Feb 6

1 MIN CHECKIN

REMINDERS

(1) Make sure you can access Autolab + piazza
(2) Ben's OH : W F ; 1 - 1:50pm → OH starts this Wed
(3) Read the book (Recall: It has a notation table!)
(4) Ask questions in class if you do not understand something

RECAP

(•) Code $C \subseteq \Sigma^n$, n: block length. Also $E: [|C|] \to \Sigma^n$
(•) $\dim(C) = k = \log_q |C|$; $q = |\Sigma|$. If k int, $E: \Sigma^k \to \Sigma^n$
(•) rate $R(C) = \frac{k}{n}$
(•) Hamming Distance $\bar{u}, \bar{w} \in \Sigma^n$, $\Delta(\bar{u}, \bar{w}) = |\{i \mid u_i \neq w_i\}|$
(•) t-error correcting ⇐ ∃ decoder that can recover transmitted $\bar{m}$ as long as $\Delta(\bar{y}, E(\bar{m})) \leq t$
(•) t-error detecting
(•) Parity code $C_\oplus(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_3 \oplus x_4)$
$k = 4$, $n = 5$
(•) Repetition code $C_{3,rep}(x_1, x_2, x_3, x_4) = (x_1, x_1, x_1, \ldots, x_4, x_4, x_4)$
$k = 4$, $n = 12$
(•) $C_\oplus$ → 1-error detecting; → NOT 2-e.d.; → NOT 1 e.c. (*)

$C_{3,rep}$ → 1 e.c.; → NOT 2 e.c.; → 2 e.d.; → NOT 3 e.d. } Ex (**)

PLAN FOR TODAY (•) Define distance of a code
(•) Generalize results (*) and (**) to arbitrary codes.

Def (Minimum) Distance: Distance of a code C

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

$\boxed{\text{Claim 1: } d(C_\oplus) = 2}$ $\boxed{\text{Claim 2: } d(C_{3,rep}) = 3}$ ← EX

Pf idea (i) $d(C_\oplus) \geq 2$ Goal: for any $\bar{m}_1 \neq \bar{m}_2 \in \{0,1\}^4$
$$\Delta(C_\oplus(\bar{m}_1), C_\oplus(\bar{m}_2)) \geq 2$$

Case 1: $\Delta(\bar{m}_1, \bar{m}_2) \geq 2 \Rightarrow \Delta(C_{\oplus}(\bar{m}_1), C_{\oplus}(\bar{m}_2)) \geq 2$

b/c the first ~~4 bits~~ $C_{\oplus}(\bar{m}_1) = (\bar{m}_1, b_f)$

$C_{\oplus}(\bar{m}_2) = (\bar{m}_2, \cdot)$

$\Delta \geq 2$

Case 2: $\Delta(\bar{m}_1, \bar{m}_2) = 1$

$\Rightarrow$ parity $(\bar{m}_1) \neq$ parity $(\bar{m}_2)$ $\quad \Delta = 1$

$\Rightarrow \Delta(C_{\oplus}(\bar{m}_1), C_{\oplus}(\bar{m}_2)) = \Delta(\bar{m}_1, \bar{m}_2) + 1 = 2.$

$\quad$ ''1

$\quad$ +1 parity part

(ii) $d(C_{\oplus}) \leq 2 \Longleftarrow$ $\bar{m}_1 = 0000 \rightarrow 0000\underline{0}$, $\bar{m}_2 = 1000 \rightarrow 1000\underline{1}$; $\Delta\begin{pmatrix} 0000\underline{0} \\ 1000\underline{1} \end{pmatrix} = 2$

since I've showed one pair of codewords that differ in 2 locations

PROP: The following statements are equivalent for any code

(1) $d = d(C) \geq 2$

(2) C is $\left(\frac{d-1}{2}\right)$ error correcting $(d: \text{odd})$ $\quad \lfloor \frac{d-1}{2} \rfloor$ general d

↳ but NOT $\left(\frac{d-1}{2}+1\right) = \frac{d+1}{2}$ - e.c

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

↳ but not d- e.d.

Cor: $C_{\oplus}$ $(d(C_{\oplus})=2) \Rightarrow$ 1 - e.d. but not 2 e.d.

$C_{3,rep}$ $(d(C_{3,rep})=3) \Rightarrow$ 1 - e.c. but not 2 e.c.

$\Rightarrow$ 2 - e.d. but not 3 e.d.

Will argue $(1) \Rightarrow (2)$

$\neg(1) \Rightarrow \neg(2)$

(leave the rest of the pf. to the book.)

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

First "official" algo   Maximum Likelihood Decoder

$$D_{MLD} : \Sigma^n \to \Sigma^k \qquad k : \text{int}$$

$$D_{MLD}(\bar{y}) = \arg\min_{\bar{m} \in \Sigma^k} \Delta(\bar{y}, C(\bar{m}))$$

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

$\Rightarrow$ C has dist $(2t+1)$ — (#)

Goal: show C is $\frac{d-1}{2} = t$ - e.c.

Claim: $\forall\, \bar{m} \in \Sigma^k$ & any $\bar{y} \in Ch(C(\bar{m}))$

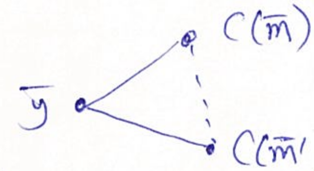
s.t. $\Delta(\bar{y}, C(\bar{m})) \leq t$

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

Pf: By contradiction Assume $\exists\, \bar{m} \in \Sigma^k$, $\bar{y} \in Ch(C(\bar{m}))$

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

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



$$\Delta(C(\bar{m}), C(\bar{m}')) \leq \Delta(C(\bar{m}), \bar{y}) + \Delta(\bar{y}, C(\bar{m}'))$$

Triangle inequality

as MLD chose $\bar{m}'$ over $\bar{m}$ $\rightarrow$

$$\leq \Delta(C(\bar{m}), \bar{y}) + \Delta(\bar{y}, C(\bar{m}))$$

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

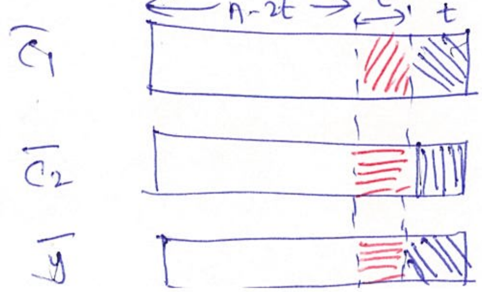
$\leq 2t \rightarrow$ contradicts (#) ∎

Pf of $\neg(1) \Rightarrow \neg(2)$ Assume C has dist $< 2t+1$

$= 2t$

Goal: C is not t - e.c.

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



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

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