Mar 31

(•) BSC_p $\quad 0 \le p \le \frac{1}{2}$ every n bit gets flipped w.p. p

(•) <u>Shannon's Capacity Thm (positive)</u> $\quad 0 \le p < \frac{1}{2}$

$\forall\ k \le \lfloor (1 - H(p+\varepsilon))n \rfloor$ $\quad \exists\ \delta > 0$ $\quad 0 < \varepsilon \le \frac{1}{2} - p$

$\exists\ E : \{0,1\}^k \to \{0,1\}^n$

$\exists\ D : \{0,1\}^n \to \{0,1\}^k$

s.t. $\forall\ \overline{m} \in \{0,1\}^k$

$$\Pr_{\overline{e} \sim BSC_p} [D(E(\overline{m}) + \overline{e}) \ne \overline{m}] \le 2^{-\delta n} \qquad \delta = \Theta(\varepsilon^2)$$

(•) <u>Proof sketch:</u> Pick E at random

$D = MLD_E$

show this is true in expectation over random E

<u>(Step 1)</u> $\exists\ E$ s.t. on average (over the messages $\overline{m}$) the dec err $\le 2^{-\delta' n}$.

<u>(Step 2)</u> Throw away a carefully chosen subset of $2^{k-1} = \frac{2^k}{2}$ of messages $(k \to k-1)$ s.t. the max dec. err $\le 2^{-\delta n}$.

<u>Probability facts / thms</u>

(I) Chernoff bound: $X_1, \dots, X_m$ independent random variables (r.v.s)

s.t. $X_i \in \{0,1\}$ $\quad X = \sum_{i=1}^{m} X_i$

$$\Pr[X - \mathbb{E}[X] > \gamma m] \le 2^{-\gamma^2 n/2}$$

(II) Linearity of expectation: $Y_1, \dots, Y_m$ be r.v.s $\mathbb{E}\left[\sum_{i=1}^{m} Y_i\right] = \sum_{i=1}^{m} \mathbb{E}[Y_i]$

(III) Union bound: $\Pr\left[\bigcup_{i=1}^{m} E_i\right] \le \sum_{i=1}^{m} \Pr[E_i]$

(IV) <u>Independent</u> r.v.s X, Y $\quad \mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$

(V) Conditional probability

$$\Pr[X = x] = \sum_{y \in \mathcal{Y}} \Pr[X = x \mid Y = y] \cdot \Pr[Y = y]$$

$\bar{e} = (e_1, \dots, e_n) \sim BSC_p$ $\quad \forall i \quad e_i = \begin{cases} 1 & \text{w.p. } p \\ 0 & \text{o/w} \end{cases}$

By I $\quad \mathbb{E}[e_i] = p \cdot 1 + (1-p)\cdot 0 = p$

$$\Pr[wt(\bar{e}) - \mathbb{E}[wt(\bar{e})] > \gamma n] \le e^{-\gamma^2 n/2}$$

$$\mathbb{E}(wt(\bar{e})) = \mathbb{E}\left(\sum_{i=1}^{n} e_i\right) \underset{\text{II}}{=} \sum_{i=1}^{n} \mathbb{E}[e_i] = \sum_{i=1}^{n} p = pn$$

$$\equiv \Pr[wt(\bar{e}) - pn > \gamma n] \le e^{-\gamma^2 n/2}$$

$$\equiv \boxed{\Pr[wt(\bar{e}) > (p+\gamma)n] \le e^{-\gamma^2 n/2}}$$

---

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

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

Ultimately bound $\mathbb{E}_E[ERR^E(\bar{m})] \le 2^{-\Omega(n)}$

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

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

$$\boxed{\mathcal{B} = B(E(\bar{m}), (p+\gamma)n)}$$

$$= \sum_{\bar{y} \in \mathcal{B}} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}} + \sum_{\bar{y} \notin \mathcal{B}} \Pr[\bar{y} \mid E(\bar{m})] \cdot \underbrace{\mathbb{1}_{D(\bar{y}) \neq \bar{m}}}_{\le 1}$$

$\bar{y} \notin \mathcal{B} \equiv \Delta(\underbrace{\bar{y}, E(\bar{m})}_{wt(\bar{e})}) > (p+\gamma)n$

$$\le \underbrace{\sum_{\bar{y} \notin \mathcal{B}} \Pr[\bar{y} \mid E(\bar{m})]}_{\Pr[wt(\bar{e}) > (p+\gamma)n]} \le e^{-\gamma^2 n/2}$$

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

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

by lin of exp

$$= e^{-\gamma^2 n/2} + \sum_{\bar{y} \in \mathcal{B}} \mathbb{E}_E\Big(\underbrace{\Pr(\bar{y} \mid E(\bar{m}))}_{\text{independent of } E} \cdot \underbrace{\mathbb{1}_{D(\bar{y}) \neq \bar{m}}}_{\text{only dependent on } E \text{ (independent of } BSC_p)}\Big)$$

$$\text{IV} = e^{-\gamma^2 n/2} + \sum_{\bar{y} \in \mathcal{B}} \mathbb{E}_E\Big(\underbrace{\Pr(\bar{y} \mid E(\bar{m})]}_{\text{doesn't depend on } E}\Big) \, \mathbb{E}\left(\mathbb{1}_{D(\bar{y}) \neq \bar{m}}\right)$$

$$= e^{-\gamma^2 n/2} + \sum_{\bar{y} \in B} \Pr(\bar{y} \mid E(\bar{m})) \cdot \underbrace{\mathbb{E}(\mathbb{1}_{D(\bar{y}) \neq \bar{m}})}_{\text{goal}}$$

Claim: $\mathbb{E}(\mathbb{1}_{D(\bar{y}) \neq \bar{m}}) \leq 2^{-n(H(p+\varepsilon) - H(p+\gamma))}$

$$\Rightarrow \mathbb{E}_{E}(\mathrm{ERR}^{E}(\bar{m})) \leq e^{-\gamma^2 n/2} + \sum_{\bar{y} \in B} \Pr(\bar{y} \mid E(\bar{m})) \cdot 2^{-n(H(p+\varepsilon) - H(p+\gamma))}$$

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

$$\leq e^{-\gamma^2 n/2} + 2^{-\underbrace{n(H(p+\varepsilon) - H(p+\gamma))}_{\gamma = \frac{\varepsilon}{2}}}$$

$\Theta(\varepsilon^2) \cdot n$

$$\leq \sum_{\bar{y} \in \{0,1\}^n} \Pr[\bar{y} \mid E(\bar{m})]$$

$$= \sum_{\bar{e} \in \{0,1\}^n} \Pr[\bar{e} \text{ is added by } BSC_p]$$

$$= 1$$

$$\leq e^{-\varepsilon^2 n/8} + 2^{-\Theta(\varepsilon^2) \cdot n}$$

$$\leq 2^{-\delta' n} \quad \text{for } \delta' = \Theta(\varepsilon^2)$$

$\forall \bar{m} \in \{0,1\}^k \rightarrow \mathbb{E}_{E}(\mathrm{ERR}^{E}(\bar{m})) \leq 2^{-\delta' n}$.

$\Rightarrow \forall \bar{m} \in \{0,1\}^k \quad \exists E \text{ s.t. } \mathrm{ERR}^{E}(\bar{m}) \leq 2^{-\delta' n}$.

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

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

uniformly at random.

$$\Rightarrow \mathbb{E}_{E} \left(\mathbb{E}_{\bar{m}} \mathrm{ERR}^{E}(\bar{m}) \right) \leq 2^{-\delta' n}$$

$$\Rightarrow \exists E \text{ s.t. } \mathbb{E}_{\bar{m}} \mathrm{ERR}^{E}(\bar{m}) \leq 2^{-\delta' n}.$$