Feb 20

1 Min checkin

REMINDERS ← Do NOT skip!

(•) HW 0 has been graded. (•) HW 1 due 11:59pm Wed

(•) Reminders about HW

- (–) Only four sources are allowed
  - ↳ If you used an unallowed source follow instructions on HW 1 webpage
- (–) Can collaborate in groups of size ≤ 3
  - ↳ Only to the extent of discussing ideas

RECAP

(•) $[n,k,d]_q$ code

- ↳ Can be represented by $\min(kn, (n-k)n)$ $\mathbb{F}_q$ symbols
- ↳ Encoding can be done by $O(kn)$ ops over $\mathbb{F}_q$
- ↳ Error detection ——— $O((n-k)n)$ ———

(•) Lemma 1: For any $[n,k,d]_q$ code C $d = \min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C}} wt(\bar{c})$

(•) Lemma 2: For any $[n,k,d]_q$ code w/ parity check matrix H, $d =$ min # of lin. dependent columns $\Rightarrow d \le n-k+1$

Plan for today

(•) Prove Lemma 2

(•) (General) Hamming code

(•) Perfect codes

(•) Family of codes

Pf of Lem 2: $d \geq$ min # lin. dependent columns of H

Goal: Given C has dist $d \Rightarrow \exists$ d columns that are linearly dependent.

By Lemma 1, $\exists\ \bar{c} \neq \bar{0} \in C$ s.t. $wt(\bar{c}) = d$.

$\bar{c} = (c_1, \dots, c_n)$ $\qquad S = \{i \mid c_i \neq 0\}$ $\qquad$ note: $|S| = d$

Since H is a parity check matrix for C

$$H\bar{c}^T = \bar{0}$$

$$\begin{array}{c} \uparrow \\ n-k \\ \downarrow \end{array} \underbrace{\begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ H_1 & H_2 & \cdots & H_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}}_{\longleftarrow\ n\ \longrightarrow} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \begin{array}{c} \uparrow \\ n-k \\ \downarrow \end{array}$$

$H\bar{c}^T = c_1 H_1 + c_2 H_2 + \cdots + c_n H_n = \bar{0}$

$\bar{0} = \sum_{i=1}^{n} c_i H_i = \sum_{i \in S} c_i H_i$

$\Rightarrow \{H_i \mid i \in S\}$ is a set of linearly dep ✓

$\sum_{i \in S} c_i H_i = 0$ Assume $1 \in S$

$\equiv c_1 H_1 = -\sum_{i \in S\setminus\{1\}} c_i H_i$

$\equiv H_1 = -\frac{1}{c_1} \sum_{i \in S\setminus\{1\}} c_i H_i$

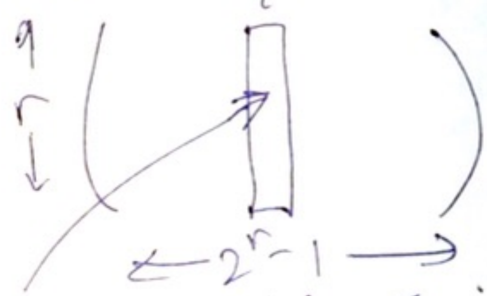
$= \sum_{i \in S\setminus\{1\}} \left(-\frac{c_i}{c_1}\right) H_i$

$(\leq)$ See book. ∎

(General) Hamming code

C_H from earlier $r = 3$ $\quad r \geq 2$ $\quad [\underset{= n}{2^r - 1}, \underset{= k}{2^r - 1 - r}, 3]_2$

$H_r =$



Binary representation of i

$1 \leq i \leq 2^r - 1$

Def: $C_{H,r}$ is the linear code with parity check matrix H_r

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

Claim: $C_{H,r}$ is $[\underset{= n}{2^r - 1}, \underset{= k}{2^r - 1 - r}, 3]_2$ $\quad n - k = r$

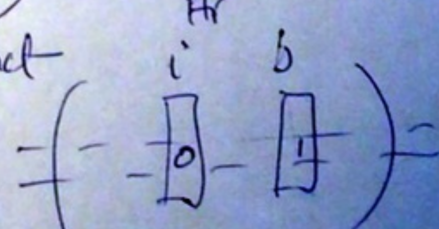
+ H_r has full rank $\quad \underset{\leftarrow n \rightarrow}{n-k\left(H_r\right)}$ $\Rightarrow k = n - r = 2^r - 1 - r$

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

Pf idea: Use Lemma 2 & argue $\underbrace{\text{min \# lin. dependent columns}}_{= t}$ in H_r $= 3$ $\quad (t = 3)$

$\Rightarrow (t \geq 3)$ Any 2 columns are distinct

$\exists$ one row where they differ



$\Rightarrow$ i & j are lin. independent

$\Rightarrow$ any 2 columns are lin. indep.

$\Rightarrow t \geq 3$

$(t \le 3)$ $\begin{pmatrix}0\\ \vdots\\ 0\\ 0\\ 1\end{pmatrix} + \begin{pmatrix}0\\ 1\\ \vdots\\ 0\\ 1\\ 0\end{pmatrix} = \begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 1\end{pmatrix}$ $\Rightarrow$ 1^{st} 3 columns of H_r are linearly dependent.

$\blacksquare$

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

Hamming bound: Any $[n,k,3]_2$ code has

$$k \le n - \log_2(n+1)$$

$C_{H,r}$: $k = 2^r-1-r$

$C_{H,r}$: $2^r-1-\log_2(2^r-1+1)$
$= 2^r-1-\log_2 2^r$
$= 2^r-1-r$

$\Rightarrow C_{H,r}$ is optimal!

Def: A code is perfect if it matches the (generalized) Hamming bound.

Q: What are the possible binary perfect codes?

A: (i) $C_{H,r}$ $\forall r \ge 2$
(ii) Trivial code: All 0s & all 1s
(iii) 2 specific codes due to Golay

AND THAT'S IT! (provably)

Family of codes (Book: Sec 1.8)

(mostly) until now, codes with specific const n, k
eg $C_{\oplus}$ $[5,4,2]_2$

from now on: family of codes $(\underbrace{n,k}_{\text{variables}})_q$

Def (family of code) $C = \{C_i\}_{i \ge 1}$ with C_i $(n_i, k_i, d_i)_q$ code

$n_{i+1} > n_i$ is a family of codes.

<u>Eg</u> $C_{Ham} = \{ C_{H,r} \}_{r \geq 2}$

$n_r = 2^r - 1$
$k_r = 2^r - 1 - r$
$d_r = 3$