HAMMING CODES

- perfect codes for correcting single errors
  ↳ minimum possible redundancy
- defined for m bits of redundancy as (n,k) codes where $d_{min} = 3$

$$n = 2^m - 1$$
$$k = 2^m - k - 1$$

Ex: Hamming codes
$(3,1) \dots (7,4) \dots (15,11)$

Def: A perfect binary code $\&$ corrects single errors iff all columns of parity check matrix H are (a) nonzero (b) different

Ex: (3,1) Hamming code

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

Ex: (7,4) Hamming code

$$H = \begin{pmatrix} \overset{7}{0} & \overset{6}{0} & \overset{1}{0} & \overset{5}{1} & \overset{2}{1} & \overset{3}{1} & \overset{4}{1} \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \} n-k$$

$\underbrace{\qquad\qquad\qquad}_{n}$

$H \rightarrow G$ possible for systematic codes:

$$H_{sys} = (P^T \mid I) \quad \Downarrow \quad G_{sys} = (I \mid P)$$

For (7,4)-code we have

$$H_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

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

Decoding:

input $\vec{u}$; code-word $\vec{v} = \vec{u} \cdot G$

(transmission)

$\vec{w}$ received $\quad \vec{w} \cdot H^T = \vec{0}$

a) $\vec{u} = (0101) \rightarrow \vec{v} = (0101010)$

$\vec{v} \cdot H^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\vec{v}$ is a code-word !!

b) single error: $\vec{v} = (0101010) \rightarrow$

$\rightarrow \vec{w} = (0100010)$

$\vec{w} \cdot H^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \vec{s}$ $\vec{w}$ is not a code word, $\vec{s}$ corresponds to the column in H where the error occured

Ex: Why is this possible?

$\vec{w} = \vec{v} + \vec{e}$

Note: vector $\vec{e}$ has all-but-one bits 0

$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T = \underbrace{\vec{v} \cdot H^T}_{\vec{0}} + \vec{e} \cdot H^T$

$\vec{e} \cdot H^T$ copies out the i-th column of H

c) double error: $\vec{w} = (0000010)$

$\vec{w} \cdot H^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ $\vec{w}$ is not a code word, but incorrectly estimates $\vec{v} = (0000000)$

$\Rightarrow d_{min} = 3$, cannot correct double errors !

$H \rightarrow G$ possible for systematic codes:

$H_{sys} = (P^T \mid I)$ $\Rightarrow$ $G_{sys} = (I \mid P)$

For (7,4)-code we have

$$H_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{sys} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Decoding:

input $\vec{u}$; code-word $\vec{v} = \vec{u} \cdot G$

(transmission)

$\vec{w}$ received $\quad \vec{w} \cdot H^T = \vec{0}$

a) $\vec{u} = (0101) \rightarrow \vec{v} = (0101010)$

$$\vec{v} \cdot H^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$ $\vec{v}$ is a code-word !!

b) single error: $\vec{v} = (0101010) \rightarrow$

$\rightarrow \vec{w} = (0100010)$

$$\vec{w} \cdot H^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \vec{s}$$

$\vec{w}$ is not a code word, $\vec{s}$ corresponds to the column in H where the error occured

Ex: Why is this possible?

$\vec{w} = \vec{v} + \vec{e}$

Note: vector $\vec{e}$ has all-but-one bits 0

$$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T = \underbrace{\vec{v} \cdot H^T}_{\vec{0}} + \vec{e} \cdot H^T$$

Copies out the i-th column of H

c) double error: $\vec{w} = (0000010)$

$$\vec{w} \cdot H^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$ $\vec{w}$ is not a code word, but incorrectly estimated $\vec{v} = (0000000)$

$\Rightarrow d_{min} = 3$, cannot correct double errors !

$H \rightarrow G$ possible for systematic codes:

$H_{sys} = (P^T \mid I)$ $\Downarrow$ $G_{sys} = (I \mid P)$

For (7,4)-code we have

$$H_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{sys} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

PROPERTIES

1. if $\vec{w}_1 \in K$ and $\vec{w}_2 \in K$: $\vec{w}_1 \oplus \vec{w}_2 \in K$!
2. $a \in \{0,1\}, \vec{w} \in K$: $a \cdot \vec{w} \in K$
   → $\vec{w} = \vec{0}$ is always a codeword
3. code can be expressed as a set of linear equations

Ex: repetition code (3,1)

000
111

→

$w_0 \oplus w_1 = 0$
$w_1 \oplus w_2 = 0$ ×
$w_0 \oplus w_2 = 0$

not needed!

$$\vec{w} \cdot H^T = \vec{0}$$

$\vec{u} = (u_0, u_1, u_2, \dots, u_{k-1})$

$\vec{w} = (w_0, w_1, \dots, w_{n-1})$

$u_i \in \{0,1\}$
$w_i \in \{0,1\}$

OBTAINING H

$\vec{w} \cdot H^T = \vec{0}$

$\vec{u} \cdot G \cdot H^T = \vec{0} \quad \forall \vec{u}$

⇓

$$G \cdot H^T = \vec{0}$$

SYSTEMATIC CODE

- separated plaintext and ECC blocks
  information parity

Ex: linear (4,2) code

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

$H = ?$

easy for systematic code!

$$G_{sys} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

I (identity) P (parity)

Rule: for $G_{sys} = [\mathbb{I}_{k\times k} \; \mathbb{P}_{k\times(n-k)}]$

the $H_{sys} = [\mathbb{P}^T_{(n-k)\times k} \; \mathbb{I}_{(n-k)\times(n-k)}]$.

$\mathbb{P} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow \mathbb{P}^T = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ this is just coincidence!

$\Rightarrow \boxed{H_{sys} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}}$ $\quad H^T_{sys} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\vec{u} = (01)$

$\vec{w} = \vec{u} \cdot G_{sys} = (0110)$

$\vec{w} \cdot H^T_{sys} = (0110) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ✓

(?) $\vec{w}' = (1110)$

$\vec{w}' \cdot H^T_{sys} = (1110) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ×

Ex: repetition code (3,1)

$G_{sys} = [1 \,|\, 11]$

$\mathbb{P} = [11] \Rightarrow \mathbb{P}^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$H_{sys} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Longleftrightarrow \begin{matrix} w_0 \oplus w_1 = 0 \\ w_0 \oplus w_2 = 0 \end{matrix}$!

SYSTEMATIC CODE

- separated plaintext and ECC blocks
  information parity

Ex: linear (4,2) code

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

$H = ?$

easy for systematic code!

$G_{sys} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

$\mathbb{I}$ (identity) $\quad \mathbb{P}$ (parity)

Rule: for $G_{sys} = [\mathbb{I}_{k\times k} \; \mathbb{P}_{k\times(n-k)}]$

the $H_{sys} = \begin{bmatrix} \mathbb{P}^T_{(n-k)\times k} & \mathbb{I}_{(n-k)\times(n-k)} \end{bmatrix}$.

$\mathbb{P} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow \mathbb{P}^T = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ this is just coincidence!

$\Rightarrow \boxed{H_{sys} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}}$ $\quad H^T_{sys} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\vec{u} = (01)$

$\vec{w} = \vec{u} \cdot G_{sys} = (0110)$

$\vec{w} \cdot H^T_{sys} = (0110) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ✓

(?) $\vec{w}' = (1110)$

$\vec{w}' \cdot H^T_{sys} = (1110) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ×

Ex: repetition code (3,1)

$G_{sys} = [1 \vdots 11]$

$\mathbb{P} = [11] \Rightarrow \mathbb{P}^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$H_{sys} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Longleftrightarrow \begin{matrix} w_0 \oplus w_1 = 0 \\ w_0 \oplus w_2 = 0 \end{matrix}$!

$\vec{w}$ .... error word $\vec{e}$ contains single 1

$\vec{w}' = \vec{w} + \vec{e}$ ... single error

$\vec{w}' \cdot H^T = (\vec{w} + \vec{e}) \cdot H^T = \vec{w} \cdot H^T + \vec{e} \cdot H^T$

$= \vec{0} + \vec{e} \cdot H^T$

"pointer" selects the column of H where e_i is equal to 1

for (7,4)

$H_{sys} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

Ex: Hamming (3,1) ... repetition code

$G_{sys} = [1\ 1\ 1]$

$P = [1\ 1] \Rightarrow P^T = \begin{bmatrix}1\\1\end{bmatrix}$

$H_{sys} = \begin{bmatrix}1&1&0\\1&0&1\end{bmatrix}$

$\vec{u} = (000)$, $\vec{e} = (001)$ $\Big\}\ u' = (001)$

$u' \cdot H^T = (001) \cdot \begin{bmatrix}1&1\\1&0\\0&1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$

$u' \cdot H^T = (101) \cdot \begin{bmatrix}1&1\\1&0\\0&1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$

$n = 2^m - 1$

HAMMING CODES

Construction:

a) from H (7,4)

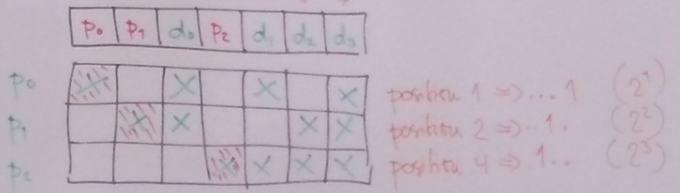
$$H = \underbrace{\begin{bmatrix}1&2&3&4&5&6&7\\0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}}_{n \text{ columns}} \Big\}\ m \text{ rows}$$

- columns are distinct
- represent numbers from 1 to n

$$H_{sys} = \begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}$$

b) using parity bit assignment
non-systematic code
construct a parity bit assignment and copy it to systematic G afterwards

	p_2	p_1	p_0
1	...	0	0	1
2	...	0	1	0
3	...	0	1	1
4	...	1	0	0
5	...	1	0	1
6	...	1	1	0
7	...	1	1	1



$$G = \underbrace{\begin{bmatrix}1&1&1&0&0&0&0\\1&0&0&1&1&0&0\\0&1&0&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}}_{n} \Big\}\ k$$

$\vec{u} \cdot G = \vec{v}$

$\Rightarrow$
$p_0 = d_0 \oplus d_1 \oplus d_3$
$p_1 = d_0 \oplus d_2 \oplus d_3$
$p_2 = d_1 \oplus d_2 \oplus d_3$