

Cases: ✓ (1) C_1 incurs a single error
 — it can detect & correct
 = the error

✓ (2) C_2 incurs a double error
 — it can detect the error
 & there will be a decoding
error

✓ (3) C_2 incurs a triple error
 — can not detect or correct

Exp. $d_{\min} = 5$



$r_1, c_1, c_2, \dots$

H.W.

$C_{\text{ord}} < \frac{d_{\text{min}}}{2}$

detect $d_{\text{min}} - 1$

Conclusion

(a) If the block code has minimum distance d_{min} then the decoder can detect all error patterns

with $t = d_{\text{min}} - 1$ or fewer errors

is called the error correction limit
detection

(b) the decoder can correct all the error patterns with $t = \frac{d_{\text{min}} - 1}{2}$

error correction
limit.

$$\underline{t} \rightarrow p = \frac{\underline{t}}{2}$$

or lesser errors

H.W.

- Q { ①
②

What happens
or what happens

if $d_{min} = \text{even?}$
to $r \rightarrow \left\lceil \frac{d_{min}-1}{2} \right\rceil$
or $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$

Linear Code.

A (n, k) block code is said to be a linear code if sum/addition of any two codewords is a codeword.



in a code word
 i.e. $c_i, c_j \in C$
 then $c_k = c_i + c_j \in C$

(a)

The all-zero word $(\underbrace{000\dots0}_n)$
 is always a code word.

(b)

if $c_k = c_i + c_j$

$\Rightarrow d(c_i, c_j) = \text{wt}(c_k)$

i.e. the distance b/w two codewords
 is the ~~less~~ weight of the
 sum of the codewords.

(c)

The minimum distance of
 a linear code $d_{\min} = \text{wt}_{\min}$

$C_{\min}$

= the smallest weight of the nonzero codewords.

$r=3$ $(7, 4)$ — ~~Hamming~~ Code has ~~min~~ $d_{\min} = 3$

$r=4$ $(15, 11)$ — Hamming code has $d_{\min} = ?$

Sol. Hamming Code is a linear
code.

Ex. $(n, K) = (7, 4)$

$$\bar{i} = (i_1 \ i_2 \ i_3 \ i_4)$$

$$\bar{c} = (i_1 \ i_2 \ i_3 \ i_4 \ p_1 \ p_2 \ p_3)$$

parity check
equations.

$$p_1 = i_1 + i_2 + i_3$$

$$p_2 = i_2 + i_3 + i_4$$

$$p_3 = i_1 + i_2 + i_4$$

$$(i_1 \ i_2 \ i_3 \ i_4 \ p_1 \ p_2 \ p_3) =$$

$$\begin{pmatrix} i_1 & i_2 & i_3 & i_4 \\ \hline \hline \hline \end{pmatrix}_{4 \times k} \begin{bmatrix} G \\ I_k \\ P \end{bmatrix}_{k \times n}$$

$$\bar{c} = \bar{i} G \leftarrow$$

11.

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right]_{4 \times 7}$$

① generator matrix for the $(7,4)$ Hamming code

② the code words are in systematic form

$$G = [I_4 | P]$$

↑ parity matrix

$$\begin{bmatrix} A_1 & A_2 & \dots & A_n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

$$= x_1 A_1 + x_2 A_2 + \dots + x_n A_n$$

Q.
=

What happens if G is
not of $[k(P)]$ form?

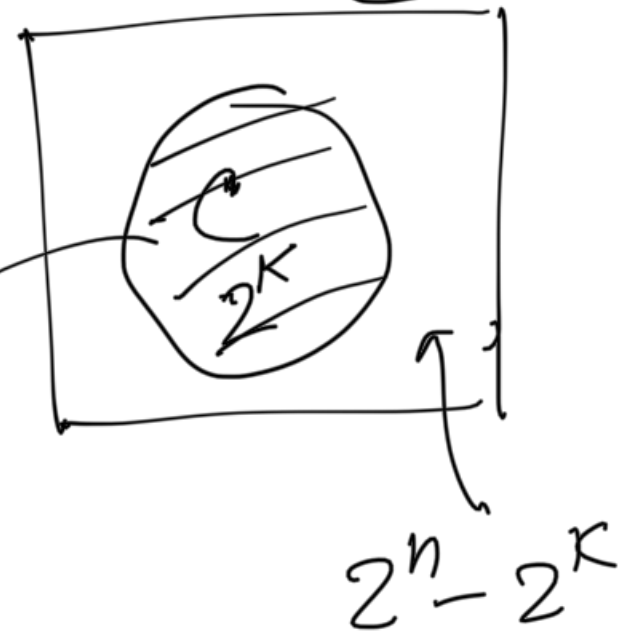
Q. If G is not of
this form then what
modification should we
do to obtain the code
with systematic form?

Linear block code.

lec-20

(n, k) block code
 ↓
 # of information bits
 ↙
 block length

$\mathbb{Z}_2^n$ vector space
 $\{0, 1\}^n$



Linear block code subspace

$d_{min} = wt_{min}$

Generator matrix.

$$\left[\begin{array}{c|c} \bar{I} & \bar{P} \end{array} \right] \equiv \bar{C} = \bar{I} G \leftarrow \text{Linear code.}$$

$$C = \{ \bar{c} \mid c \in \mathcal{C} \}$$

$(7, 4)$ Hamming Code

$$G = [I_4 \mid P]$$

parity matrix

Code in systematic form

$$G = [I_k \mid P_{k \times (n-k)}]$$

If $\underline{G}$ is a generator matrix

Row elementary operations

- (1) Swapping any two rows.
- (2) adding any row with row.

any other ...

Two codes that differ only by permutation of bits are called equivalent.

Every linear code is equivalent to a linear code with systematic form.

Ex 12

$(5,3)$ linear code.

add 2nd row
to the 3rd row

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

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

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

add ~~the~~
 3rd row to 1st row

$$\bar{C} = \vec{I} G$$

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

$$\left[I_K \mid P_{n \times (n-k)} \right]$$

Systematic form

non-systematic code

$$\begin{aligned} C_1 &= (000) \\ C_2 &= (001) \\ C_3 &= (010) \\ C_4 &= (100) \\ C_5 &= (011) \\ C_6 &= (101) \\ C_7 &= (110) \\ C_8 &= (111) \end{aligned}$$

$$\begin{aligned} (00000) \\ (01110) \\ (01001) \\ (10100) \\ (00111) \end{aligned}$$

$$\begin{aligned} (000100) \\ (001111) \\ (010101) \\ (100111) \\ (011110) \end{aligned}$$

$$y = (1 \ 1 \ 1)$$

$$AX = b$$

$$A_1 X = b_1$$

$$[A \mid b] \xrightarrow{R_1} [A_1 \mid b_1] \xrightarrow{R_2} [A_2 \mid b_2]$$

$$A_k X = b_k \quad \left[\begin{array}{ccc|c} 0 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ & & & 1 \end{array} \right] \leftarrow \dots$$

(n, k) - block code

$$G = \left[I_k \mid P_{k \times (n-k)} \right]_{k \times n}$$

parity matrix

Parity-Check matrix.

Unique Error??

$$H^T = \begin{bmatrix} P \\ I \end{bmatrix}$$

$$\bar{b} = \bar{e} H^T$$

$$H = \begin{bmatrix} P^T & I_{n-k} \end{bmatrix}_{(n-k) \times n}$$

transpose of the parity matrix

$$\text{Then } G H^T = \begin{bmatrix} I_{k \times k} & P_{k \times (n-k)} \end{bmatrix} \begin{bmatrix} P_{k \times (n-k)} \\ I_{(n-k) \times (n-k)} \end{bmatrix}$$

$$= P_{k \times (n-k)} + P_{k \times (n-k)}$$

$$= 2P$$

$$= 0$$

Recall,

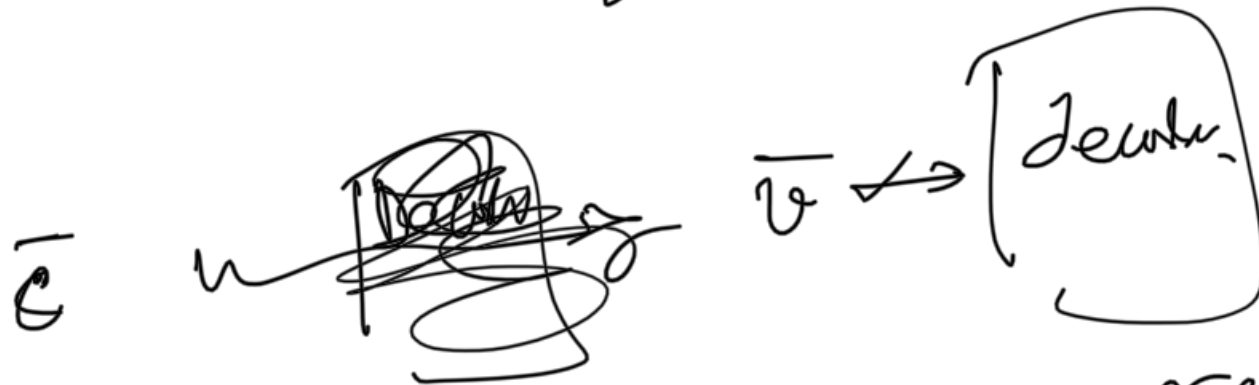
$$\bar{c} = \bar{i} G$$

$$\Rightarrow \bar{c} H^T = \bar{i} G H^T = 0$$

true
for all
codewords

$$\Rightarrow \boxed{\bar{c} H^T = \bar{0}}$$

✓ ✓ $\bar{c}$



Testing
word $\bar{v}$ in a code word:



$\bar{v}$

in

a

code word:



$\hookrightarrow 0$

if/then $\bar{v}$ is a ✓
code word

i.e. $\underline{\overline{v} H^T} = \begin{cases} \neq 0 & \text{if/then } \overline{v} \text{ is} \\ & \text{not a codeword.} \end{cases}$

$$\overline{v} H^T = (\overline{c} + \overline{e}) H^T$$

$$= \underbrace{\overline{c} H^T} + \overline{e} H^T$$

$$\overline{s} = \underbrace{\overline{e} H^T}$$

since $\overline{c} H^T = 0$

$n = 7$
 $k = 4$

Error Syndrome of $\overline{v}$

$$\boxed{\overline{s}_{1 \times (n-k)} = \overline{v}_{1 \times n} H_{n \times (n-k)}^T}$$

If $\overline{v}$ contains no errors then (i.e., $\overline{s} = 0$)

$$\bar{e} = 0)$$

Error:

not all the error patterns
give non zero error syndrome.

H.W.

Create an example.

Algorithm:

① Compute $\bar{e} = \bar{r} H^T$

②

Find the error patterns
corresponding to all the
error syndrome / Error
syndrome table.
i.e. find $\bar{e}$

$$\bar{e} = \bar{e} H^T$$

$$\textcircled{2} \quad \boxed{\bar{c} = \bar{v} + \bar{e}}$$

$$Ax = b$$

$\downarrow$ ~~x_1~~

$$\textcircled{E_1} \quad Ax = E_1 b$$