March 14, 2019

# REMINDERS

(•) HAPPY $\pi$ DAY!

(•) HW 3 out by tonight & due in 2 weeks (~~April 2nd~~ Mar 28)

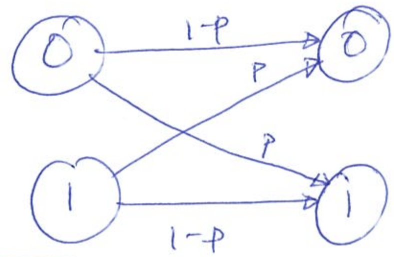
(•) 2-page report due in ~2.5 weeks (April 2)

(•) 2nd round of proof reading has started.

---

## 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 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 $\exists\ \delta > 0$, $E: \{0,1\}^k \to \{0,1\}^n$, $D: \{0,1\}^n \to \{0,1\}^k$ for $k \le \lfloor \underbrace{(1 - H(p+\varepsilon))}_{\text{quantitative diff } 1-H(p)-\varepsilon} n \rfloor$ s.t.

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

② If $k \ge \lceil (1 - H(p) + \varepsilon) n \rceil$, then $\forall$ $E: \{0,1\}^k \to \{0,1\}^n$, $D: \{0,1\}^n \to \{0,1\}^k$

$\exists\ \bar{m} \in \{0,1\}^k$ s.t.

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

---

$\Rightarrow$ Capacity of $BSC_p$ is $1 - H(p)$

---

Pf sketch of ①: Pick $E$ at random. $D = MLD_E$

(Step 1) For random $E$, average (over $\bar{m} \in \{0,1\}^k$) decoding error is $2^{-\Omega(n)}$.

(Step 2) Show similar result $\forall\ \bar{m} \in \{0,1\}^k$ by dropping half of codewords.

---

## TODAY: Pf reader → Anna.

(•) Prove ① of Shannon's result.

(•) Overview of pf of part ② → Reading assignment: Sec 6.3.1 in book.

2 sources of randomness:

1. Choice of $E$ ← for prob method
2. noise from $BSC_p$ ← contribute to decoding error

   $\bar{e} \sim BSC_p$

---

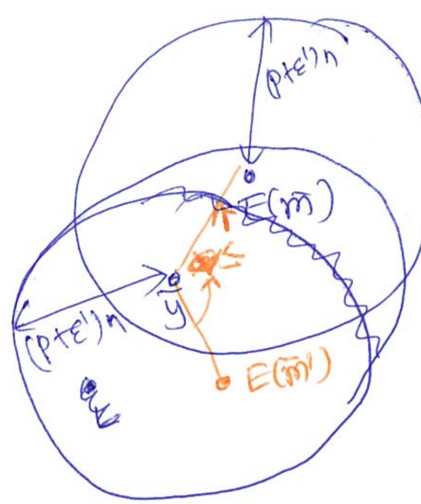
"Pf" by picture: fix $\bar{m} \in \{0,1\}^k$

Upper bound $\Pr_{\bar{e} \sim BSC_p}[D(E(\bar{m})+\bar{e}) \neq \bar{m}]$ $(\le 2^{-\Omega(n)})$

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

By Chernoff bound up $\le 2^{-\Omega(n)}$

$\Pr[wt(\bar{e}) \ge (p+\varepsilon')n] \le 2^{-\Omega((\varepsilon')^2 n)}$




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

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

Dec error prob (via $\bar{m}' \neq \bar{m}$)

$$\le \frac{Vol_2((p+\varepsilon')n, n)}{2^n} \le \frac{2^{H(p+\varepsilon')n}}{2^n} = 2^{-n(1-H(p+\varepsilon'))}$$

Since $\le 2^k-1$ choices of $m'$

Dec error prob $\le (2^k-1)\cdot 2^{-n(1-H(p+\varepsilon'))}$

$$\le 2^k \cdot 2^{-n(1-H(p+\varepsilon'))}$$

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

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

$$\le 2^{-\Omega(n)} \quad \text{if } \varepsilon' = \frac{\varepsilon}{2}.$$

Probability tools:

(I) Chernoff bound: $X_1, \ldots, X_m \in \{0,1\}$ r.v. $X = \sum_{i=1}^{n} X_i$

$$\Pr[\,|X - \mathbb{E}[X]| > \gamma m\,] \leq 2 e^{-\gamma^2 m/2}.$$

(II) Linearity expectation: r.v.s $Y_1, \ldots, Y_m$

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

(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. $X, Y$; $\mathbb{E}[X \cdot Y] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$

---

Application of (I)+(II): $\bar{e} = (e_1, \ldots, e_n) \sim BSC_p$

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

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

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

(I) $\Rightarrow \Pr[wt(\bar{e}) - pn > \gamma n] \leq 2 \cdot e^{-\gamma^2 m/2}$

---

Pf of part (1): $\bar{y} = E(\bar{m}) + \bar{e}$ fix $\bar{m} \in \{0,1\}^k$, $\bar{e} \sim BSC_p$

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

$$= \sum_{\bar{y} \in B(E(\bar{m}), (p+\varepsilon')n)} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}} + \underbrace{\sum_{\bar{y} \notin B(E(\bar{m}), (p+\varepsilon')n)} \Pr[\bar{y} \mid E(m)] \, \underbrace{\mathbb{1}_{D(\bar{y}) \neq \bar{m}}}_{\leq 1}}_{\leq \sum_{\bar{y} \notin B(E(\bar{m}), (p+\varepsilon')n)} \Pr[\bar{y} \mid E(\bar{m})] \,=\, \Pr[wt(\bar{e}) > (p+\varepsilon')n] \,\leq\, e^{-(\varepsilon')^2 n/2}}$$

$$\overset{\#}{\Rightarrow} \left(ERR^{E}(\bar{m})\right) \leq e^{-(\varepsilon')^2 n/2} + \# \left(\sum_{\bar{y} \in B(E(\bar{m}), (p+\varepsilon')n)} \Pr[\bar{y} \mid E(\bar{m})] \cdot \mathbb{1}_{D(\bar{y}) \neq \bar{m}}\right)$$

By linearity of exp:

depends on BSCp but not E

$$\mathop{\mathbb{E}}_{E}\left[\mathrm{ERR}^{E}(\bar{m})\right] \le e^{-(\varepsilon')^2 n/2} + \sum_{\bar{y}\in B(E(\bar{m}),(p+\varepsilon')n)} \mathop{\mathbb{E}}_{E}\left(\Pr[\bar{y} \mid E(\bar{m})]\, \mathbb{1}_{D(\bar{y})\neq \bar{m}}\right)$$

depends on E but not on BSCp

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

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

$$\Rightarrow \mathop{\mathbb{E}}_{E}\left[\mathrm{ERR}^{E}(\bar{m})\right] \le e^{-(\varepsilon')n/2} + 2^{-n\left(H(p+\varepsilon)-H(p+\varepsilon')\right)}\cdot \underbrace{\sum_{\bar{y}\in B(E(\bar{m}),(p+\varepsilon')n)} \Pr[\bar{y}\mid E(\bar{m})]}_{\le \underbrace{\sum_{\bar{y}\in\{0,1\}^n} \Pr[\bar{y}\mid E(\bar{m})]}_{=1}}$$

$$\le e^{-(\varepsilon')n/2} + 2^{-n\left(H(p+\varepsilon)-H(p+\varepsilon')\right)}$$

$$\le 2^{-\delta' n} \qquad \& \ \varepsilon' = \frac{\varepsilon}{2}, \quad \delta' = \Theta(\varepsilon^2)$$

---

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

Since $\bar{m}$ was abitrary $\forall \bar{m}\in\{0,1\}^k$, $\mathop{\mathbb{E}}_{E}\left(\mathrm{ERR}^{E}(\bar{m})\right) \le 2^{-\delta' n}$.

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

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

uniform over $\{0,1\}^k$

m & E are indep.

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

prob method

$$\Longrightarrow \exists E \text{ s.t. } \mathop{\mathbb{E}}_{m}\left(\mathrm{ERR}^{E}(\bar{m})\right) \le 2^{-\delta' n}.$$

Av error $\leq 2^{-\delta n}$ $\Rightarrow$ Max error $\leq 2^{-\delta n}$
(dropping half the codewords)

Claim 2: $\{0,1\}^k = \overline{m}_1, \overline{m}_2, \ldots, \overline{m}_{2^k}$ $\quad P_i = \mathrm{ERR}^E(\overline{m}_i)$

$P_1 \leq P_2 \leq \ldots \leq P_{2^k}$. $\quad \frac{1}{2^k}\sum_{i=1}^{2^k} P_i \leq 2^{-\delta' n}$

$\Rightarrow \quad P_{2^k/2} \leq 2 \cdot 2^{-\delta' n}$. $\quad \delta = \delta' - \frac{1}{n} \Rightarrow 2 \cdot 2^{-\delta' n} \leq 2^{-\delta n}$.

$\Rightarrow$ Only use $\overline{m}_1, \ldots, \overline{m}_{2^k/2}$ in final code $\left(\begin{matrix}\text{dim}: \\ k \to k-1\end{matrix}\right)$

DONE! (except Claims 1+2)

Pf of Claim 2: Pf by contradiction.

Ass. $P_{2^{k-1}} > 2 \cdot 2^{-\delta' n}$

$$2^k \cdot 2^{-\delta' n} \geq \sum_{i=1}^{2^k} P_i \geq \sum_{i=2^{k-1}+1}^{2^k} P_i \geq \sum_{i=2^{k-1}+1}^{2^k} P_{2^{k-1}}$$

$$> \sum_{i=2^{k-1}+1}^{2^k} 2 \cdot 2^{-\delta' n} = \frac{2^k}{2} \cdot 2 \cdot 2^{-\delta' n}$$

$$= 2^k \cdot 2^{-\delta' n} \;!!$$

Claim 1: $\mathbb{E}_E\left[\mathbb{1}_{D(\overline{y}) \neq \overline{m}}\right] \leq 2^{-n(H(p+\varepsilon) - H(p+\varepsilon'))}$

$$\mathbb{E}_E\left(\mathbb{1}_{D(\overline{y}) \neq \overline{m}}\right) = \Pr_E\left[D(\overline{y}) \neq \overline{m} \mid E(\overline{m})\right]$$

Def of MLD

$$= \Pr_E\left[\exists\, \overline{m}' \neq m \text{ s.t. } \Delta(\overline{y}, E(\overline{m}')) \leq \Delta(\overline{y}, E(\overline{m})) \,\middle|\, E(\overline{m})\right]$$

Union bound

$$\leq \sum_{\overline{m}' \neq \overline{m}} \Pr\left[\underbrace{\Delta(\overline{y}, E(\overline{m}')) \leq \underbrace{\Delta(\overline{y}, E(\overline{m}))}_{\leq (p+\varepsilon')n}}_{\Rightarrow\, \Delta(\overline{y}, E(m')) \,\leq\, (p+\varepsilon')n} \,\middle|\, E(\overline{m})\right]$$

$A \Rightarrow B$, $\Pr[A] \leq \Pr[B]$

$$\leq \sum_{\overline{m}' \neq \overline{m}} \Pr\left[\Delta(\overline{y}, E(m')) \leq (p+\varepsilon')n \mid E(m)\right]$$

$E(\overline{m})$ & $E(m')$ are indep

$$= \sum_{\overline{m}' \neq \overline{m}} \underbrace{\Pr\left[\Delta(\overline{y}, E(\overline{m}')) \leq (p+\varepsilon')n\right]}_{\frac{Vol_2((p+\varepsilon')n, n)}{2^n}}, \quad = \frac{Vol_2((p+\varepsilon')n, n)}{2^n}$$

$$\leq \sum_{\overline{m}' \neq \overline{m}} \frac{Vol_2((p+\varepsilon')n, n)}{2^n} \leq 2^k \cdot \frac{2^{H(p+\varepsilon')n}}{2^n}$$

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