Mar 16

REMINDERS

(•) HW 3 due by 11:59 pm tonight

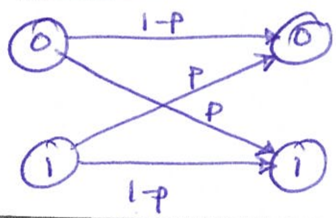
(•) Mini project 2-pg report due by 11:59pm on Wed, Mar 30 — in exactly two weeks

(•) Please vote on proposed HW grading policy change

(•) If you want to sign up for a future proof reading, 5pm Mon (Mar 21) is the deadline.

RECAP

(•) BSC_p



Each of the n transmitted bits 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]

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

① $\exists\ \delta > 0$, $E: \{0,1\}^k \to \{0,1\}^n$; $D: \{0,1\}^n \to \{0,1\}^k$

~~for~~ $\forall k \le \lfloor (1 - H(p+\varepsilon)) n \rfloor$ s.t. — last lecture by mistake stated $\lfloor (1-H(p)-\varepsilon)n \rfloor$

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

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. $\Pr_{\bar{e} \sim BSC_p} [\, D(E(\bar{m}) + \bar{e}) \ne \bar{m} \,] \ge \frac{1}{2}$.

(•) Capacity of BSC_p is $1 - H(p)$

TODAY: Pf reader: Manaswini

(•) Start w/ proof of part ①

(•) Reading assignment for part ②: Sec 6.3.1

Pf. sketch of ①

via probilistic method: Pick E at random

$\forall\ \bar{m} \in \{0,1\}^k$, $E(\bar{m})$ is distributed uniformly over $\{0,1\}^n$

choice is independent for each $\bar{m}$.

D: MLD_E

2 steps:

Step 1: Show for any fixed $m \in \{0,1\}^k$, for random E the prob of decoding error is $2^{-\Omega(n)}$.

Q: Is the above enough $\Rightarrow \forall \bar{m} \in \{0,1\}^k$, $\exists E$ with dec error prob $2^{-\Omega(n)}$

A: NO for every $\bar{m}$, $\exists$ a "good" E but we need the same E that is good $\forall \bar{m}$.

Step 2: show similar result $\forall \bar{m} \in \{0,1\}^k$
↳ involve dropping half of the messages.

Aside: 2 sources of randomness

1. Choice of E: for prob. method.
2. randomness in BSCp noise: contribute to the decoding error prob.

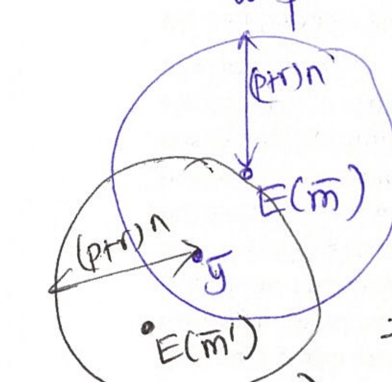
"Pf. by picture" fix $\bar{m} \in \{0,1\}^k$

Goal: upper bound $\Pr_{\bar{e} \sim BSC_p}[D(E(\bar{m})+\bar{e}) \neq \bar{m}] \stackrel{def}{=} ERR^E(\bar{m})$
$(\leq 2^{-\Omega(n)})$

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

By Chernoff bound $\Pr_{\bar{e} \sim BSC_p}[wt(\bar{e}) \geq (p+r)n] \leq 2^{-\Omega(r^2 n)}$ ↑ coming soon!. $r^2 n/3$

w.p. $1 - 2^{-\Omega(nr^2)}$, $\Delta(\bar{y}, E(\bar{m})) \leq (p+r)n$



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

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

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

Even fixing $E(\bar{m})$, $\bar{e} \Rightarrow \bar{y}$ is fixed, $E(\bar{m}')$ is still a uniformly random vector $\in \{0,1\}^n$

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

$= \dfrac{Vol_2((p+r)n, n)}{2^n} \leq \dfrac{2^{H(p+r)n}}{2^n}$

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

Since there are $2^k - 1$ $\bar{m}' \neq \bar{m} \Rightarrow \leq 2^k$ choices for $\bar{m}'$

Dec error prob $\leq 2^k \cdot 2^{-n(1-\cancel{~~} H(p+r))}$ $k \leq (1-H(p+\varepsilon))_r$

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

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

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

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

Recap/Review [Ch. 3] Probability

(I) Chernoff bound: $X_1, \ldots, X_m$ be independent random variables (r.v.s) $X_i \in \{0,1\}$

$$X = \sum_{i=1}^{m} X_i$$

$$\Pr[X - \mathbb{E}[X] > rm] \leq e^{-r^2 m/2}$$

(II) Linearity of expectation: For any r.v. $Y_1, \ldots, Y_m$

$$\mathbb{E}\left(\sum_{i=1}^{m} Y_i\right) = \sum_{i=1}^{m} \mathbb{E}(Y_i)$$

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

(IV) for independent r.v.s X, Y $\mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$

Application of (I) + (II) $\bar{e} = (\underbrace{e_1, \ldots, e_n}_{\text{indep.}}) \sim BSC_p$ $e_i = \begin{cases} 1 & \text{w.p. } p \\ 0 & \text{o/w} \end{cases}$

By (I)

$\Rightarrow \Pr[wt(\bar{e}) - \overbrace{\mathbb{E}(wt(e))}^{pn} > rn] \leq e^{-r^2 n/2}$

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

$\mathbb{E}(wt(\bar{e})) = \mathbb{E}\left(\sum_{i=1}^{n} e_i\right)$ $wt(e) = \sum_{i=1}^{n} e_i$

(II) $\rightarrow = \sum_{i=1}^{n} \mathbb{E}[e_i] = \sum_{i=1}^{n} p = pn.$

$\Rightarrow \Pr[wt(e) - pn > rn] \leq e^{-r^2 n/2}$