February 5
2019

REMINDERS:

Make sure you:

(1) Sign up on piazza + consider filling in the feedback polls
(2) Read the syllabus on course webpage
(3) Make sure you have 4/545 on Autolab

RECAP: Code: $C \subseteq \Sigma^n$ or $C: [M] \longrightarrow \Sigma^n$ where $M = |C|$

(•) $\Sigma \to$ alphabet, $n \to$ block length
(•) $q = |\Sigma|$ (alphabet size)
(•) $\mathrm{Dim}(C) = \log_q |C| = k$
(•) $\mathrm{Rate}(C) = \frac{k}{n}$
(•) $C_{\oplus}(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_3 \oplus x_4)$
(•) $C_{3,rep}(x_1, x_2, x_3, x_4) = (x_1, x_1, x_1, x_2, x_2, x_2, x_3, x_3, x_3, x_4, x_4, x_4)$
(•) High level goal: Optimal tradeoff between $\underbrace{\text{redundancy}}_{\text{``rate''}}$ & error correction?

PROOFREADING → Volunteer for today
→ Make sure you have a section each on → Typos
→ Formatting
→ Suggestions for improvement

ERROR CORRECTION:

Def (Encoding) $C \subseteq \Sigma^n \equiv E: [\,|C|\,] \longrightarrow \Sigma^n$, $[\,|C|\,] \cong \Sigma^k$ (k integer)

→ Need 'reverse' for error-correction

Def (Decoding fn): $D: \Sigma^n \longrightarrow [\,|C|\,] \cong \Sigma^k$

Def (error correction): $C \subseteq \Sigma^n$. Let $t \geq 1$ be an integer.
C is t-error correcting if $\exists$ a decoding fn D s.t
$\forall\, \bar{m} \in [\,|C|\,]$ and any error pattern $\bar{e}$ with $\leq t$ errors,

$$D(C(\bar{m}) + \bar{e}) = \bar{m}.$$

$$\underbrace{\bar{m} \to C(\bar{m})}_{\text{Encoding}} \xrightarrow[\uparrow \bar{e}]{\text{channel}} \underbrace{\bar{y} = C(\bar{m}) + \bar{e} \mapsto \bar{m}}_{\text{Decoder}}$$

received word ($\bar{y}$)

Def (error detection): $C \subseteq \Sigma^n$. $t \geq 1$ integer. C is t-error detecting if $\exists$ a error detection fn: $D : \Sigma^n \to \{0,1\}$

$$D(\bar{y}) = \begin{cases} 0 & \text{if } \bar{y} \in C \\ 1 & \text{o/w} \end{cases}$$

Eg: CRC checksum on TCP/IP

$C_\oplus$: $q=2$, $n=5$, $k=4$, $R=\frac{4}{5}$

$C_{3,rep}$: $q=2$, $n=12$, $k=4$, $R=\frac{1}{3}$

Claim 1: $C_{3,rep}$ is 1-error correcting. $\bar{y}_j \in \{0,1\}^3$ $j \in [4]$

Pf sketch: Consider $\bar{y} \in \{0,1\}^{12} = (\bar{y}_1, \bar{y}_2, \bar{y}_3, \bar{y}_4)$

Set $x_j = \text{Maj}(\bar{y}_j)$

Claim 2: $C_{3,rep}$ is not 2-error correcting.

Pf sketch:

$$111 \xrightarrow{\text{2 errors}} 010$$

$$000 \xrightarrow{\text{1 error}} 010$$

Issue: decoder cannot say for sure if transmitted bit is 0 or 1. (there is NO side information)

So far: → Adversarial noise model (Hamming '50)

→ Stochastic (Eg. BSC_p (Shannon '48)

↳ flip each bit independently w/ prob p.

Noise modeling is an important task (but we'll ignore this)

Note: Can make up noise models that are "better" for certain codes BUT we will not.

PROP 1: $C_\oplus$ 1-error-detecting

Pf idea: Error-detecting fn: parity of all 5 bits

COR: $C_\oplus$ can detect odd # errors

$00000 \leftarrow 11000$

10001

Prop 2: $C_\oplus$ is not 1-error-correcting

10001

10000

$00000 \to 10000$

DISTANCE OF A CODE:

Def (Hamming distance): $\bar{u}, \bar{w} \in \Sigma^n$, $\Delta(\bar{u}, \bar{w})$

→ oblivious to the actual error locations $= |\{i \mid u_i \neq w_i\}|$

$\Delta(111, 010) = 2$ $\quad\quad$ $\Delta(111, 100) = \Delta(111, 001) = 2$

Def ((Minimum) Distance) of a code C

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

Claim: $d(C_\oplus) = 2$

→ ≥ 2:
- $\Delta(\bar{m}_1, \bar{m}_2) \geq 2 \Rightarrow (C_\oplus(m_1), C_\oplus(m_2)) \geq 2$
- $\Delta(\bar{m}_1, \bar{m}_2) = 1 \Rightarrow$ parity $(\bar{m}_1) \neq$ parity $(\bar{m}_2)$ $\Rightarrow \Delta(C_\oplus(\bar{m}_1), C_\oplus(\bar{m}_2)) = 2$.

→ ≤ 2: pick any $\bar{m}_1, \bar{m}_2$ s.t $\Delta(\bar{m}_1, \bar{m}_2) = 1$

$0000 \to 00000$

$1000 \to 10001$

Claim: $d(C_{3,rep}) = 3$

→ ≥ 3: for any $m_1 \neq m_2$, they differ in ≥ 1 bit $\Rightarrow \geq 3$ bits in code

→ ≤ 3: $\bar{m}_1 = 0000$, $\bar{m}_2 = 1000$ $\Rightarrow \Delta(C_{3,rep}(\bar{m}_1), C_{3,rep}(\bar{m}_2)) = 3$

PROPOSITION: The following statements are equivalent for a code C.

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

(2) C is $\frac{d-1}{2}$ - error correcting (d is odd) (not $\frac{d+1}{2}$ ——)

→ d: even $(\frac{d}{2} - 1)$-error correcting but NOT $\frac{d}{2}$-error correcting.

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

$C_\oplus$: 1-error detecting but not 2 error detecting

$C_{3,rep}$: 1 —— correcting —————— 2 —— correcting.

Today: (1) $\equiv$ (2)

First "official" algo:

Maximum Likelihood decoder (MLD)

$D_{MLD}: \Sigma^n \longrightarrow C$ Output the closest codeword

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

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

Show: C is t-error correcting

Claim: $\forall\, \bar{m} \in \Sigma^k$, all error patterns with $\le t$ errors

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

Pf: For sake of contradiction assume $\exists\, \bar{m} \in \Sigma^k$, $\exists\, \bar{e}$ with $\le t$ errors

s.t $D_{MLD}(\bar{y}) \neq C(\bar{m})$ $\Big\} = C(\bar{m}') \neq C(\bar{m})$

$\bar{y} = C(\bar{m}) + \bar{e}$

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

$$\begin{aligned}
\Delta(\bar{c}, \bar{c}') &\overset{\Delta\text{-ineq}}{\le} \Delta(\bar{c}, \bar{y}) + \Delta(\bar{c}', \bar{y}) \\
&\overset{D_{MLD}(\bar{y}) = \bar{c}'}{\le} \Delta(\bar{c}, \bar{y}) + \Delta(\bar{c}, \bar{y}) \\
&= 2\Delta(\bar{c}, \bar{y}) \\
&\le 2t \Rightarrow \text{contradicts the fact that } d(C) = 2t+1 \quad \blacksquare
\end{aligned}$$