FEB 8

1 MIN CHECKIN

REMINDERS

(∘) Make sure you have access to Autolab + Piazza

(∘) HW 0 released later today (~~[illegible]~~ due next Wed)

(∘) Group composition / Team Registration form due next Wed. ↙ ZERO ON ENTIRE PROJECT if you miss this deadline!!

RECAP

(∘) $\overline{u}, \overline{w} \in \Sigma^n$, $\Delta(\overline{u}, \overline{w}) = |\{ i \mid u_i \neq w_i \}|$

(∘) $d(C) = \min_{\overline{c_1} \neq \overline{c_2} \in C} \Delta(\overline{c_1}, \overline{c_2})$ (∘) $d(C_{3,rep}) = 3$, $R(C_{3,rep}) = \frac{1}{3}$

(∘) PROP: Let $d = 2t+1$. $t \geq 1$ C has dist $d \Leftrightarrow C$ is t-e.c.

(∘) Big Q: Optimal tradeoff b/w redundancy & error correction

PLAN for TODAY (∘) Formal version of Big Q

(∘) Hamming code

(∘) (Unlikely but if we have time) Hamming Bound

PROP $\Rightarrow$ (Big Q) Optimal tradeoff between rate & distance?

EQV. Q: Given dist d, what is the largest rate of a code C s.t. $d(C) = d$

Simpler Q: Best rate of for $d = 3$?

By $C_{3,rep}$ $\Rightarrow$ for $d = 3$, best rate $\geq \frac{1}{3}$

Hamming code (C_H) $k = 4$, $q = 2$, $n = 7$

$$C_H(X_1, X_2, X_3, X_4) = \begin{pmatrix} X_1, X_2, X_3, X_4, & X_2 \oplus X_3 \oplus X_4, \\ & X_1 \oplus X_3 \oplus X_4, \\ & X_1 \oplus X_2 \oplus X_4 \end{pmatrix}$$

e.g. $C_H(\overset{X_1}{1}, 0, 0, \overset{X_4}{0}) = (1, 0, 0, 0, 0, 1, 1)$

Claim 1: $d(C_H) = 3$ $R = \frac{4}{7} > \frac{1}{3} \rightarrow$ better than repetition code.

(Later) ~~ff~~ ~~k~~ $d = 3$, $k = 4$, C_H is the best possible

$$\hookrightarrow C_H(X_1, X_2, X_3, X_4) = (X_1\ X_2\ X_3\ X_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Addition is $\oplus$

↳ linear map

Def (Hamming wt) $q \geq 2$, $\bar{u} \in \underbrace{\{0,1,\dots,q-1\}}_{=\Sigma}^{n}$

$wt(\bar{u}) = |\{i \mid u_i \neq 0\}|$ = # non-zero positions in $\bar{u}$

$wt(1,0,0,0,0,1,1) = 3$

Pf of Claim 1
$$\min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C_H}} wt(\bar{c}) = 3 \quad \text{—— (1)}$$

$\bar{0}$ ← all 0s codeword

$$d(C_H) = \min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C_H}} wt(\bar{c}) \quad \text{—— (2)}$$

(1) + (2) ⇒ Claim 1.

Pf (idea): (o) $\min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C_H}} wt(\bar{c}) \leq 3$ ← $(1,0,0,0,0,1,1)$ is a non-zero codeword in C_H.

(•) ≥ 3 $\equiv$ $\forall\, \bar{c} \neq \bar{0} \in C_H$, $wt(\bar{c}) \geq 3$

$\equiv$ $\forall\, \bar{x} \in \{0,1\}^4,\ \bar{x} \neq \bar{0}$ $\quad wt(C_H(\bar{x})) \geq 3$.

Case 1: $wt(\bar{x}) \geq 3$ ⇒ $C_H(\bar{x})$ has ≥ 3 non-zero bits in the 1st 4 bits

Case 2: $wt(\bar{x}) = 2$
Case 3: $wt(\bar{x}) = 1$
$\}$ $wt(C_H(\bar{x})) \geq 3$ by inspection ◻

⇒ (1) is true

Note: (i) $\forall\ \bar{x}, \bar{y} \in \{0,1\}^n$

$$\Delta(\bar{x}, \bar{y}) = wt(\bar{x} + \bar{y})$$

component-wise XOR

$$\begin{array}{r} 1000\ 011 \\ +\ 1100\ 101 \\ \hline 0100\ 110 \end{array}$$

(ii) $C_H(\bar{x}) + C_H(\bar{y}) = C_H(\bar{x} + \bar{y})$ (Pf: Ex)

$$d(C_H) = \min_{\substack{\bar{x} \neq \bar{y} \\ \in \{0,1\}^4}} \Delta(C_H(\bar{x}), C_H(\bar{y}))$$

for (i)
$$= \min_{\substack{\bar{x} \neq \bar{y} \\ \in \{0,1\}^4}} wt(C_H(\bar{x}) + C_H(\bar{y}))$$

$$f_{\min}(\text{ii}) \xrightarrow{} = \min_{\substack{\bar{x} \neq \bar{y} \\ \in \{0,1\}^4}} wt\left(C_H(\bar{x}+\bar{y})\right)$$

$\{\bar{x}+\bar{y} \mid \bar{x} \neq \bar{y} \in \{0,1\}^4\}$

$= \{\bar{z} \mid \bar{z} \neq \bar{0} \in \{0,1\}^4\}$

$$= \min_{\substack{\bar{z} \neq \bar{0} \\ \bar{z} \in \{0,1\}^4}} wt\left(c_H(\bar{z})\right)$$

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

C_H: $k=4$, $d=3$, $n=7$

Hamming bound: special case show if $k=4$, $d=3$, $n \geq 7$