Feb 7

REMINDERS:
- (•) Register on piazza
- (•) Log on to Autolab
- (•) Yunus OH:
  - Mon, 1-1:50pm (i)
  - Tue, 1-1:50pm (i)
  - Wed, 12-12:50pm (v)
  - ↳ His OH starts from tomorrow

RECAP: (•) Code $C \subseteq \Sigma^n$ n: block length
- (•) $\dim(C) = k = \log_q |C|$ $q = |\Sigma|$
- (•) rate $R(C) = \frac{k}{n}$
- (•) $\bar{u}, \bar{w} \in \Sigma^n$, Hamming dist $\Delta(\bar{u}, \bar{w}) = |\{i \mid u_i \neq w_i\}|$
- (•) $d(C) = \min_{\bar{c}_1 \neq \bar{c}_2} \Delta(\bar{c}_1, \bar{c}_2)$

PROPOSITION: The following statements are equivalent for any code C
- (1) $d(C) = d \geq 2$ ← (but not $(\frac{d+1}{2})$-error correcting)
- (2) [If d is odd] C is $(\frac{d-1}{2})$-error correcting
- (3) C is $(d-1)$-error detecting (but not d-error detecting)

PLAN for today
(Show)(■) (1) $\Rightarrow$ (2) and $\neg(1) \Rightarrow \neg(2)$
(■) Go back to our overall goal: optimal tradeoff b/w distance rate & error correction

PROOF READER: Maalolan + Andrew (Li) + ~~(NEED ANOTHER VOLUNTEER)~~

Goal 1: (1) $\Rightarrow$ (2)

First "official" algo: Maximum Likelihood decoder (MLD)

$D_{MLD}: \Sigma^n \to C$ ← note: we're allowing output a codeword instead of a message (WLOG as when $d(C) \geq 2$, Bijection between codewords & messages

$D_{MLD}(\bar{y}) = \arg\min_{\bar{c} \in C} \Delta(\bar{y}, \bar{c})$

Pf: (1) $\Rightarrow$ (2) $\quad d = 2t+1 \quad t \geq 1$

$\parallel$

$d(C) \rightarrow$ C has distance $2t+1$ (#)

Goal: Show that C is $\frac{d-1}{2} = t$-error correcting

Need: A decoding algo

↳ Use MLD.

Claim: $\forall\ \bar{m} \in [|C|]$ and any $\bar{y} = Ch(C(\bar{m}))$

s.t $\Delta(\bar{y}, C(\bar{m})) \leq t$,

$D_{MLD}(\bar{y}) = C(\bar{m})$

Pf: For the sake of contradiction assume $\exists\ \bar{m}, \bar{y} = Ch(C($

s.t $\Delta(\bar{y}, C(\bar{m})) \leq t$ ——— (*)

BUT $D_{MLD}(\bar{y}) = C(\bar{m}') \neq C(\bar{m})$

$\bar{c} = C(\bar{m}), \quad \bar{c}' = C(\bar{m}')$

$\Delta(\bar{c}, \bar{c}') \leq \Delta(\bar{c}, \bar{y}) + \Delta(\bar{y}, \bar{c}')$ ← as MLD outputs $\bar{c}'$ instead of $\bar{c}$

Δ-inequality $\leq \Delta(\bar{c}, \bar{y}) + \Delta(\bar{y}, \bar{c})$

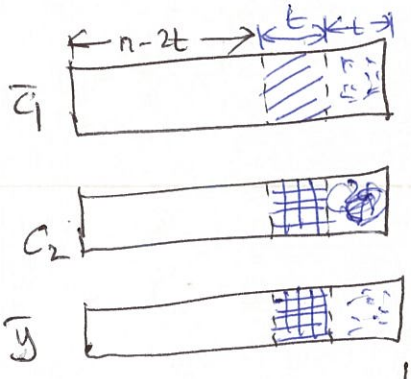
$= 2\Delta(\bar{c}, \bar{y})$

by (*) $\leq 2t \Rightarrow$ contradicts the assumption (#) that $d(C) = 2t+1$ ∎

Pf of ¬(1) $\Rightarrow$ ¬(2) C has distance $< 2t+1$ → Goal: C is NOT t-error correcting

assume $d(C) = 2t \Rightarrow \exists\ \bar{c}_1 \neq \bar{c}_2 \in C$ $\Delta(c_1, c_2) = 2t$

$\Rightarrow \exists\ \bar{y}$ s.t $\Delta(\bar{y}, \bar{c}_1) = t = \Delta(\bar{y}, \bar{c}_2)$



Assume C is t-error correcting.

(##) Fix a decoder D for C that always correctly decodes any received word with $\leq t$ errors

Scenario: $\bar{c}_1$ or $\bar{c}_2$ was transmitted & $\bar{y}$ is received

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

Case 1: $\bar{c}' \notin \{\bar{c}_1, \bar{c}_2\} \Rightarrow$ D is wrong if $\bar{c}_1$ or $\bar{c}_2$ was transmitted

Case 2: $\bar{c}' = \bar{c}_1$: D is wrong if $\bar{c}_2$ was transmitted

Case 3: $\bar{c}' = \bar{c}_2$: ——— $\bar{c}_1$ ———

$\Rightarrow$ contradicts the assumption (##) ∎

PROP ⇒ Big Q! What is the optimal tradeoff between R and distance d of a code?

Reformulate: What is the largest possible rate for a code of distance d?

Smaller Q: Best rate for $d=3$?

$d=3$, $R \geq \frac{1}{3}$ (as $C_{3,rep}$ has dist $=3$ & rate $=\frac{1}{3}$)

Hamming code (C_H) $\quad k=4,\ q=2$

$(x_1, x_2, x_3, x_4) \in \{0,1\}^4 \quad n=7$

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

E.g.

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

Alternate linear algebra view:

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

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

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

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

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

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