Example. Hamming $[7,4]$-code. $\mathcal{C}$.

message: 4 bits $\vec{v} \in \mathbb{F}_2^4$

codewords: 7 bits $\vec{v}G \in \mathbb{F}_2^7$

$\Big\}$ $\mathcal{C}$ has dim 4.

$$G = \begin{array}{c} \overbrace{}^{I_4}\ \overbrace{}^{P} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array} \begin{array}{l} \vec{r}_1 \\ \vec{r}_2 \\ \vec{r}_3 \\ \vec{r}_4 \end{array}$$

generating matrix $G = [I_4\ P]$

Define "parity check matrix"

$$H = [P^T\ I_3]$$

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

$$H^T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{bmatrix} P \\ I_3 \end{bmatrix}$$

Note: $\vec{r}_1 H^T = (1000110)\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (000)$

In fact $\vec{r}_i H^T = (000)$

Fact: $\boxed{\mathcal{C} = \ker_L (H^T)}$ ← left

(the purpose of H^T)

Pf. Check $\vec{r}_i H^T = (000)$. So $\mathcal{C} \leq \ker(H^T)$.

It suffices to show $\ker(H^T)$ has dim 4.

$H^T : \mathbb{F}_2^7 \to \mathbb{F}_2^3$

But image = rowspace includes (100), (010) & (001),

So it has dim 3.

By Rank-Nullity Thm, kernel has dim 4. $\square$

Moral: H^T checks if something is a codeword. ie. $\vec{v}H^T = (000) \iff \vec{v} \in \mathcal{C}$.

More is true:

"syndrome"

$(1000000)H^T = (110) = 1^{st}$ row of H^T ie. detects "error in 1^{st} position".

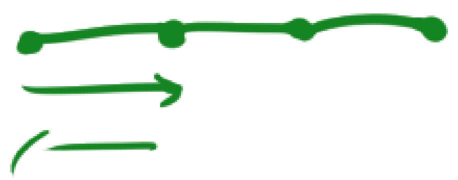
$(0100\ldots0)H^T = (101) = 2^{nd}$ row of H^T ie. " " 2^{nd} "

(key idea: $(\text{codeword} + \text{error})H^T = \text{error}\,H^T$)

So the received message can be corrected if there's one error.

Basic Stats of this code:

- binary: $q = 2$
- length: $n = 7$
- codewords: $M = 2^4$
- minimum distance: $d = d(\mathcal{C}) = 3$
- Can $\begin{cases} \text{detect } 2 \text{ errors} \\ \text{correct } 1 \text{ error} \end{cases}$
- code rate: $R = \dfrac{\log_q M}{n} = \dfrac{\log_2(2^4)}{7} = \dfrac{4}{7}$



This is a $(7, 2^4, 3)$-code

or $[7, 4, 3]$-code

or $[7, 4]$-code

Minimum Distance of a Linear Code

Def^n The Hamming weight of $\vec{v}$ is $wt(\vec{v}) = d(\vec{v}, \vec{0})$.
= how many entries are non-zero.

Prop. Let $\mathcal{C}$ be a linear code.
Then $d(C) = \min\{wt(\vec{u}) : \vec{u} \neq 0, \vec{u} \in \mathcal{C}\}$

In our example of $[7,4]$, the smallest Hamming wt. is 3.

Proof.
$$d(\vec{u}, \vec{0}) = wt(\vec{u}).$$
$$d(\vec{u}-\vec{v}, \vec{0}) = wt(\vec{u}-\vec{v})$$
$$d(\vec{u}, \vec{v}) = d(\vec{u}-\vec{v}, \vec{0})$$

So
$$\begin{aligned} d(C) &= \min\{d(\vec{u},\vec{v}) : \vec{u},\vec{v} \in \mathcal{C}\} \\ &= \min\{wt(\vec{u}-\vec{v}) : \vec{u},\vec{v} \in \mathcal{C}\} \\ &= \min\{wt(\vec{w}) : \vec{w} \in \mathcal{C}\} \end{aligned}$$

since $\{\vec{u}-\vec{v} : \vec{u},\vec{v} \in \mathcal{C}\} = \{\vec{w} : \vec{w} \in \mathcal{C}\}$ $\boxtimes$

Linear Codes in General

$\mathcal{C}$ $[n,k]$-linear code = k-dim^{l} subspace of $\mathbb{F}^n$
= span of k linearly indep vec.'s
= span of rows of $k \times n$ matrix.

G = "generating matrix" rank k, $k \times n$.

$\mathcal{C}$ = rowspace of G.

We call G <u>systematic</u> if $G = [\underbrace{I_k}_{\text{information symbols}} \ \overbrace{P}^{\text{check symbols}}]$

<u>Idea</u>: ① can do row/col operations to get this
② then 1^{st} k bits are the "message".

<u>Def^n</u> H is a <u>parity check matrix</u> for $\mathcal{C}$ if the left-kernel of H^T, i.e.
$\{\vec{v} \in \mathbb{F}^n : \vec{v} H^T = \vec{0}\}$
<u>is</u> the code $\mathcal{C}$.

Theorem. $H = [-P^T \; I_{n-k}]$ is a parity check matrix for the systematic code generated by $G = [I_k \; P]$.

Pf. Write $v_1, \ldots, v_k$ for rows of G.

$$v_i = (0, \ldots, 0, \underset{i^{th}}{1}, 0, \ldots, 0, p_{i,1}, \ldots, p_{i,n-k})$$

Then $v_i H^T = \left(v_i \cdot (j^{th} \text{ col of } H^T)\right)_j$

$$j^{th} \text{ col of } H^T = (-p_{1,j}, \ldots, -p_{n-k,j}, 0, \ldots, 0, \underset{n-k+j \text{ pos.}}{1}, 0 \ldots 0)$$

So $v_i \cdot (j^{th} \text{ col of } H^T) = -p_{i,j} + p_{i,j} = 0$.

So $\mathcal{C} \subseteq \ker H^T$.

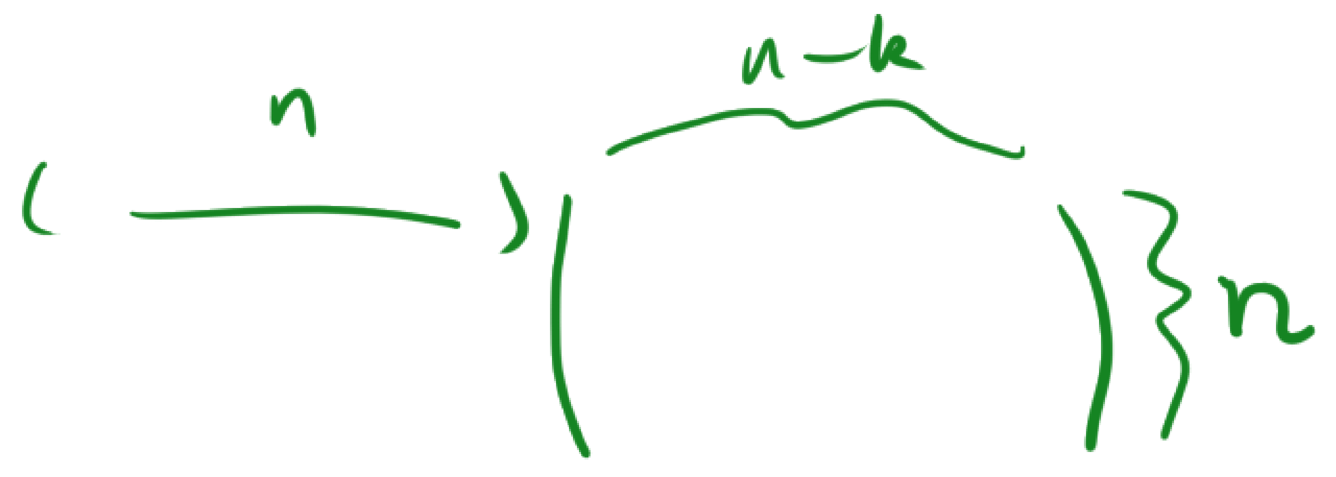
But $\mathcal{C}$ has dim k and so does $\ker H^T$ (since H^T has rank $n-k$).

So $\mathcal{C} = \ker H^T$. $\blacksquare$

Def^n H is a parity check matrix for $\mathcal{C}$ if the left-kernel of H^T, i.e.

$$\{\vec{v} \in \mathbb{F}^n : \vec{v} H^T = \vec{0}\}$$

is the code $\mathcal{C}$.



$$\mathbb{F}^n \longrightarrow \mathbb{F}^{n-k}$$

Cosets of a Code

Def^n. If $\mathcal{C}$ is a linear code, and $\vec{u} \in \mathbb{F}^n$ (length n)

then $u + \mathcal{C} = \{ u + c : c \in \mathcal{C} \}$

is a <u>coset</u> of $\mathcal{C}$

$$\mathcal{C} \xrightarrow{\cdot H^T} \vec{0}$$

$$u_1 + \mathcal{C} \xrightarrow{\cdot H^T} u_1 H^T$$