Basic Parameters

code $\mathcal{C}$ $\begin{cases} \text{length } n \\ M \quad \# \text{ of codewords} \\ d = d(\mathcal{C}) \quad \text{minimum distance} \\ q\text{-ary} \end{cases}$

(n, M, d)-q-ary code

The code information rate / code rate of a q-ary code is (efficiency)

$$R = \frac{\log_q M}{n} = \frac{\text{symbols needed to specify a codeword (info)}}{\text{transmitted symbols per codeword (space)}}$$

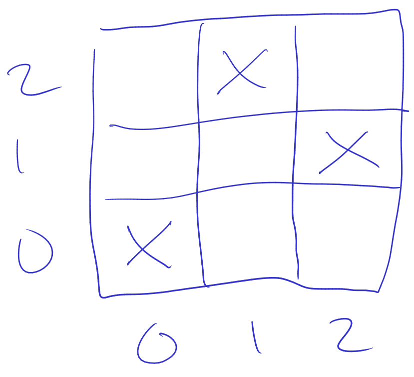
eg. $\{000, 111\}$ is a binary $(3, 2, 3)$-code

w/ $R = \dfrac{\log_2 2}{3} = \dfrac{1}{3}$.

Linear Codes

code = subspace of a vector space

eg. ① $\mathbb{F}_3^2 \supseteq \{(0,0),(1,2),(2,1)\}$



$y = 2x$

$[2,1]$

$(2,3)$

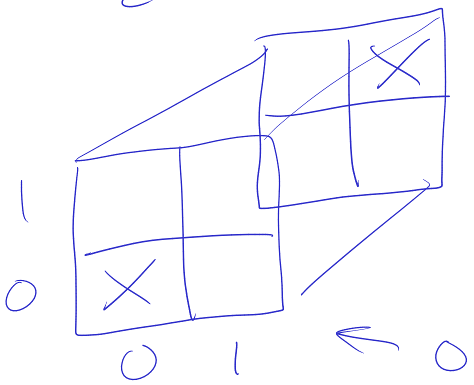
Def^n A linear code of dimension k and length n over $\mathbb{F}$ is a k-dim^l subspace of $\mathbb{F}^n$.

Terminology:

an "$[n,k]$ - code"

or "$[n,k,d]$-code" where $d = d(\mathcal{C})$

② $\mathbb{F}_2^3 \supseteq \{(0,0,0),(1,1,1)\}$



line

$[3,1]$

$(3,2)$

So $[n,k,d]$-code over $\mathbb{F}_q$ is an (n, q^k, d)-code

size of the subspace $= M$

Minimum Distance of a Linear Code

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

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

Pf.

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

Fact:

A vector space is closed under addition, subtraction, scalar multiplication.

General $[n,k]$-linear code

G = generating matrix $k \times n$

$\mathcal{C}$ = rowspace of G

$$G = [\, I_k \quad P \,]$$

information symbols

check symbols

"systematic"

other linear codes could be (hopefully) put in this form

Example. $[7,4]$-code (Hamming) over $\mathbb{F}_2$

$$G = \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}}^{7} \begin{matrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{matrix}$$

message bits

check bits (along for the ride)

rows & all sums of rows = code

eg. message 1101

$r_1 + r_2 + r_4$

codeword

$$\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline \underbrace{1 \quad 1 \quad 0 \quad 1}_{\text{message}} & & & & \underbrace{1 \quad 0 \quad 0}_{\text{check}} & & \end{array}$$

General

Def^n H is a <u>parity check matrix</u> for a code $\mathcal{C}$ if the left kernel of H^T <u>is</u> the code $\mathcal{C}$.

i.e. $\mathcal{C} = \{ \vec{v} \in \mathbb{F}^n : \vec{v} H^T = \vec{0} \}$

Thm. $H = [-P^T \; I_{n-k}]$ is a parity check matrix for $G = [I_k \; P]$

transpose

check symbols

Note: $H^T = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}$

Example

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

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

eg. codeword $= 1101100$

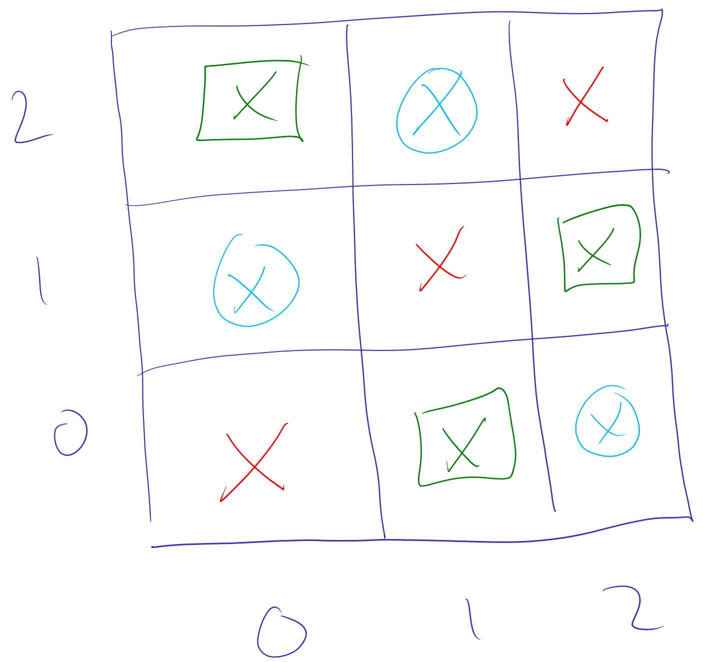
$$vH^T = (1101100) \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \text{sum of } \begin{matrix} 110 \\ 101 \\ 111 \\ 100 \end{matrix} = 000 \; \checkmark$$

1 2 4 5

rows to add

yes codeword

General



Example