Mar 18

REMINDERS

- Mini project 2-pg report due by 11:59pm on Wed, Mar 30
- Please vote on proposed HW grade policy change
- Deadline to sign up for future proof reading: 5pm, Mon Mar 21
- Piazza off for next week (Enjoy your spring break!)

RECAP

- BSC$_p$ → Each of the n transmitted bits independently get flipped w/ prob p $\left(0 \le p \le \frac{1}{2}\right)$
- $\bar{e} \sim BSC_p$ → $\bar{e} \in \{0,1\}^n$ sampled according to BSC$_p$
  → $\Pr_{\bar{e} \sim BSC_p}[wt(\bar{e}) > (p+\gamma)n] \le e^{-\gamma^2 n/2}$ for any $\gamma > 0$ ——— (*)
- **Shannon's Capacity thm for BSC$_p$ (positive part)**

  $\forall\ 0 \le p < \frac{1}{2}$, $0 \le \varepsilon \le \frac{1}{2} - p$, $\exists\ \delta > 0$ s.t following holds for large enough n:

  → $\forall\ k \le \lfloor (1 - H(p+\varepsilon))n \rfloor$, $\exists\ E: \{0,1\}^k \to \{0,1\}^n$, $D: \{0,1\}^n \to \{0,1\}^k$

  s.t $\forall\ \bar{m} \in \{0,1\}^k$, $E_{ERR}^{E}(\bar{m}) \overset{def}{=} \Pr_{\bar{e} \sim BSC_p}[D(E(\bar{m}) + \bar{e}) \ne \bar{m}] \le 2^{-\delta n}$.

- Pf. sketch: → Pick E at random
  → $D = MLD_E$
  - Step 1: Show for fixed $\bar{m} \in \{0,1\}^k$, $\mathbb{E}_E(E_{ERR}^{E}(\bar{m})) \le 2^{-\Omega(n)}$
  - Step 2: Drop half of messages to show $\exists\ E$ s.t $\forall\ \bar{m} \in \{0,1\}^k$ $E_{ERR}^{E}(\bar{m}) \le 2^{-\delta n}$.

PROBABILITY FACTS: (i) Linearity of expectation (ii) Union Bound

(iii) For indep r.v. $\mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$

(iv) $\Pr(X = x) = \sum_y \Pr(X = x \mid Y = y) \cdot \Pr(Y = y)$

PROOF READERS for today: Sai Kiran, Sai Neeraj, Vignesh

Plan for today: Prove +ve part of Shannon's capacity thm for BSC$_p$

Pf of part ① of Shannon's Thm $\bar{e} = (e_1, \ldots, e_n) \sim BSC_p$

fix $\bar{m} \in \{0,1\}^k$ $\bar{y} = E(\bar{m}) + \bar{e}$ $D = MLD_E$

$\mathbb{1}_P = \begin{cases} 1 & \text{if } P \text{ is true} \\ 0 & \text{o/w} \end{cases}$

$$Err^E(\bar{m}) \overset{\text{def}}{=} \Pr_{\bar{e} \sim BSC_p}[D(\bar{y}) \neq \bar{m}]$$

$$= \sum_{\bar{y} \in \{0,1\}^n} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}}$$

($\bar{y}$ was received, $E(\bar{m})$ was transmitted)

$$= \sum_{\bar{y} \in B(E(\bar{m}), (p+\gamma)n)} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}} + \sum_{\bar{y} \notin B(E(\bar{m}), (p+\gamma)n)} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}}$$

$\bar{y} \in B(E(\bar{m}), (p+\gamma)n) \equiv \bar{y} : \Delta(E(\bar{m}), \bar{y}) \leq (p+\gamma)n$

$\bar{y} \notin B(E(\bar{m}), (p+\gamma)n) \equiv \bar{e} = \bar{y} - E(\bar{m})$ has $wt(\bar{e}) > (p+\gamma)n$ by (*)

$\mathbb{1}_{D(\bar{y}) \neq \bar{m}} \leq 1$

$$\leq \sum_{\bar{y} \in B(E(\bar{m}), (p+\gamma)n)} \Pr[\bar{y} \mid E(\bar{m})] + \Pr_{\bar{e} \sim BSC_p}[wt(\bar{e}) > (p+\gamma)n]$$

by (*) $\leq e^{-\gamma^2 n/2}$

$$Err^E(\bar{m}) \leq e^{-\gamma^2 n/2} + \sum_{\bar{y} \in B(E(\bar{m}), (p+\gamma)n)} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}} \quad (B)$$

$$\Rightarrow \mathop{\mathbb{E}}_{E}(Err^E(\bar{m})) \leq e^{-\gamma^2 n/2} + \mathop{\mathbb{E}}_{E}\left(\sum_{\bar{y} \in B} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}}\right)$$

$$= e^{-\gamma^2 n/2} + \sum_{\bar{y} \in B} \mathop{\mathbb{E}}_{E}\left(\Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}}\right)$$

(lin. of $\mathbb{E}$)

($\Pr[\bar{y} \mid E(\bar{m})]$: constant under $\mathbb{E}_E$; only depends on randomness in BSC_p. $\mathbb{1}_{D(\bar{y}) \neq \bar{m}}$: depends only on E + BSC_p)

$$= e^{-\gamma^2 n/2} + \sum_{\bar{y} \in B} \Pr[\bar{y} \mid E(\bar{m})] \mathop{\mathbb{E}}_{E}\left[\mathbb{1}_{D(\bar{y}) \neq \bar{m}}\right]$$

Goal: bound this

Claim 1: $\mathop{\mathbb{E}}_{E}\left[\mathbb{1}_{D(y)\neq \bar{m}}\right] \le 2^{-n(H(p+\varepsilon)-H(p+\gamma))}$

$$\Rightarrow \mathop{\mathbb{E}}_{E}\left(Err^{E}(\bar{m})\right) \le e^{-\gamma^2 n/2} + \sum_{\bar{y}\in B} Pr[\bar{y}\mid E(\bar{m})]\cdot 2^{-n(H(p+\varepsilon)-H(p+\gamma))}$$

$$= e^{-\gamma^2 n/2} + 2^{-n(H(p+\varepsilon)-H(p+\gamma))} \sum_{\bar{y}\in B} Pr[\bar{y}\mid E(\bar{m})]$$

$$\le e^{-\gamma^2 n/2} + 2^{-n(H(p+\varepsilon)-H(p+\gamma))} \sum_{\bar{y}\in\{0,1\}^n} Pr[\bar{y}\mid E(\bar{m})]$$

$$\le e^{-\gamma^2 n/2} + 2^{-n(H(p+\varepsilon)-H(p+\gamma))} \cdot 1$$

if $\gamma = \frac{\varepsilon}{2} > 0$, $\approx \varepsilon^2$

$$\le 2^{-\delta' n}, \text{ where } \delta' = \Theta(\varepsilon^2)$$

$$\sum_{\bar{y}\in\{0,1\}^n} Pr[\bar{y}\mid E(\bar{m})] = \sum_{\bar{e}\in\{0,1\}^n} Pr[\bar{e} \text{ is error pattern}] = 1.$$

$$\Rightarrow \text{For every fixed } \bar{m}\in\{0,1\}^k \quad \mathop{\mathbb{E}}_{E}\left(Err^{E}(\bar{m})\right) \le 2^{-\delta' n}$$

$$\mathop{\mathbb{E}}_{E}(\cdot)\cdot Pr[\bar{m} \text{ was chosen}] \le 2^{-\delta' n} \le 2^{-\delta' n}$$

$$\sum_{\bar{m}\in\{0,1\}^k} \le 2^{-\delta' n} \le Pr[\bar{m} \text{ was chosen}]$$

By prob method $\Rightarrow \forall \bar{m}\in\{0,1\}^k, \exists E$ s.t. $Err^{E}(\bar{m}) \le 2^{-\delta' n}$

Goal show: $\exists E, \forall \bar{m}, \ldots$

$$\Rightarrow \mathop{\mathbb{E}}_{\bar{m}\in\{0,1\}^k}\left(\mathop{\mathbb{E}}_{E}\left(Err^{E}(\bar{m})\right)\right) \le 2^{-\delta' n}$$

($\bar{m}$ uniform)

$$\Rightarrow \mathop{\mathbb{E}}_{E}\left(\mathop{\mathbb{E}}_{\bar{m}\in\{0,1\}^k} Err^{E}(\bar{m})\right) \le 2^{-\delta' n}$$

(since choices for E & $\bar{m}$ are indep.)

$$\Rightarrow \exists E \text{ s.t. } \mathop{\mathbb{E}}_{\bar{m}\in\{0,1\}^k} Err^{E}(\bar{m}) \le 2^{-\delta' n}$$

By prob method

fix such an E

Average error $\le 2^{-\delta' n}$ $\Rightarrow$ max error $\le 2\cdot 2^{-\delta' n}$

(by dropping strategically half of message)

Claim 2: Let $\{0,1\}^k = \bar{m}_1, \ldots, \bar{m}_{2^k}$

$p_i = \mathrm{ERR}^E(\bar{m}_i)$

$p_1 \le p_2 \le \cdots \le p_{2^k}$ $\quad \frac{1}{2^k}\sum_{i=1}^{2^k} p_i \le 2^{-\delta' n}$

$\Rightarrow p_{\frac{2^k}{2}} \le 2 \cdot 2^{-\delta' n}$.

$\Rightarrow$ final code just use messages $\bar{m}_1, \ldots, \bar{m}_{\frac{2^k}{2}}$

$\Rightarrow$ max dec err $\le 2 \cdot 2^{-\delta' n} = 2^{-\delta n}$ $\quad \delta = \delta' - \frac{1}{n}$

$k \to k+1 \to$ change in rate is negligible

$\Rightarrow$ DONE!