# Galois Field:

## Properties:

(1) $a, b \in F \Rightarrow a+b, a \cdot b \in F$

(2) Commutative Law: $a+b = b+a$ where $a, b \in F$
$a \cdot b = b \cdot a$

(3) Associative Law: $(a+b)+c = a+(b+c)$ where $a, b, c \in F$
$(a \cdot b) c = a \cdot (b \cdot c)$

(4) Distributive Law: $a \cdot (b+c) = a \cdot b + b \cdot c$

(5) Further, identity elements: 0 and 1 must exist in F satisfying:

(a) $a+0 = a$ (b) $a \cdot 1 = a$

(c) If $a \in F$, there exists an additive inverse $(-a)$ such that

$a + (-a) = 0$

(d) If $a \in F$, there exists a multiplicative inverse $\left(\frac{1}{a}\right) / (a^{-1})$ such that $a \cdot \left(\frac{1}{a}\right) = 1$ (or) $a \cdot a^{-1} = 1$

---

Ex: $GF(2) = \{0, 1\}$ mod 2 $(1+1 = 2 \bmod 2 = 0)$

(Exclusive OR)

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

# Galois Field:

## Properties:

(1) $a, b \in F \Rightarrow a+b, a \cdot b \in F$

(2) Commutative Law: $a+b = b+a$ where $a, b \in F$
$a \cdot b = b \cdot a$

(3) Associative Law: $(a+b)+c = a+(b+c)$ where $a, b, c \in F$
$(a \cdot b) c = a \cdot (b \cdot c)$

(4) Distributive Law: $a \cdot (b+c) = a \cdot b + b \cdot c$

(5) Further, identity elements: 0 and 1 must exist in F satisfying:

(a) $a+0 = a$ (b) $a \cdot 1 = a$

(c) If $a \in F$, there exists an additive inverse $(-a)$ such that

$a + (-a) = 0$

(d) If $a \in F$, there exists a multiplicative inverse $\left(\frac{1}{a}\right)$ / $(a^{-1})$ such that $a \cdot \left(\frac{1}{a}\right) = 1$ (or) $a \cdot a^{-1} = 1$

---

Ex: $GF(2) = \{0, 1\}$ mod 2 $(1+1 = 2 \bmod 2 = 0)$

(Exclusive OR)

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Ex: $GF(2) = \{0, 1\}$ ∴ given field is a Galois Field

→ Additive inverse of '1' is 1 [As $1 \oplus 1 = 0$]
(1 belongs to GF(2))

→ Additive inverse of '0' is $0 \in GF(2)$ [As $0 \oplus 0 = 0$]

→ Multiplicative inverse of '1' is $1 \in GF(2)$ [As $1 * 1 = 1$]

<> (Multiplicative inverse calculated only for non-zero elements)

Ex: $GF(3) = \{0, 1, 2\}$ ✱ mod P (mod 3)

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

(2+2=4) (4 mod 3 = 1)

| * | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

(2*2=4) (4 mod 3 = 1)

- Additive inverse of '1' is $2 \in GF$
  " " '2' is $1 \in GF$

- Multiplicative inverse of '1' is $1 \in GF$
  " " '2' is $2 \in GF$

∴ Given is a Galois field

Ex GF(4)

| + | 0 | |
|---|---|---|
| 0 | 0 | |
| 1 | 1 | |
| 2 | 2 | |
| 3 | 3 | 0 |

- Its
Multip

✱ GF(2)

✱ GF($2^m$)

Generator

← k →
encoded

- Extra
- These
checker

$2^k$ message sequences { 000 ... 111 ...

Ex GF(4) = {0, 1, 2, 3} (mod 4)

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

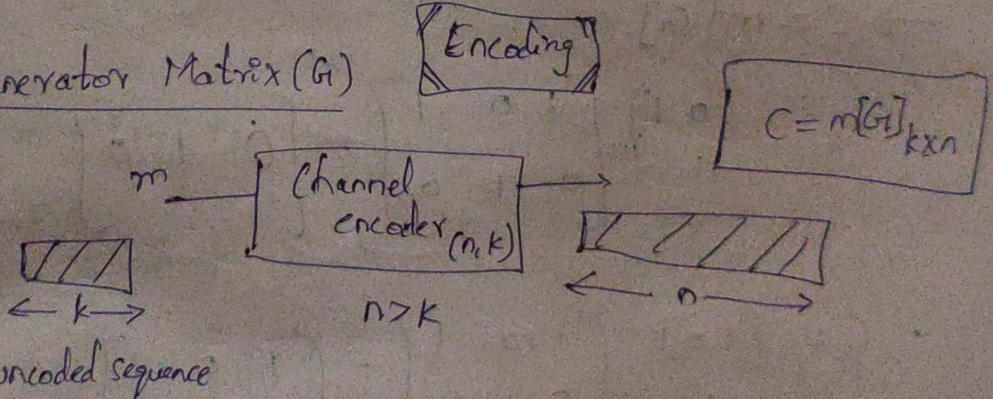
- Its not a field as '2' does not have Multiplicative inverse belonging to GF

---

# GF(2) → 2 - prime number

# GF($2^m$) → Extension field , m → Integer

Generator Matrix (G)




uncoded sequence

- Extra bits are added to uncoded sequence.
- These extra bits called as Redundant or Parity checker bits.

$2^k$ message sequences { 000...0, 000..., ..., 111...1 } ($2^k$ x n) $2^k$ codewords { 0000...0, ..., 111...1 }

Ex: $GF(4) = \{0, 1, 2, 3\}$ (mod 4)

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

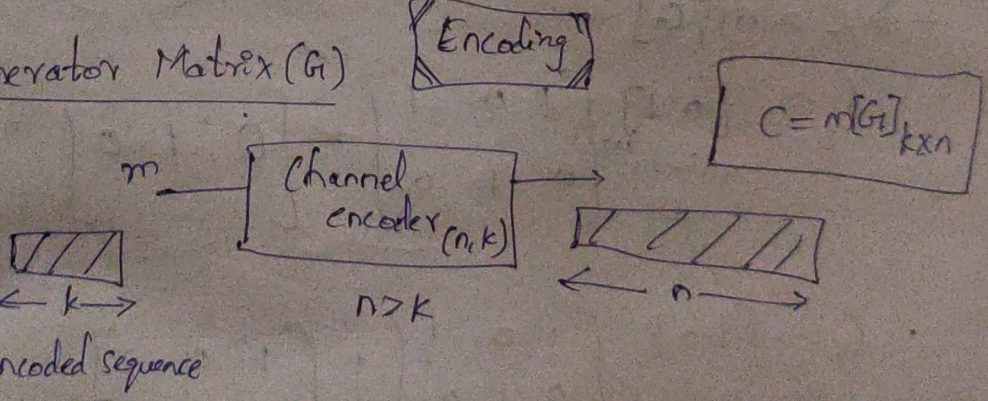
- Its not a field as '2' does not have Multiplicative inverse belonging to GF

---

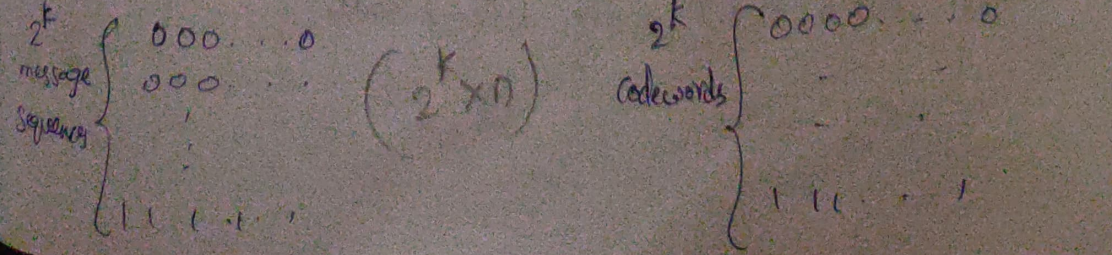
# $GF(2)$ → 2 – prime number

# $GF(2^m)$ → Extension field, m → Integer

Generator Matrix (G)




- Extra bits are added to uncoded sequence.
- These extra bits called as Redundant or Parity checker bits.



Generated: $C = m[G]_{k \times n}$

→ Generator matrix ($G_1$) is a better way of representing encoded sequences in terms of coded forms.

Ex: $G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}_{2\times 3}$ (over GF(2))

$I_{2\times 2}$ $P_{2\times 1}$

$k \times n = 2 \times 3$

$\Rightarrow k = 2$

$n = 3$

- No. of encoded sequences $= 2^k = 2^2 = 4$

| msg. sequences (m) | Codeword (c) | |
|---|---|---|
| 0 0 | 0 0 0 | $R_1 + R_2$ |
| 0 1 | 0 1 0 | $R_1$ |
| 1 0 | 1 0 1 | $R_2$ |
| 1 1 | 1 1 1 | $R_1 \oplus R_2$ |

→ $C = m[G]$

- $C_2 = \begin{bmatrix} 0 & 1 \end{bmatrix}_{1\times 2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}_{2\times 3} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$

- $C_3 = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$

- $C_4 = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$

- This code is (n, k), i.e. (3, 2) code

$G_1 =$

$m = [x_1$

$\# C = m G_1$

$C = [x_1 g_1 + x_2$

$C = [c_1$

Codeword as Column Vector for

$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{bmatrix} = x$

$$G = \begin{bmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1n} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2n} \\ \vdots & & & & \\ g_{k1} & g_{k2} & g_{k3} & \cdots & g_{kn} \end{bmatrix}_{k \times n}$$

$$m = [x_1 \; x_2 \; \cdots \; x_k]_{1 \times k}$$

$$\# \; C = m G$$

$$C = [\underbrace{x_1 g_{11} + x_2 g_{21} + \cdots + x_k g_{k1}}_{c_1} \quad \underbrace{x_1 g_{12} + x_2 g_{22} + \cdots + x_k g_{k2}}_{c_2} \quad \cdots \quad \underbrace{x_1 g_{1n} + \cdots + x_k g_{kn}}_{c_n}]$$

$$C = [c_1 \; c_2 \; c_3 \; \cdots \; c_n]_{1 \times n}$$

Codeword in (Column Vector form)

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{bmatrix} = x_1 \begin{bmatrix} g_{11} \\ g_{12} \\ g_{13} \\ \vdots \\ g_{1n} \end{bmatrix} + x_2 \begin{bmatrix} g_{21} \\ g_{22} \\ g_{23} \\ \vdots \\ g_{2n} \end{bmatrix} + \cdots + x_k \begin{bmatrix} g_{1n} \\ g_{2n} \\ g_{3n} \\ \vdots \\ g_{kn} \end{bmatrix}$$

→ Codeword is simply a linear combination of rows of 'G'

$$C_{1\times n} = m_{1\times k}\, G_{k\times n}$$

→ Rows of 'G' are linearly independent.

→ Rows of 'G' are basis vectors, not unique

→ 'G' is also not unique

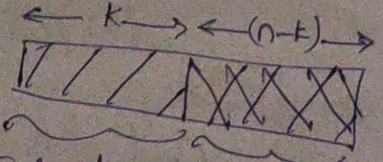
(any vector can be expressed as a linear combination of basis vectors)

Systematic form:

$$G = \left[ I_{k\times k} \;:\; P_{k\times(n-k)} \right]_{k\times n}$$

$I_{k\times k}$ → Identity Matrix

$P_{k\times(n-k)}$ → Parity Matrix

$C =$ 


Information bits | Parity bits

$$G = \begin{bmatrix} 0000\ldots01 & : & P_{11}\ P_{12}\ \ldots\ P_{1(n-k)} \\ 0000\ldots10 & : & P_{21}\ P_{22}\ \ldots\ P_{2(n-k)} \\ \vdots & & \vdots \\ 1000\ldots00 & : & P_{k1}\ P_{k2}\ \ldots\ P_{k(n-k)} \end{bmatrix}$$

- Maximum distance Codes : $d^* = n-k+1$

$$\boxed{d^* \leq n-k+1}$$

02/02/2023

- Generator matrix (G) is useful at Encoder.
- Parity check matrix (H) is useful at Decoder.

## Parity Check Matrix (H):

(In Systematic form)

$$H = \left[ -P^t_{(n-k)\times k} : I_{n-k} \right]_{(n-k)\times n}$$

$$GH^T = \begin{bmatrix} I & P \end{bmatrix} \begin{bmatrix} -P^t \\ I \end{bmatrix} = 0$$

→ Minimum distance : $d^*$ = No of columns that are Linearly dependent in "H".

→ $d^* - 1$ = No. of columns that are linearly independent.

## Decoding:

→ $(n, k)$ code can detect $d^* - 1$ errors.

→ $(n, k)$ code can correct upto $t = \left\lfloor \frac{d^* - 1}{2} \right\rfloor$ errors.

→

# Decoding

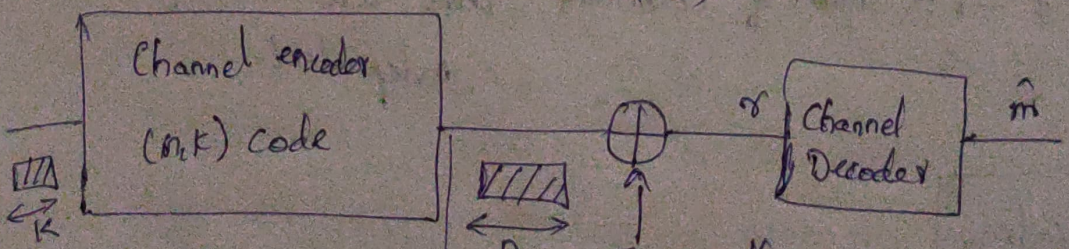
- Detection and Correction are different.
- Even after detecting there are errors in code, we need to find at which places error is there.

Ex: Consider the (5, 2) code

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{2\times 5} \quad \text{(Encoding)}$$

- $C = \{\underset{c_1}{00000}, \underset{c_2}{10111}, \underset{c_3}{01101}, \underset{c_4}{11010}\}$
- $d^* = 3$
- It can detect $(d^* - 1) = 2$ errors, and
- It can correct only $t = \left[\left[\frac{d^*-1}{2}\right]\right] = 1$ error.

(floor)




$C = \{c_1, c_2, c_3, c_4\}$

Error pattern (e)

$2^n$ error patterns

00000
00001
00010
10111
01101
11010
11111

received codewords (r)

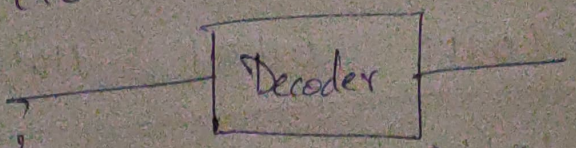
$2^n$ received codewords

00000
00001
00010
11111

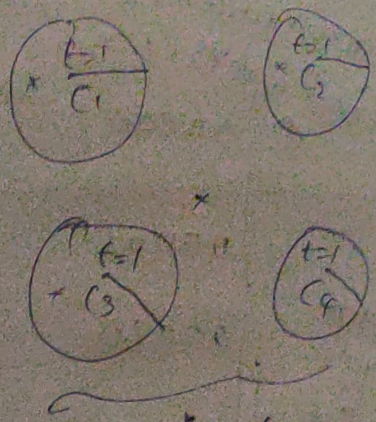
$r = c + e$

$c = r - e$

• $r = c + e$




$c_2 = 10111$ } → 11010 = $c_4$
$e = 01101$ }
(Undetectable errors)




$2^k$ spheres

In Summary:

• $(2^n)$ – Error Patterns (including all zero error pattern)

• $(2^k)$ – Undetectable error patterns

• $(2^n - 2^k)$ – Detectable error patterns.

• $(2^{n-k} - 1)$ – Correctable

Here, Correctable = $2^{5-2} - 1 = 7$

• No. of ~~spheres~~ points in each sphere:

$$= 2^k \{ 1 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_t \} \leq 2^n$$

$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n \quad \text{(Hamming bound)}$$

→ Equality holds for perfect code.

# (1) Standard Array Decoding

(2) Syndrome Decoding

Error patterns (or) Coset leaders $C_1 = 2^{n-k}$

| | $C_2$ | $C_3$ | $C_4$ (Valid codewords) |
|---|---|---|---|
| 00000 | 10111 | 01101 | 11010 |
| 00001 | 10110 | 01100 | 11011 |
| 00010 | 10101 | 01110 | 11000 |
| 00100 | 10011 | 01001 | 11110 |
| 01000 | 11111 | 00101 | 10010 |
| 10000 | 00111 | 11101 | 01010 |
| 00011 | 10100 | 01110 | 11001 |
| 00110 | 10001 | 01011 | 11100 |
| 01100 | 11011 | 00001 | 10110 |
| 11000 | 01111 | 10101 | 00010 |

(Each row is called Coset)

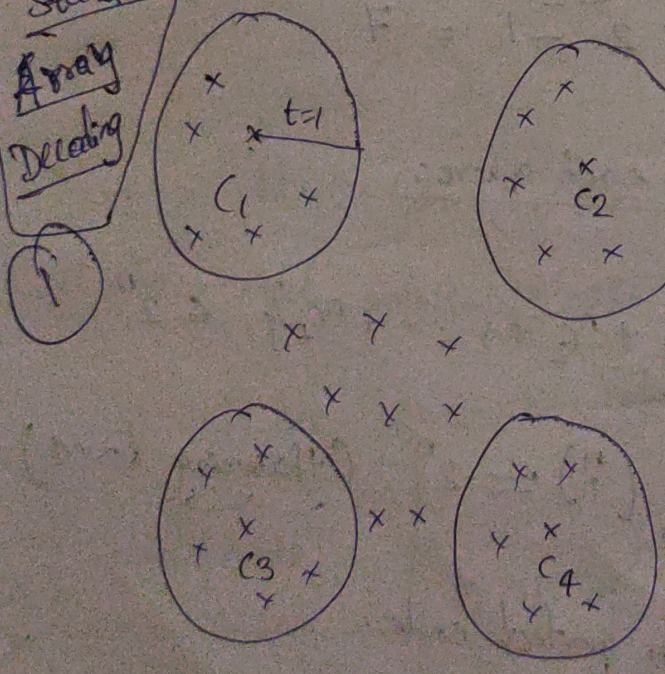
$w = 2$

Correct to consider as they are already repeated

~~10111~~
~~01100~~
~~11011~~

~~01101~~
~~01100~~
~~00001~~
~~11010~~
~~01100~~
~~10101~~

Standard Array Decoding



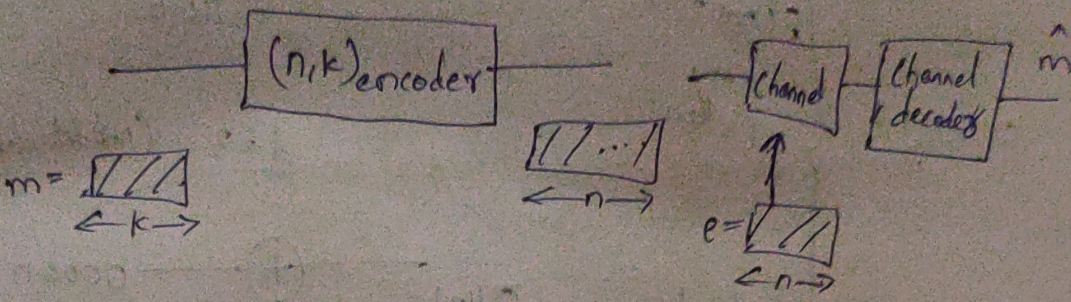

→ (5, 2) can detect and correct 1-bit error.

→ (5, 2) can detect 2-bit errors but can correct pattern of (00011), (00110)

8/08/2023

# $(n, k)$ code can detect upto $(d^* - 1)$ errors.

# $(n, k)$ code can correct upto $\left\lfloor \frac{(d^* - 1)}{2} \right\rfloor$ errors.




→ $(2^n - 1)$ non-zero error patterns are there.

→ $(2^k - 1)$ corresponding to non-zero codewords that are not detectable.

→ $(2^n - 2^k)$ error patterns, ~~codewords~~ are detectable.

→ $(2^{n-k} - 1)$ are correctable.

Ex: $(5, 2)$ code

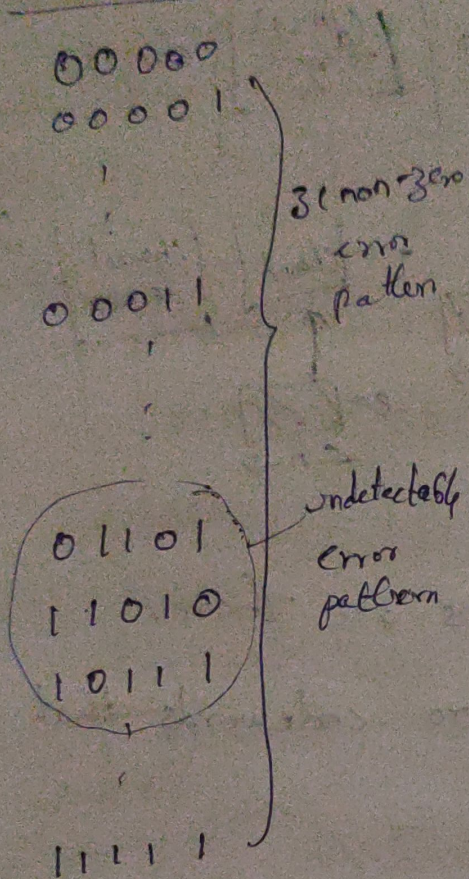
- $2^5 - 1 = 31$ non-zero error patterns
- $2^2 - 1 = 3$ non-zero codewords (undetectable error patterns)
- $2^5 - 2^2 = 28$ error patterns are detectable
- $2^{5-2} - 1 = 7$ are correctable.

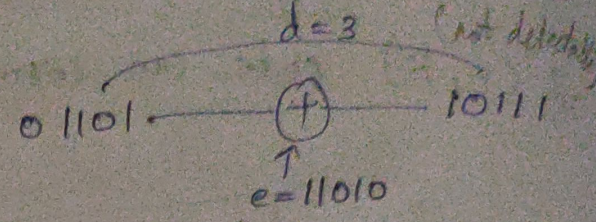
Explanation

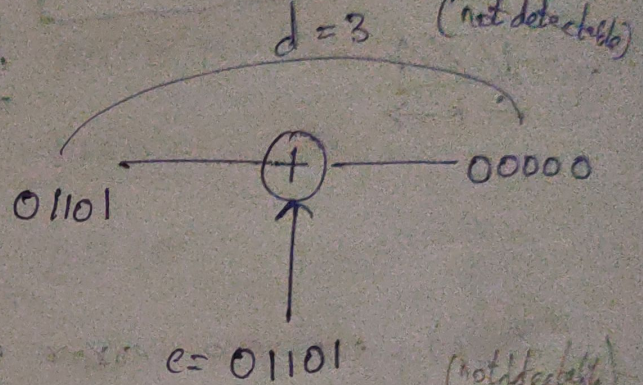
→ $d^* = 3$ for given (5, 2)

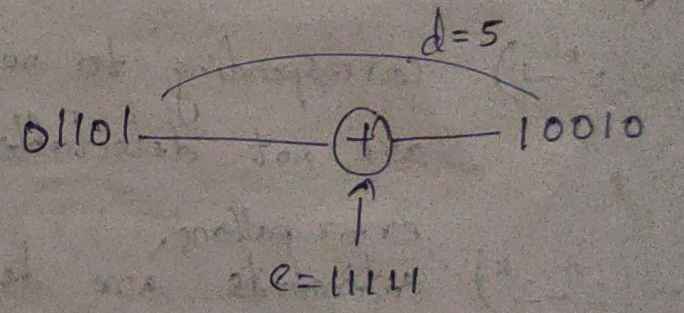
→ (5, 2) can detect upto 2 errors

Error Patterns



## (2) Syndrome Decoding :

# $2^{n-k}$ syndrome Vectors

- Syndrome of the coset leader(e)

$$S = rH^T \quad ; \quad r - \text{received codeword}$$

$$= (c+e)H^T \quad ; \quad c - \text{original/Actual codeword}$$

$e$ - error pattern

$$= cH^T + eH^T \qquad (\text{As } GH^T = 0)$$

$$= \cancel{cH^T}^{0} + eH^T$$

$$= eH^T$$

$$S = e_{1\times n}\, H^T_{n\times(n-k)}$$

$$= S_{1\times(n-k)}$$

$$\therefore S = eH^T$$

Ex: (5,2) code $\quad G = \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{I_{2\times2}} \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}}_{P_{2\times3}}_{2\times5}$

- $H = \begin{bmatrix} P^T \\ (n-k)\times k \end{bmatrix} ; \underbrace{I_{n-k}}_{(n-k)\times(n-k)} = \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}}_{P^T_{3\times2}} \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}}_{I_{3\times3}}_{3\times5}$

As $G = [I_{k\times k} \; ; \; P_{k\times(n-k)}]_{k\times n}$

| Coset Leader (e) | Syndrome |
|---|---|
| 00000 | 000 |
| 00001 | 001 |
| 00010 | 010 |
| 00100 | 100 |
| 01000 | 101 |
| 10000 | 111 |
| 00011 | 011 |
| 00110 | 110 |

# There are total of $2^{n-k}$ syndrome vectors

- Here, there are 8 Syndromes

Explanation:

If: $r = 10010$ (received codeword)

$S = rH^T = 101$ → The corresponding error pattern is $e = 01000$

∴ Transmitted Codeword: $C = r - e$

$\Rightarrow C = [10010] - [01000]$

$C = [11010]$

(2 3)

10010
01000
11010

∴ Transmitted message sequence: $m = [1\ 1]$

# [if it is in systematic form, the first 'k' bits are the message sequence]

$S = rH^T$

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

$= [1\ 0\ 1]$

for $e = 01000$

$S = eH^T$

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

$= [1\ 0\ 1]$

## Hamming Code

. $(n, k) = (2^m - 1, 2^m - 1 - m)$

. For $m = 3$,

## Dual Code

. If $C \sim (n, k)$

. Any codeword in $C^{\perp}$.

. The generator parity check

Problem: A co
self-dual cod
the rate is e

Sol: Given: Code

∴ Rate:

09/02/2023

## Hamming Code

- $(n, k) = (2^m - 1, 2^m - m - 1)$
- For $m = 3$, $(n, k) = (7, 4)$

## Dual Code

- If $C \sim (n, k)$ then $C^{\perp} \sim (n, n-k)$
- Any codeword in 'C' is orthogonal to any codeword in $C^{\perp}$.
- The generator matrix for dual code is the parity check matrix of 'C'.

---

**Problem:** A code is self-dual. Show that in a self-dual code the block length is always even and the rate is 0.5.

**Sol:** Given: Code is self-dual $\Rightarrow C = C^{\perp}$

$\Rightarrow (n, k) = (n, n-k)$

$\Rightarrow k = n - k$

$\Rightarrow \frac{k}{n} = \frac{1}{2}$

$\Rightarrow n = 2k$

$\therefore$ Rate: $\frac{k}{n} = 0.5$

$\therefore$ The block length is always even

**Problem:** Consider a Linear code with codewords $\{0000, 1010, 0101, 1111\}$. Find the dual of the code & show that the given code is self dual

**Sol:** $C \sim (n, K)$ . As no. of codewords $= 4 = 2^2 = 2^k$

$\Rightarrow K = 2$

$\therefore C \sim (4, 2)$

$C^{\perp} \sim (n, n-k)$

$\therefore C^{\perp} \sim (4, 2)$

$$G_1 = \left[ I_{2\times 2} : P_{2\times 2} \right] = \left[\begin{array}{cc:cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right]_{2\times 4}$$

$$H = \left[ P^T_{2\times 2} : I_{2\times 2} \right] = \left[\begin{array}{cc:cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right] = G_1^{\perp}$$

---

**Problem:** A code 'C' consists of all binary sequence of length '6' & weight '3'.

a) Is this code a linear block code?

b) What is the rate of this code & minimum distance of code & minimum weight of this code?

(c) This code used for error detection, how many errors it can detect?

(d) This code used on BSC with crossover probability 'p'

What is the probability that an undetectable error occurs?

Sol: 011100
101010
⋮
111000
} ${}^6C_3 = 20$ codewords

(a) Given code is a Non-Linear code,
as all zero codeword is not a codeword
sum of two codewords is not belonging to the code.

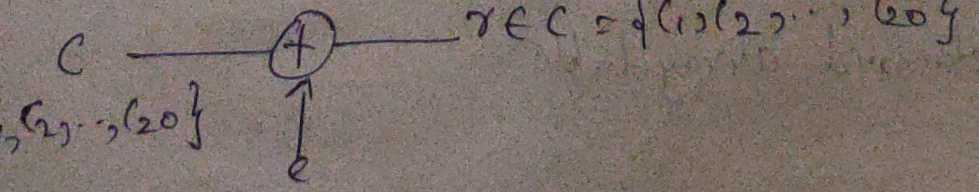
(b) Rate: $R = \frac{k}{n} = \frac{\log_2 20}{6} = 0.72$

(b) $d_{min} = 2 \Rightarrow$ this code can detect upto 1 error.

(c)

$w^*_{min} = 3$

(d) The probability of undetected error is the probability of receiving another codeword.




Let $c_1$ is transmitted, $c_1 = 111000$

$C_1 = 111000$ , $C_2 = 011100$

$d(C_1, C_2) = 2 \Rightarrow P_e = p^2(1-p)^4$

→ 9 codewords are at a distance of 2 from $C_1$

→ 9 codewords are at a distance of 4 from $C_1$

→ 1 codeword is at a distance of 6 from $C_1$

$\therefore P_e = 9p^2(1-p)^4 + 9p^4(1-p)^2 + 1p^6$

---

Problem: The Generator matrix for a code (6,3)

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}_{3\times 6}$$

(a) Find G in systematic form

(b) Find Dual codewords of this code.

(c) Form the Standard Array (decoding) for this code.

(d) How many codewords are there of weight 0, 1, 2, 3, 4, 5, 6.

(e) Find the codeword with 101 as data symbol.

(f) Decode the received codeword 1110001 from the standard array table

from $C_1$

from $C_1$

from $C_1$

p6

ode (6,3)

systematic form

de words of this

for this code.

ht 0, 1, 2, 3, 4, 5, 6.

symbol.

o1 from the

Sol: $(R_1 \rightarrow R_1 + R_3)$

(a) $G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$

$(R_2 \rightarrow R_1 + R_2)$

$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$

($R_1$ below $R_3$)

$\therefore G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

P I

$H = [I : -P^T]$

$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} = G_1^{\perp}$

(b) $C^{\perp} = \{ 000000, \underset{R_1}{100101}, \underset{R_2}{010011}, \underset{R_1+R_2}{110110}, \underset{R_2+R_3}{011101}, \underset{R_1+R_2+R_3}{111000}, \underset{R_3}{001110}, \underset{R_1+R_3}{101011} \}$

→ Dual of the code is Linear combination of rows of H or $G^{\perp}$

→ $C = \{000000, 101011, 011101, 110110, 011010, 110001, 000111, 101100\}$

(c)

| | 000000 | 101011 | . . . | 101100 |
|---|---|---|---|---|
| # No. of coset leaders $= 2^{n-k} = 2^{6-3} = 8$ | 000001 | | | |
| | 000010 | | | |
| | 000100 | | | |
| | 001000 | | | |
| | 010000 | | | |
| | 100000 | | | |
| | 001001 | | | |

(d)

| weight | No. of codewords |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 0 |
| 3 | 4 |
| 4 | 3 |
| 5 | 0 |
| 6 | 0 |

(e) $C = [$

$G_1 = [$

(f) From

11100

# $G_1 = [$

→ $G_1 = [$

→ By rev

$G_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$

(Reversing

$G_1 = [$

(Reversing

$G_1 = [$

(e) $C = [101]$

$G_1 = [1\ 1\ 0\ 0\ 0\ 1]$

(f) From Standard array table,

111001 can be decoded as 110001

---

# $G_1 = [I : P]$ , $H = [-P^T : I]$

→ $G_1 = [P : I]$ , $H = [I ; -P^T]$

→ By reversing rows and columns.

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(Reversing rows)

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

(Reversing the columns)

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

**Problem:** A (6,3) systematic code encodes the information sequence $X = (x_1, x_2, x_3)$ into $C = (c_1, c_2, c_3, c_4, c_5, c_6)$ such that

$c_4 = c_1 + c_2$, $c_5 = c_2 + c_3$, $c_6 = c_1 + c_3$,

(a) Determine the generator matrix in systematic form.

(b) Find Parity check matrix in systematic form.

(c) Find the minimum distance using parity check matrix.

(d) How many errors is this code capable of correcting

(e) If the received sequence is $r = 100000$, what is the transmitted sequence.

**Sol:** (a) $G_1 = [\, I_{3\times 3} : P_{3\times 3} \,]$

$$[c_1\ c_2\ c_3\ c_4\ c_5\ c_6] = [x_1\ x_2\ x_3]\ G_1$$

$$= [x_1\ x_2\ x_3] \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$$= [\, c_1 \quad c_2 \quad c_3 \quad \underbrace{c_1+c_2}_{c_4} \quad \underbrace{c_2+c_3}_{c_5} \quad \underbrace{c_1+c_3}_{c_6} \,]$$

$$\therefore G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

(b) $H = [P^T : I] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

(c) $d_{min}$ = no. of colomns that are linearly dependent in 'H'.

Linear Dependency : $a_1\bar{v}_1 + a_2\bar{v}_2 + a_3\bar{v}_3 = 0$

• In "H", Colouns 1,2,3 are dependent linearly.

$\therefore d_{min} = 3$

(d) $t = \left[\frac{d_{min}-1}{2}\right] = 1$ , $\therefore$ It can correct upto 1 error.

(e) $r = 100\,000$ can be corrected as $000\,000$

• $S = rH^T = [1\ 0\ 1]$

• $S = eH^T$

$e = 100\,000$

• $C = r - e$

$= 000\,000$

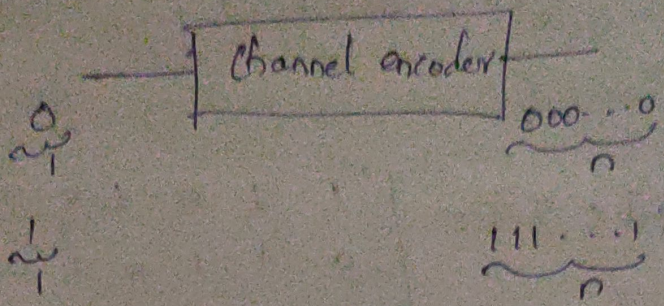
| Error pattern (e) | Syndrome |
|---|---|
| 000000 | 000 |
| 000001 | 001 |
| 000010 | 010 |
| 000100 | 100 |
| 001000 | 011 |
| 010000 | 110 |
| 100000 | 101 |
| 100010 / 001100 | 1001 |

$2^{n-k}$ Syndromes

8 Syndromes

100010 / 001100

## Repetation Code: (n, 1) code




- $C = \{000\cdots0, 111\cdots1\}$ · $d_{min} = n$

- $G = \left[ I_{1\times1} : P_{1\times(n-1)} \right]_{1\times n}$

$$= \left[ 1 : \underbrace{111\cdots1}_{n-1} \right]$$

- $H = \left[ P^T_{(n-1)\times1} : I_{(n-1)\times(n-1)} \right]_{(n-1)\times n}$

$$= \begin{bmatrix} 1 & : & 1\,0\,0\cdots0 \\ 1 & : & 0\,1\,0\cdots0 \\ 1 & : & 0\,0\,1\cdots0 \\ \vdots & & \\ 1 & : & 0\,0\,0\cdots1 \end{bmatrix}$$

**Problem:** Let a (4,3) code defined over GF(3) with

$$G_1 = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 \end{bmatrix}$$

# 4 mod 3 = 1
# 4 mod 3 = 2

$R_3 \to R_3 - R_2 - R_1$ $\qquad$ $R_1 \to R_1 - R_3$

$$G = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{bmatrix} \qquad G = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

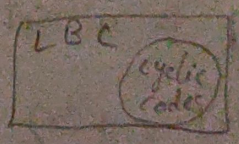
$C_4 \leftrightarrow C_1$ ; $C_1 \leftrightarrow C_2$ ; $C_2 \leftrightarrow C_3$ ; $C_3 \leftrightarrow C_4$

$$G = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}}_{I \quad P}$$

G in Systematic form

---

## Cyclic Codes:




- These are special cases of Linear Block code

→ A Linear code 'C' over GF(2) is called a Cyclic code, if $c = (c_0\, c_1 \cdots c_{n-1}) \in C$

then $c' = (c_{n-1}\, c_0\, c_1 \cdots c_{n-2}) \in C$

Ex: $C = \{0000, 0101, 1010, 1111\}$

$0101 \in C$ $\qquad$ $1111 \in C$

$1010 \in C$