Feb 17

1 min Checkin

REMINDERS

- (•) Project groups are now all assigned
- (•) Video topic due (via G form) in ~ 2 weeks (Wed, Mar 1)
- (•) HW 1 is out : Due by 11:59pm Wed next week

RECAP

(•) Linear code $[n,k,d]_q$ is a linear subspace $\subseteq \mathbb{F}_q^n$

(•) Any linear subspace S $k \le n$

① $\dim(S) = k$

② Can be ~~rep~~ "generated" as $S = \{\bar{x} \cdot G \mid \bar{x} \in \mathbb{F}_q^k\}$

$G \in \mathbb{F}_q^{k \times n}$: full rank $\quad \overset{\leftarrow k \rightarrow}{(\;\;)} \; \underset{\leftarrow n \rightarrow}{k\updownarrow(\;\;)}$

$[7,4,3]_2 \xrightarrow{G_3}$ Hamming code $= 4\updownarrow\underbrace{\begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}}_{\leftarrow 7 \rightarrow}$

(3) Also by parity check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ [full rank]

$C = \{\bar{c} \in \mathbb{F}_q^n \mid H\bar{c}^T = \bar{0}\}$

$$H_3 \underset{7-4}{=} 3\updownarrow \underbrace{\overset{\leftarrow n=7 \rightarrow}{\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}}}_{\text{binary repr of integers } 1-7}$$

Plan for today (•) Finish the Theorem for linear subspace (add (4) to above

(•) Implications for linear codes

(•) Distance of linear codes

(•) (General family of) Hamming codes

---

(4) G & H are orthogonal.

$G \cdot ~~F~~ H^T = \bar{0}$

$$k\updownarrow\underset{\leftarrow n \rightarrow}{\begin{pmatrix} & G & \end{pmatrix}} \; n\updownarrow\overset{\leftarrow n-k \rightarrow}{\begin{pmatrix} \\ H \\ \\ \end{pmatrix}} = k\updownarrow\underset{\leftarrow n-k \rightarrow}{\begin{pmatrix} 0 \end{pmatrix}}$$

$H^T[i,j] = H[j,i]$

Lemma: ~~Let~~ G is a generator matrix for S_1

Let H —— parity check —— S_2

If $GH^T = \bar{0} \Rightarrow S_1 = S_2$

Ex. $G_3 \cdot H_3^T = \bar{0}$

$$\begin{pmatrix} \boxed{1\;0\;0\;0\;0\;1\;1} \\ 0\;1\;0\;0\;1\;0\;1 \\ 0\;0\;1\;0\;1\;1\;0 \\ 0\;0\;0\;1\;1\;1\;1 \end{pmatrix} \cdot \begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 0&1&1 \\ 1&0&0 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix} = \begin{pmatrix} \overset{=2 \bmod 2 = 0}{1\cdot 0 + 1\cdot 1 + 1\cdot 1 = 0} & \\ & 0 \end{pmatrix}$$

Recall: linear codes $\equiv$ linear subspaces

Properties:

Prop 1: Any $[n,k]_q$ code can be represented by min $(kn, (n-k)n)$ symbols over $\mathbb{F}_q$

$G \nearrow kn$, $(n-k)n \nwarrow H = $ [illegible] $\leq n^2$

Prop 2: Any $[n,k]_q$ code can be encoded with $O(kn)$ operations over $\mathbb{F}_q$ (given G)

$$\underset{\in \mathbb{F}_q^k}{\bar{x}} \longmapsto \bar{x} \cdot G$$

$$\underbrace{\begin{pmatrix} \ \bar{x}\ \end{pmatrix}}_{\leftarrow k \rightarrow} \ \updownarrow k \underbrace{\begin{pmatrix} & G & \end{pmatrix}}_{\leftarrow n \rightarrow} = C(\bar{x})$$

Prop 3: For any $[n,k]_q$ code, we can do error detection in $O((n-k)n)$ ops over $\mathbb{F}_q$

$\bar{y} \in \mathbb{F}_q^n$ Q: $\bar{y} \overset{?}{\in} C \equiv H\bar{y}^T = \bar{0}$

Solves a special case of HW 1

$$n-k \updownarrow \underbrace{\begin{pmatrix} & H & \end{pmatrix}}_{\leftarrow n \rightarrow} \updownarrow n \begin{pmatrix} y^T \end{pmatrix} \overset{?}{=} \begin{pmatrix} \bar{0} \end{pmatrix} \updownarrow n-k$$

Distance of linear codes

Lemma 1: For any $[n,k,d]_q$ code C

$$d = \min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C}} wt(\bar{c})$$

proved earlier for $[7,4,3]_2$ C_H code

Pf (sketch)

$\leq$: Let $\bar{c}' = \arg\min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C}} wt(\bar{c})$

$$\min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C}} wt(\bar{c}) = wt(\bar{c}') = \Delta(\underset{\in C}{\bar{c}'}, \underset{\in C}{\bar{0}}) \geq d$$

$\geq$: Let $\bar{c}_1 \neq \bar{c}_2 \in C$ $\Delta(\bar{c}_1, \bar{c}_2) = d$ (such $\bar{c}_1, \bar{c}_2$ $\exists$ as $d(C) = d$)

$\Delta(\bar{c}_1, \bar{c}_2) = wt(\bar{c}_1 - \bar{c}_2) = d$

$\left(\underline{\text{Claim:}}\ \bar{c}_1 - \bar{c}_2 \in C \right) \Rightarrow d = wt(\underbrace{\bar{c}_1 - \bar{c}_2}_{\in C}) \geq \min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C}} wt(\bar{c})$

& $\bar{c}_1 - \bar{c}_2 \neq \bar{0}$

Pf: (·) $-\bar{c}_2 \in C$

$-\bar{c}_2 = \underset{\in \mathbb{F}_q}{(-1)} \cdot \underset{\in C}{\bar{c}_2} \xRightarrow{\text{property (ii) of lin. subspaces}} (-1) \cdot \bar{c}_2 \in C$

(·) $\bar{c}_1 - \bar{c}_2 = \underset{\in C}{\bar{c}_1} + \underbrace{(-1) \cdot \bar{c}_2}_{\in C} \xRightarrow{\text{property (i) of lin. subspaces}} \bar{c}_1 + (-1) \cdot \bar{c}_2 \in C$ ∎

<u>Lemma 2:</u> Let C be an $[n,k,d]_q$ code with parity check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ $\Rightarrow$

d = <u>min</u> # of <u>dependent</u> columns in H

$\Rightarrow$ any $(d-1)$ columns of H are linearly independent!

rank $(H) = n-k \Rightarrow$ at most $(n-k)$ columns of H are linearly independent.

$d - 1 \leq n - k \Rightarrow d \leq n - k + 1$ (holds for ALL codes)