Mar 29

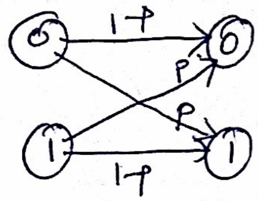
1 min checkin

REMINDERS

(•) Mini-project 2 pg. report due by 11:59pm TONIGHT.
(•) HW 4 out today.

RECAP

(•) BSC_p



Each of the n transmitted bit independently get flipped w/ prob $0 \le p \le \frac{1}{2}$.
[$\bar{e} \sim BSC_p$: noise vector $\bar{e} \in \{0,1\}^n$ sampled from BSC_p]

Shannon's capacity thm for BSC_p $\forall\ 0 \le p < \frac{1}{2}$, $0 \le \varepsilon \le \frac{1}{2} - p$

① $\exists\ \delta > 0$, $E: \{0,1\}^k \to \{0,1\}^n$, $D: \{0,1\}^n \to \{0,1\}^k$
$\forall\ k \le \lfloor (1 - H(p+\varepsilon)) n \rfloor$ — last lecture by mistake stated $(1-H(p)-\varepsilon)$!

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

② If $k \ge \lceil (1 - H(p) + \varepsilon) n \rceil$, then $\forall E: \{0,1\}^k \to \{0,1\}^n$, $\forall D: \{0,1\}^n \to \{0,1\}^k$
$\exists\ \bar{m} \in \{0,1\}^k$ s.t. $\Pr_{\bar{e} \sim BSC_p} [D(E(\bar{m}) + \bar{e}) \ne \bar{m}] > \frac{1}{2}$.

(•) Capacity of BSC_p is $1 - H(p)$

Plan for today (•) Start with proof of ①

Pf. sketch of ① Via probabilistic method.

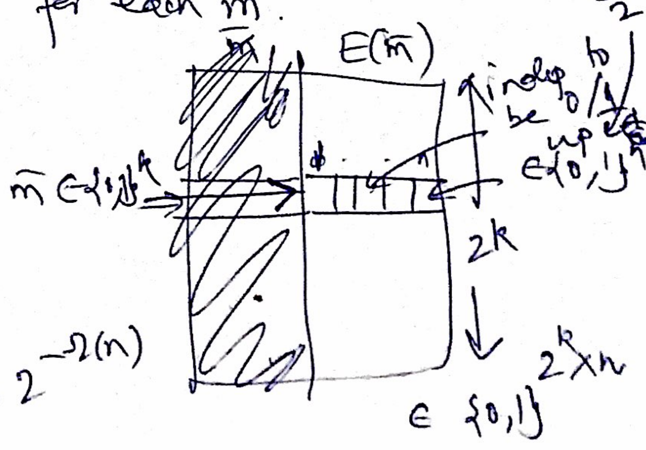
Pick E at random ← exactly same as general random code in HW 3
$\forall\ \bar{m} \in \{0,1\}^k$ $E(\bar{m})$ is distributed uniformly in $\{0,1\}^n$
↖ choice is independent for each $\bar{m}$.

D: MLD_E

→ 2 steps

Step 1: for a fixed $\bar{m} \in \{0,1\}^k$, for random E, MLD_E has decoding error $\le 2^{-\Omega(n)}$

$\Pr [MLD_E (E(\bar{m}) + \bar{e}) \ne \bar{m}] \le 2^{-\Omega(n)}$



$\Rightarrow \forall \bar{m} \in \{0,1\}^k, \exists E$ s.t. decoding error prob for $\bar{m}$ is $\leq 2^{-\Omega(n)}$.

$\rightarrow$ Not enough since we want the same E to work for all messages.

<u>Step 2:</u> From step 1, show $\exists E$ with low decoding error prob $\forall \bar{m} \in \{0,1\}^k$

$\hookrightarrow$ We take the "average E" from step 1 & drop half of the messages.

<u>Aside:</u> 2 sources of randomness:

① choice of E $\rightarrow$ in our control, $\rightarrow$ need to apply prob. method.

② randomness in BSC_p $\rightarrow$ <u>not</u> in our control. contributes to dec error prob.

<u>"pf by picture"</u> fix $\bar{m} \in \{0,1\}^k$

<u>Goal:</u> upper bound $\Pr_{\bar{e} \sim BSC_p}\left[D(E(\bar{m})+\bar{e}) \neq \bar{m}\right] \stackrel{def}{=} ERR^E(\bar{m})$

<u>Argue:</u> $ERR^E(\bar{m})$ is $\underset{2^{-\Omega(n)}}{\text{small}}$ for random E

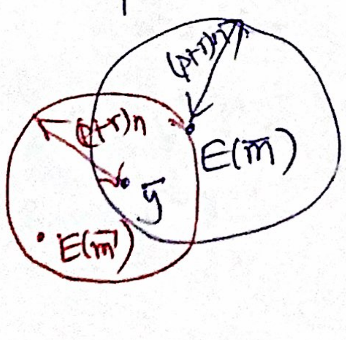
$$\mathop{\mathbb{E}}_{E}\left(ERR^E(\bar{m})\right) \leq 2^{-\Omega(n)}$$

$$\bar{m} \rightarrow E(\bar{m}) \xrightarrow{BSC_p} \bar{y} = E(\bar{m}) + \bar{e}$$

By <u>Chernoff bound</u> $\Pr_{\bar{e} \sim BSC_p}\left[wt(\bar{e}) > (p+r)n\right] \leq 2^{-r^2 n/2}$

$\Rightarrow$ w.p. $1 - 2^{-r^2 n/2}$, $wt(\bar{e}) \leq (p+r)n$

$\equiv \Delta(\bar{y}, E(\bar{m})) \leq \underline{(p+r)n}$



Say dec error happens $\qquad D = MLD_E$

$$\bar{m} \neq \bar{m'} = D(\underbrace{E(\bar{m})+\bar{e}}_{=\bar{y}})$$

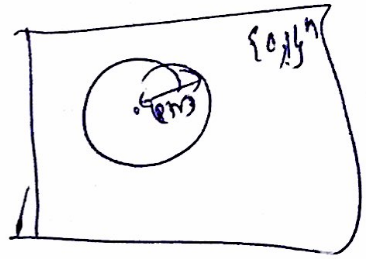
$$\underbrace{\Delta(\bar{y}, E(\bar{m'}))}_{\leq (p+r)n} \leq \Delta(\bar{y}, E(\bar{m}))$$

$\Rightarrow$ Dec error prob (due to $\bar{m}' \neq \bar{m}$) for fixed $\bar{m}'$

$$\leq \Pr\left[E(\bar{m}') \in B(\bar{y}, (p+r)n)\right]$$

Even if you fix $E(\bar{m})$, $\bar{y}$, conditioned on these 2 events $E(\bar{m}')$ is still uniformly at random $\in \{0,1\}^n$

$$= \frac{Vol_2((p+r)n, n)}{2^n}$$



$$\leq \frac{2^{H(p+r)n}}{2^n}$$

$$= 2^{-n(1-H(p+r))}$$

$\bar{m}$ is decoded incorrectly if $\exists\ \bar{m}' \neq \bar{m}$ s.t $D(E(\bar{m}) + \bar{e}) = \bar{m}'$

Since there are $2^k - 1$ $(\leq 2^k)$ choices of $\bar{m}' \neq \bar{m}$

Dec-error prob $ERR_+^E(\bar{m}) \leq (2^k - 1) \cdot 2^{-n(1-H(p+r))}$ $\quad k \leq (1 - H(p+\varepsilon))n$

$$< 2^k \cdot 2^{-n(1-H(p+r))}$$

$$\leq 2^{n(1-H(p+\varepsilon))} \cdot 2^{-n(1-H(p+r))}$$

$$= 2^{n(\cancel{1} - H(p+\varepsilon) - \cancel{1} + H(p+r))}$$

$$= 2^{-n(H(p+\varepsilon) - H(p+r))}$$

$$\leq 2^{-\Omega(n)} \text{ if } r = \frac{\varepsilon}{2}$$

Review chap 3

- $\rightarrow$ Chernoff bound
- $\rightarrow$ linearity of expectation
- $\rightarrow$ Union bound
- $\rightarrow$ $\mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$ indep X, Y