Feb 3

1 MIN CHECKIN

REMINDERS

(1) Make sure you can access Autolab + piazza
(2) Read the Syllabus CAREFULLY
(3) There is a notation table in the book. Also read the book!
(4) Ask Questions if you do not understand something.

RECAP Code $C \subseteq \Sigma^n$ or $C : [M] \to \Sigma^n$ where $|C| = M$
← or encoding function E

(•) $\Sigma \to$ alphabet, $n \to$ block length (•) an element of $\bar{c} \in C$ is a codeword
(•) $q = |\Sigma|$ (alphabet size)
(•) $\dim(C) = \log_q |C| \overset{def}{=} k$. If k is an integer $\Rightarrow C : \Sigma^k \to \Sigma^n$
(•) Rate $\doteq \frac{k}{n} = R(C)$
(•) $C_{\oplus}(X_1, X_2, X_3, X_4) = (X_1, X_2, X_3, X_4, X_1 \oplus X_2 \oplus X_3 \oplus X_4)$ ← $k=4, n=5$
(•) $C'_{\oplus}(\underbrace{X_1, X_2}_{\text{message}}) = (X_1, X_2, X_1 \oplus X_2)$ ← $k=2, n=3$

$C'_{\oplus}(0,0) = (0,0,0)$
$C'_{\oplus}(0,1) = (0,1,1)$
$C'_{\oplus}(1,0) = (1,0,1)$
$C'_{\oplus}(1,1) = (1,1,0)$

$C'_{\oplus} = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$

(•) $C_{3,rep}(X_1, X_2, X_3, X_4) = (X_1, X_1, X_1, X_2, X_2, X_2, X_3, X_3, X_3, X_4, X_4, X_4)$ $k=4, n=12$
(•) **High level goal** Optimal tradeoff between $\underset{= \text{rate}}{\text{redundancy}}$ & error correction
(•) $\boxed{\bar{m} \mapsto E(\bar{m})} \longrightarrow \boxed{\text{noisy}} \longrightarrow \boxed{\bar{y} \xrightarrow{?} \bar{m}}$ $\quad \bar{y} = Ch(E(\bar{m}))$ ← received word

message, codeword

Encoding — Ch (NO side info) — Decoding, ie want $D(\bar{y}) = \bar{m}$

PLAN for today (•) Formally define error correction / error detection
(•) Error correcting detecting capabilities of $C_{\oplus}$ and $C_{3,rep}$
(•) Another code parameter: Distance

Want to: define the notion of error correction
Note: Cannot hope to recover from arbitrary error patterns
Goal: Bound the number of errors the channel can introduce.

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

$\Delta(\bar{u}, \bar{w})$ = # locations that they differ in

$= |\{ i \mid u_i \neq w_i \}|$

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

$\rightarrow$ Δ is oblivious to the locations of the error.

Def (Error correction) C is t-error correcting if

$\uparrow$ encoding function E

$\exists$ a decoding function D s.t

$\forall \bar{m} \in [|C|]$ & any $\bar{y} \in Ch(E(\bar{m}))$

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

$\Rightarrow D(\bar{y}) = \bar{m}$.

Claim 1: $C_{3,rep}$ is 1-error correcting.

Pf (sketch): Show a decoder

$\bar{y} \in \{0,1\}^{12}$ & $\exists$ some message (x_1, x_2, x_3, x_4)

s.t $\Delta((y_1, \dots, y_{12}), (x_1, x_1, x_1, \dots, x_4, x_4, x_4)) \leq 1$

This defines the decoder

$(y_1, y_2, y_3) \xrightarrow{\text{MAJ}} x_1$, ~~$(x_1, x_1, x_1)$~~

$(y_4, y_5, y_6) \xrightarrow{\text{maj}} x_2$

$(y_7, y_8, y_9) \xrightarrow{\text{maj}} x_3$

$(y_{10}, y_{11}, y_{12}) \xrightarrow{\text{maj}} x_4$

$\Rightarrow C_{3,rep}$ is 1-e.c.

Claim 2: $C_{3,rep}$ is NOT 2-e.c.

Pf sketch:

$x_1 = 1 \rightarrow 111 \xrightarrow{\text{2 errors}} 010$

$x_1 = 0 \rightarrow 000 \xrightarrow[\text{1 error}]{} 010$

Issue: No way for a fixed decoding function to definitely say $x_1 = 0$ or $x_1 = 1$.

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

$0000\underline{0}$ $1000\underline{1}$

1 error $\searrow$ $\swarrow$ 1 error

10000

Def (Error Detection) $C \subseteq \Sigma^n$ $\quad 1 \leq t \leq n$

C is t-error detecting is $\exists$ an error detector

$\bar{D} : \Sigma^n \to \{0,1\}$ s.t

$$\forall \bar{c} \in C, \quad \forall \bar{y} \in \Sigma^n \text{ s.t } \Delta(\bar{y}, \bar{c}) \leq t$$

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

PROP 2: $C_{\oplus}$ is 1-error detecting

Pf idea: $\bar{y} = (y_1, y_2, y_3, y_4, y_5) \in \{0,1\}^5$

$$\bar{D}(\bar{y}) = \begin{cases} 1 & \text{if } y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5 = 0 \\ 0 & \text{o/w.} \end{cases}$$

→ Can detect any odd number of bit flips

→ cannot detect even

⇒ $C_{\oplus}$ is not 2-e.d.

So far: Adversarial error model (Hamming)

→ Stochastic error models BSC_p (Shannon)

→ Arbitrarily varying model