# 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 to correct 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

$$H = \underbrace{\begin{array}{ccccccc} 7 & 6 & 1 & 5 & 2 & 3 & 4 \\ \end{array}}_{} \left.\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}\right\} n-k$$

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

$H \rightarrow G$ possible for systematic codes:

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

$$\Downarrow$$

$$G_{sys} = (I \mid P)$$

For (7,4)-code we have

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

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

## Decoding:

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

} (transmission)

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

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

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

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

$\to \vec{w} = (010\boxed{0}010)$

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

$$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T = \underbrace{\vec{v} \cdot H^T}_{\vec{0}} + \underbrace{\vec{e} \cdot H^T}_{\text{copies out the } i\text{-th column of } H}$$

c) double error: $\vec{w} = (0\boxed{0}0\boxed{0}010)$

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

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

## $H \to G$ possible for systematic codes:

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

$$\Downarrow$$

$$G_{sys} = (I \mid P)$$

For (7,4)-code we have

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

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

## Decoding:

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

(transmission)

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

a) $\vec{u} = (0101) \to \vec{v} = (0101\,010)$

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

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

$\to \vec{w} = (010\boxed{0}010)$

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

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

## Ex: Why is this possible?

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

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

$$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T = \underbrace{\vec{v} \cdot H^T}_{\vec{0}} + \underbrace{\vec{e} \cdot H^T}_{\text{copies out the } i\text{-th column of } H}$$

c) double error: $\vec{w} = (0\boxed{0}0\boxed{0}010)$

$$\vec{w} \cdot H^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$\vec{w}$ is not a code word, but incorrectly estimates

$\vec{v} = (0000000)$

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

$H \to G$ 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 $\vec{w}_1 \in \mathbb{K}$ and $\vec{w}_2 \in \mathbb{K}$ : $\vec{w}_1 \oplus w_2 \in \mathbb{K}$!

② $a \in \{0,1\}$, $\vec{w} \in \mathbb{K}$ : $a \cdot \vec{w} \in \mathbb{K}$

→ $\vec{w} = \vec{0}$ 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!

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

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

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

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

## OBTAINING H

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

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

⇓

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

## 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!

$$G_{sys} = \left[\begin{array}{cc:cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right]$$

I (identity) P (parity)

## 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!

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

$I$ (identity)  $P$ (parity)

Rule: For $G_{sys} = \begin{bmatrix} I_{k \times k} & P_{k \times (n-k)} \end{bmatrix}$

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

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

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

$\vec{u} = (01)$

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

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

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

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

Ex: repetition code (3,1)

$$G_{sys} = \left[\begin{array}{c|cc} 1 & 1 & 1 \end{array}\right]$$

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

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

**Rule:** For $G_{sys} = \left[ I_{k\times k} \quad P_{k\times(n-k)} \right]$

the $H_{sys} = \left[ P^T_{(n-k)\times k} \quad I_{(n-k)\times(n-k)} \right]$.

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

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

$\vec{u} = (01)$

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

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

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

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

Ex: repetition code (3,1)

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

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

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

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

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

$$\vec{w}' \cdot H^T = (\vec{w} + \vec{e}) \cdot H^T = \vec{w} \cdot H^T + \vec{e} \cdot H^T$$
$$= \vec{0} + \underset{\text{„pointer"}}{\vec{e}} \cdot H^T$$

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

for (7,4)

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