Feb 4

REMINDERS:

(1) Sign up on piazza
(2) Read (CAREFULLY) syllabus on course webpage
(3) Make sure you can see 4/545 on Autolab
(4) There is a notation table in the book.

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

(o) $\Sigma \to$ alphabet, $n \to$ block length

(o) $q = |\Sigma|$ (alphabet size)

(o) $\dim(C) = \log_q |C| \overset{\text{def}}{=} k$. If k is integer $\Rightarrow C : \Sigma^k \to \Sigma^n$

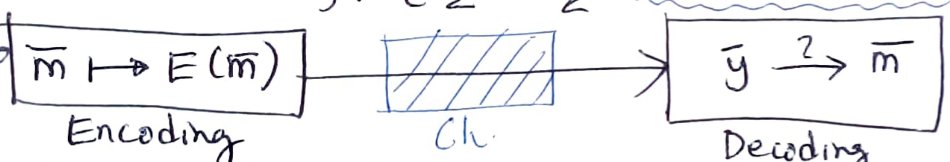
(o) Rate: $R(C) = \frac{k}{n}$

(o) $C_{\oplus}(X_1, X_2, X_3, X_4) = (X_1, X_2, X_3, X_4, X_1 \oplus X_2 \oplus X_3 \oplus X_4)$ — $k=4$, $n=5$

(o) $C_{3,rep}(X_1, X_2, X_3, X_4) = (X_1, X_1, X_1, X_2, X_2, X_2, X_3, X_3, X_3, X_4, X_4, X_4)$ — $k=4$, $n=12$

(o) High level goal: Optimal tradeoff between $\underbrace{\text{redundancy}}_{=\text{rate}}$ & error correction

(o) Hamming distance $\Delta(\bar{u}, \bar{v}) = \#$ positions $\bar{u}$ & $\bar{v}$ differ in, $\bar{u}, \bar{v} \in \Sigma^n$ ← {NO side channel}

(o) 

$\bar{y} = Ch(E(\bar{m}))$

(o) C is t-error correcting if $\exists$ a decoding function $D : \Sigma^n \to [|C|]$ s.t. $\forall\ \bar{m} \in [|C|]$ & any $\bar{y} = Ch(C(\bar{m}))$ s.t. $\Delta(\bar{y}, C(\bar{m})) \le t$, we have $D(\bar{y}) = \bar{m}$ ← note: NO gurantees if $\Delta(\bar{y}, C(\bar{m})) > t$ — divided into two def in the book

---

PROOF READERS: Casey, Joe

Def (Error detection) $C \subseteq \Sigma^n$, $1 \le t \le n$, C is t-error detecting if $\exists$ an error detector $D : \Sigma^n \to \{0,1\}$ s.t. $\forall\ \bar{m} \in [|C|], \forall\ \bar{y} \in \Sigma^n$ s.t. $\Delta(\bar{y}, C(\bar{m})) \le t$

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

Recall: $C_\oplus$: $k=4, n=5, R=4/5$

$C_{3,rep}$: $k=4, n=12, R=1/3$

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

Pf (sketch): Show a decoder $\exists$ that can correct ≤ 1 error.

Consider $\bar{y} \in \{0,1\}^{12}$ $\bar{y} = (\bar{y}_1, \bar{y}_2, \bar{y}_3, \bar{y}_4)$ $\in \{0,1\}^3$

Set $x_j \leftarrow \mathrm{Maj}(\bar{y}_j)$

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

Pf sketch: $x_1 = 1 \to 111 \xrightarrow{2 \text{ errors}} 010$

$x_1 = 0 \to 000 \xrightarrow{1 \text{ error}} 010$

Issue: No way for any decider to definitively say that $x_1 = 0$ or $x_1 = 1$

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

→ Stochastic noise model BSC_p (Shannon '48)

each bit is flipped independently with probability p

→ Arbitrary varying channel.

→ Noise modelling is an important task (which we'll ignore)

Proposition 1: $C_\oplus$ is 1-error detecting

Pf (sketch): $D(y_1, y_2, y_3, y_4, y_5) = y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5$

↳ detects odd # errors

Prop 2: $C_\oplus$ is NOT 2-error detecting code

0000 0 1000 1

0 error → 00000 ← 2 errors

Prop 3: $C_\oplus$ is NOT 1-error ~~detecting~~ correcting

0000 0 1000 1

1 error → 1000 0 ← 1-error

Def ((Minimum) distance) Distance of a code C

$$d(C) = \min_{\bar{c}_1 \neq \bar{c}_2 \in C} \Delta(\bar{c}_1, c_2)$$

$$\| \quad d$$

parity $(0\,0\,0\,0) = 0$

parity $(0\,1\,0\,0) = 1$

Claim 3: $d(C_\oplus) = 2$

Claim 4: $d(C_{3,rep}) = 3 \leftarrow$ (Ex.) Hint: each bit is repeated 3 times.

Pf (sketch):

$d(C_\oplus)$

≥ 2:

$\Delta(\bar{m}_1, \bar{m}_2) \geq 2$

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

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

$\Rightarrow$ parity $(\bar{m}_1) \neq$ parity $(\bar{m}_2)$

$\Rightarrow \Delta(C_\oplus(\bar{m}_1), C_\oplus(\bar{m}_2))$

$= 1 + 1$

$= 2$

≤ 2:

$\bar{m}_1 = 0000 \rightarrow 0000\underline{0}$

$\bar{m}_2 = 1000\bar{0} \rightarrow 1000\underline{1}$

$\Delta = 2$

$\Rightarrow$ min Ham distance between any 2 codewords ≤ 2.

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

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

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

$\hookrightarrow$ NOT $\left(\frac{d+1}{2}\right)$-error correcting

d even: $\left(\frac{d}{2} - 1\right)$ error correcting NOT $\frac{d}{2}$-e.c.

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

$\hookrightarrow$ NOT d-error detecting

By Claim 3: $C_\oplus$ is 1-error detecting but NOT 2-error detecting

By Claim 4: $C_{3,rep}$ is 1-error correcting but NOT 2-error correcting.