Feb 16

REMINDERS

- Both due by 11:59pm tonight:
  - HW 0 (submitting is optional)
  - Group composition (this is mandatory)
- HW 1 should be out by 11:59pm tonight as well
- You need to sign-up for proof reading/volunteer in a lecture before you can submit

---

RECAP: Linear code $[n,k,d]_q$

→ Any linear $[n,k]_q$ code C:

(1) Can be represented as $C = \{\bar{x} \cdot G \mid \bar{x} \in \mathbb{F}_q^k\}$
generator matrix $G \in \mathbb{F}_q^{k \times n}$

$$G_3 = \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}$$

$[7,4,3]_2$ Ham code

(2) Also by parity check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$

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

$$H_3 = \underbrace{\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}}_{\text{binary representation of integers } 1-7}$$

(3) C has $O(kn)$ operation encoding (due to (1))

(4) C has $O((n-k)n)$ —— error detection (due to (2))

Proof readers for today: Blake, Michael

PLAN for today (i) 2 different characterizations of distance of a linear code

(ii) (General family of) Hamming codes

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

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

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

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

$\geq$: Let $\bar{c}_1 \neq \bar{c}_2 \in C$ s.t. $\Delta(\bar{c}_1, \bar{c}_2) = d$

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

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

↳ By scalar mult prop: $(-1) \cdot \bar{c}_2 \in C$, sum of vector property

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

d = min number of linearly dependent # columns in H.

$\Rightarrow$ Any subset of $d-1$ columns of H are linearly independent

$\Rightarrow$ Note since H has rank $n-k \Rightarrow \exists$ some subset of size $n-k$ of cloumns that are linearly independent. Later: Also true for any code.

(~~show later~~ $\Rightarrow d-1 \leq n-k$)

Pf: (i) $d \geq$ min number of linearly dependent columns in H.

Goal: Given d, show a subset of d linearly dependent columns in H.

By Lemma 1, $\exists\ \bar{c} \in C$ s.t $wt(\bar{c}) = d$

$\bar{c} = (c_1, \ldots, c_n)$ $\quad S = \{ i \mid c_i \neq 0 \}$

Since H is a parity-check matrix, $|S| = d$

$$H\bar{c}^T = 0 \qquad \begin{array}{c c} & \overset{\longleftarrow \; n \; \longrightarrow}{} \\ n-k & \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ H_1 & H_2 & \cdots & H_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} \end{array} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \uparrow \\ n-k \\ \downarrow \end{matrix}$$

$$\bar{0} = H\bar{c}^T = c_1H_1 + c_2H_2 + \cdots + c_nH_n = \sum_{i \in S} c_i \cdot H_i$$

$\Rightarrow \{ H_i \mid i \in S \}$ is a set of d linearly dependent columns

(ii) See book for the other direction $\blacksquare$

(General) Hamming code $[2^r-1, 2^r-1-r, 3]_2$ code $\rightarrow C_{H,r}$

C_H from earlier $r=3$ $\qquad r \geq 2$

$$H_r = \begin{array}{c c} & \overset{\longleftarrow \; 2^r-1 \; \longrightarrow}{} \\ \begin{matrix} \uparrow \\ r \\ \downarrow \end{matrix} & \begin{pmatrix} & \boxed{i} & \end{pmatrix} \\ & 1 \leq i \leq 2^r-1 \end{array}$$

binary representation of i

$n-k = r$

Def: The code $C_{H,r}$ is the code whose parity check matrix is H_r.

$$C_{H,r} = \{ \bar{c} \in \{0,1\}^{2^r-1} \mid H_r \cdot \bar{c}^T = 0 \}$$

Claim: $C_{H,r}$ is $[2^r-1, 2^r-1-r]_2$-code

Lem 3: $C_{H,r}$ has distance $= 3$

Pf (sketch) Use Lemma 2 & argue that min # linearly dependent columns in H_r (t) is $= 3$

$\rightarrow$ $(t \geq 3)$ Any two columns in H_r are different

$\Rightarrow$ $\exists$ at least one row where they are different.

$\Rightarrow$ any two columns are linearly independent

$\Rightarrow t \geq 3$

$\rightarrow$ $(t \leq 3)$

$$\underset{1}{\begin{pmatrix}0\\0\\\vdots\\0\\0\\1\end{pmatrix}} + \underset{2}{\begin{pmatrix}0\\0\\\vdots\\0\\1\\0\end{pmatrix}} = \underset{3}{\begin{pmatrix}0\\0\\\vdots\\0\\1\\1\end{pmatrix}}$$

$\Rightarrow$ 1st 3 columns of H_r are linearly dependent.

$C_{H,r}$ is an $[2^r-1,\ 2^r-1-r,\ 3]_2$-code

Hamming bound: $(n,k,3)_2$-code has $k \leq n - \log_2(n+1)$

Note: $n = 2^r-1$ & $k = 2^r-1-r$ for $C_{H,r}$

$$k = 2^r-1-r = n-r = n-\log_2 2^r = n-\log_2(n+1)$$

Def: Perfect code is a code that matches the (generalized) Hamming bound.

Q: What are all the possible (binary) perfect codes?

A: (i) $C_{H,r}$

(ii) Trivial code: All 0s & all 1s are the only 2 codewords

(iii) 2 specific codes due to Golay

AND THAT'S IT!! (provably)