Feb 9

REMINDERS:

(•) Log on to Autolab

(•) Email me if you want to sign up for proofreading

RECAP:

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

(•) $d(C) = \min_{\bar{c}_1 \neq \bar{c}_2 \in C} \Delta(\bar{c}_1, \bar{c}_2)$

(•) PROP: Let $d = 2t+1$. C has distance d iff it is t-error correcting

(•) Big Q: What is the largest possible rate for code with distance d?

(•) Smaller Q: Above ↑ for $d=3$

(•) $R \geq \frac{1}{3}$ for $d=3$ [by $C_{3,rep}$]

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

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

↳ Alternate view:

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

Addition: $\oplus$

Mult: AND

$R(C_H) = \frac{4}{7} > \frac{1}{3}$

(•) Claim 1: $d(C_H) = 3$

(•) Def (Hamming wt) $\bar{u} \in \{0, 1, \ldots, q-1\}^n$, $wt(\bar{u}) = |\{i \mid u_i \neq 0\}|$

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

PLAN FOR TODAY: (•) Prove Claim 1

(•) Argue that C_H is "best possible" (for $k=4$)

(•) Proof readers: Kevin, Mihir

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 zeros vector

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

Note: (1) + (2) ⇒ Claim 1.

Pf of (1): (o) $\min_{\substack{\bar{c} \neq \bar{0} \\ \bar{c} \in C_H}} wt(\bar{c}) \le 3$ $\quad (1,0,0,0,0,1,1)$ is a non-zero codeword in C_H

(o) Show $\forall \bar{c} \neq \bar{0} \in C_H$, $wt(\bar{c}) \ge 3$.

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

Case 1: $wt(\bar{x}) \ge 3 \Rightarrow C_H(\bar{x})$ has at least 3 non-zeroes in its first 4 locations ✓

Case 2: $wt(\bar{x}) = 2$ → By inspection, ≥ 1 out of 3 parity bits are 1

Case 3: $wt(\bar{x}) = 1$ → By inspection, ≥ 2 out of 3 parity bits are 1

$\Rightarrow wt(C_H(\bar{x})) \ge 3$ ✓

Note: (i) $\Delta(\bar{x}, \bar{y}) = wt(\bar{x} + \bar{y})$ $\quad \bar{x}, \bar{y} \in \{0,1\}^n$

component wise $\oplus$

$\bar{x} = 1000011$

$\bar{y} = 1100101$

$\bar{x} + \bar{y} = 0100110$

(ii) $C_H(\bar{m}_1) + C_H(\bar{m}_2) = C_H(\bar{m}_1 + \bar{m}_2)$

Pf of (2) $\quad d(C_H) = \min_{\substack{\bar{x} \neq \bar{y} \\ \in \{0,1\}^4}} \Delta(C_H(\bar{x}), C_H(\bar{y}))$

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

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

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

$= \min_{\bar{z} \neq 0 \in \{0,1\}^4} wt(C_H(\bar{z}))$

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

Hamming bound: First non-trivial upper bound on R (or k)

THM: For any binary code $\mathcal{C}$ of block length n, dim k and distance $d = 3 \Rightarrow k \le n - \log_2(n+1)$

Note: $n = 7 \Rightarrow k \le 7 - \log_2 8 = 7 - 3 = 4$. $\Rightarrow C_H$ is best possible for $n = 7$, $d = 3$

Pf of Thm: ~~Lemma 1~~

Def: (Hamming ball) $\bar{x} \in \{0,1\}^n$

$$B(\bar{x}, e) = \{ \bar{y} \in \Sigma^n \mid \Delta(\bar{x}, \bar{y}) \le e \}$$

$$0 \le e \le n$$

Lemma 1: $\forall \ \bar{c}_1 \ne \bar{c}_2 \quad B(\bar{c}_1, 1) \cap B(\bar{c}_2, 1) = \emptyset$

Pf: If not i.e. $\bar{y} \in B(\bar{c}_1, 1)$, $\bar{y} \in B(\bar{c}_2, 1)$

$$\Rightarrow \Delta(\bar{y}, c_1) \le 1 \quad \Delta(\bar{y}, \bar{c}_2) \le 1$$

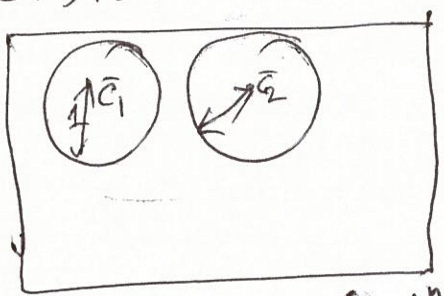
$$\Delta(\bar{c}_1, \bar{c}_2) \le \Delta(\bar{y}, \bar{c}_1) + \Delta(\bar{y}, \bar{c}_2) \le 1 + 1 = 2 \ \times$$

contradicts the assumption that C has $d=3$.

Lemma 2: $\forall \ \bar{x} \in \{0,1\}^n$

$$|B(\bar{x}, 1)| = n+1$$

Lemma 1 $\Rightarrow$



Note: $\bigcup_{\bar{c} \in C} B(\bar{c}, 1) \subseteq \{0,1\}^n$

$$\Rightarrow \left| \bigcup_{\bar{c} \in C} B(\bar{c}, 1) \right| \le 2^n \quad (*)$$

OTOH:

$$\left| \bigcup_{\bar{c} \in C} B(\bar{c}, 1) \right| \underset{\text{Lemma 1}}{=} \sum_{\bar{c} \in C} |B(\bar{c}, 1)| = \sum_{\bar{c} \in C} (n+1)$$

$$= |C| \cdot (n+1) = 2^k \cdot (n+1) \quad (\#)$$

$(*) + (\#) \Rightarrow$

$$2^k (n+1) \le 2^n \Rightarrow 2^k \le \frac{2^n}{n+1}$$

$$\Rightarrow k \le n - \log_2(n+1) \quad \blacksquare$$