February 7, 2019

## REMINDERS:

(•) Register on piazza

(•) Logon to AutoLab.

---

**RECAP:** (•) Code: $C \subseteq \Sigma^n$ $n$: blocklength

$q = |\Sigma|$ rate $R = \frac{k}{n}$

(•) $k = \log_q |C|$

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

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

**PROP:** The following statements are equivalent for a code $C$.

(1) $C$ has distance $d \geq 2$

(2) ($d$ is odd) $C$ is $\frac{d-1}{2}$ - error ~~correctable~~ correcting

(3) $C$ is $(d-1)$ error detecting.

---

Showed last time: (1) $\Rightarrow$ (2)

---

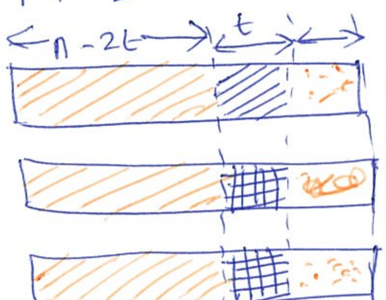
Proof reading volunteer? Due by noon on Tue.

---

Show: $\neg(1) \Rightarrow \neg(2)$ $d = 2t+1$

$C$ has dist $\leq d-1 = 2t$ (assume $d(C) = 2t$) worst-case scenario

$\Rightarrow \exists\, \bar{c}_1 \neq \bar{c}_2 \in C$ s.t. $\Delta(\bar{c}_1, \bar{c}_2) = 2t$




$\bar{c}_1$

$\bar{c}_2$

$\bar{y}$

In particular,

$\Delta(\bar{y}, \bar{c}_1) = \Delta(\bar{y}, \bar{c}_2) = t$

fix any Decoding function $D$.

Let $\bar{c}' = D(\bar{y})$

Case 1: $\bar{c}' \notin \{\bar{c}_1, \bar{c}_2\} \Rightarrow$ incorrect decoding

Case 2: $\bar{c}' = \bar{c}_2 \Rightarrow$ when $\bar{c}_1 \rightarrow \bar{y}$ "

Case 3: $\bar{c}' = \bar{c}_1 \Rightarrow$ incorrect decoding $\bar{c}_2 \rightarrow \bar{y}$.

**Big Q:** What is the largest possible rate $R$ of a code $C$ with distance $d$?

---

for $d = 3$, $R \geq \frac{1}{3}$ is possible (due to (3, rep))

Small(er) Q: Can we have $R > \frac{1}{3}$ for $d = 3$?

## Hamming Code: $C_H$ $\quad k=4, q=2$

$(x_1, x_2, x_3, x_4) \in \{0,1\}^4$

$$C_H(x_1,x_2,x_3,x_4) = (x_1,x_2,x_3,x_4,\ x_2 \oplus x_3 \oplus x_4,\ x_1 \oplus x_3 \oplus x_4,\ x_1 \oplus x_2 \oplus x_4)$$

$$C_H(1,0,0,0) = (1,0,0,0,0,1,1)$$

### Alternate linear algebra view:

$$(x_1\ x_2\ x_3\ x_4)\begin{pmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{pmatrix}$$

addition is $\oplus$
mult is AND

($C_H$ is a 'linear' code)

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

---

**Claim 1:** $d(C_H) = 3 \Rightarrow$ for $d=3$ can do better than $C_{3,rep}$

**Def** (Hamming wt) $q \geq 2$. $\bar{u} \in \{0,1,\dots,q-1\}^n$

$$wt(u) = |\{i \mid u_i \neq 0\}|$$

**Pf of Claim 1:**

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

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

Note: (1) + (2) $\Rightarrow$ Claim 1.

**Pf of (1):** (i) $\min_{\substack{\bar{c} \neq \bar{0}\\ \in C_H}} wt(\bar{c}) \leq 3$ $\quad$ (as $wt(C_H(1,0,0,0)) = 3$)

(ii) Show $\forall\ \bar{c} \neq \bar{0} \in C_H$, $wt(\bar{c}) \geq 3$

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

**Case 1:** $wt(\bar{x}) \geq 3 \Rightarrow wt\ C_H(\bar{x}) \geq 3$

**Case 2:** $wt(\bar{x}) = 2$ $\quad$ ↑ similar

**Case 3:** $wt(\bar{x}) = 1$. By inspection $\geq 2$ out of 3 parities are 1

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

Do not consider $\bar{x} = \bar{0}$ as $C_H(\bar{x}) = \bar{0}$

Note: (i) $\Delta(\bar{x}, \bar{y}) = wt(\bar{x} + \bar{y})$ ← component-wise $\oplus$

$\in \{0,1\}^7$

$\in \{0,1\}^n$

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

$\bar{m}_1, \bar{m}_2 \in \{0,1\}^4$

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

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

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

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

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

---

Can have $R \geq \frac{4}{7}$ for $d = 3$.

Q1: Can we get $d = 3$ for $R > \frac{4}{7}$? (A: Yes, later...)

Q2: Can we get $d = 3$, $n = 7$ and $k > 4$?

---

Hamming bound — First non-trivial upper bound on $R$ (on $k$)

THM: For every binary code of block length $n$, dim $k$ and $d = 3$

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

Note: if $n = 7$, $\Rightarrow k \leq 7 - \log_2(7+1) = 7 - 3 = 4$. $\Rightarrow$ NO for Q2.

---

Def (Hamming ball): $\bar{x} \in \Sigma^n$

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

---

Pf (of Hamming bound): $\forall \bar{c}_1 \neq \bar{c}_2 \in C$ $\quad B(\bar{c}_1, 1) \cap B(\bar{c}_2, 1) = \phi$

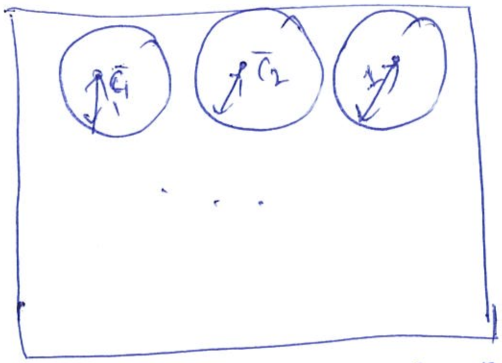
Lemma 1 ↗

(If not $\exists\ \bar{y}$ $\cup \Rightarrow$

$\Delta(\bar{c}_1, \bar{y}) \leq 1$, $\Delta(\bar{c}_2, \bar{y}) \leq 1$

By triang ineq $\Delta(\bar{c}_1, \bar{c}_2) \leq \Delta(\bar{c}_1, \bar{y}) + \Delta(\bar{c}_2, \bar{y}) \leq 2$.

contradict $d(C) = 3$.



$\{0,1\}^n$

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

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

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

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

<u>Otoh:</u>

$$\left| \bigcup_{\bar{c} \in C} B(\bar{c},1) \right| \underset{\uparrow \text{ Lemma 1}}{=} \sum_{\bar{c} \in C} |B(\bar{c},1)| \qquad |C| = 2^k$$

$$= \sum_{\bar{c} \in C} (n+1) = (n+1)\,2^k$$

Above with $(*)$ $\Rightarrow$

$$(n+1)\,2^k \le 2^n \Rightarrow 2^k \le \frac{2^n}{n+1} \Rightarrow k \le n - \log_2(n+1) \qquad \blacksquare$$

---

<u>General Hamming bound</u> A code of block length $n$, dim $k$, dist $d$, ~~alphabet~~ alphabet $\Sigma$

$(n,k,d)_\Sigma$ or $(n,k,d)_q$. $(q = |\Sigma|)$

<u>THM 2:</u> For any $(n,k,d)_q$ code:

$$k \le n - \log_q \left( \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right)$$

<u>Lemma 1':</u> $\forall \bar{c}_1 \neq \bar{c}_2 \in C$ $\quad B\left(\bar{c}_1, \lfloor \frac{d-1}{2} \rfloor\right) \cap B\left(\bar{c}_2, \lfloor \frac{d-1}{2} \rfloor\right) = \emptyset$

<u>Lemma 2':</u> $\forall \bar{x} \in \{0,\ldots,q-1\}^n$

$$|B(\bar{x}, e)| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i$$