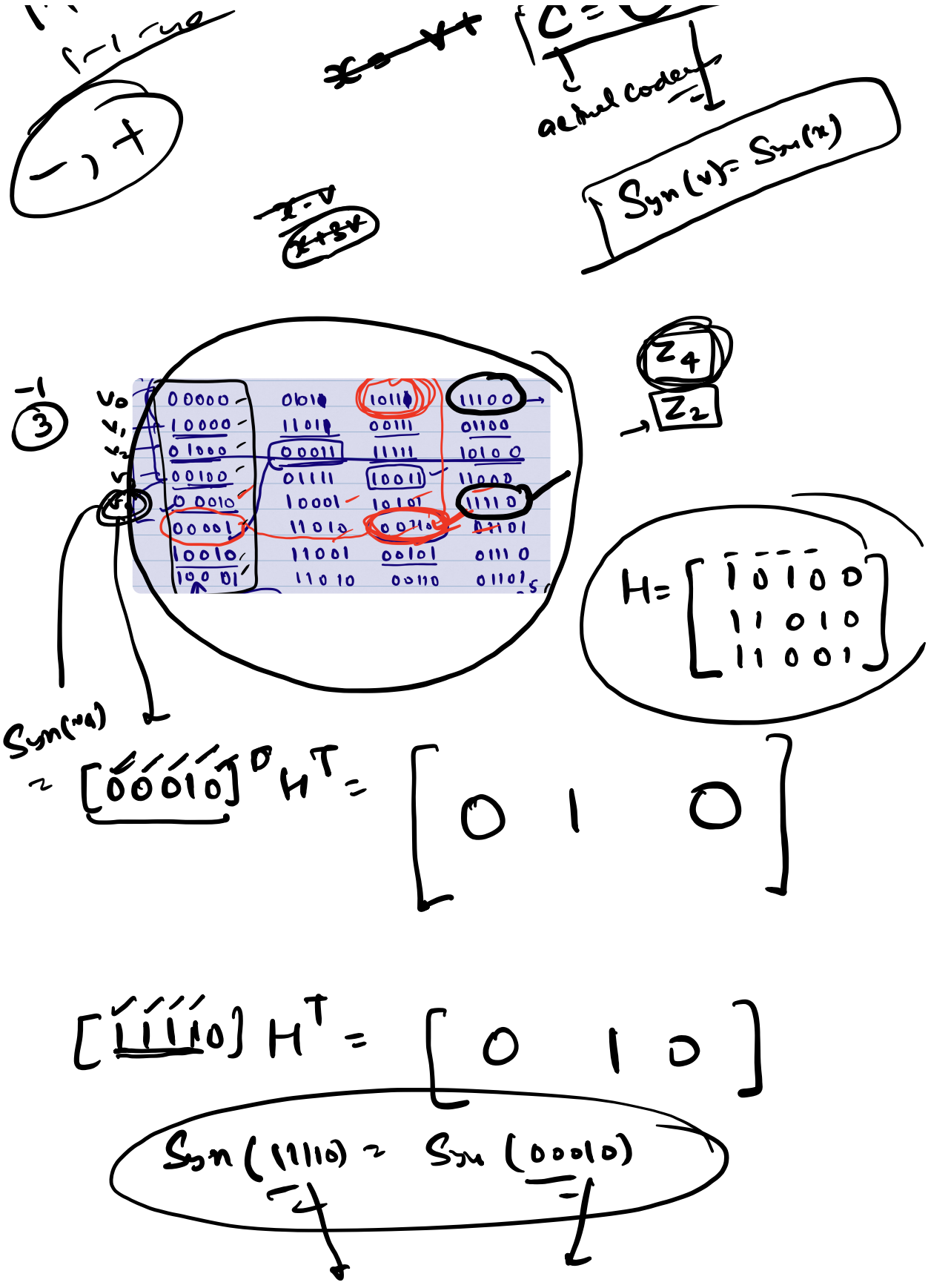
$x = v + c_1$:

$xH^T = vH^T + c_1 H^T$

$Syn(x) = vH^T + 0$

$Syn(x) = Syn(v)$

$x + v$


Syn(v) = Syn(x)
H = [1 0 1 0 0; 1 1 0 1 0; 1 1 0 0 1]
Syn(x) = [0 0 0 1 0] H^T = [0 1 0]
[1 1 1 1 0] H^T = [0 1 0]
Syn(11110) = Syn(00010)

$$C = 11110 + 00010$$

$$= 11100$$