Apr 3

1 min checkin

REMINDERS

(•) HW 4 is due by 11:59pm Wed

(•) HW 5 (2nd last HW!) out by 11:59pm Wed

(•) Project report to be graded by the weekend

RECAP

(•) BSC_p : each bit independently gets flipped w.p p

(•) Proof of positive part of Shannon's capacity thm for BSC_p

(→) Let E be random encoding function

(→) $D \leftarrow MLD_E$ (→) $E_{RR}^{E}(\bar{m}) = \Pr_{\bar{e} \sim BSC_p}[D(E(\bar{m}) + \bar{e}) \neq \bar{m}]$

(⇒) $\mathbb{E}_{E}\left(\mathbb{E}_{\bar{m}}[E_{RR}^{E}(\bar{m})]\right) \leq 2^{-\delta' n}$ for $\delta' = \theta(\varepsilon^2)$

$\Rightarrow \exists E$ s.t $\mathbb{E}_{\bar{m}}[E_{RR}^{E}(\bar{m})] \leq 2^{-\delta' n}$.

Plan for today (•) Finish off the proof show $\exists E$ s.t $\forall m$ $E_{RR}^{E}(\bar{m}) \leq 2^{-\Omega(n)}$.

(•) Follow up Q to Shannon's result

(•) Hamming vs. Shannon → Qualitative → Quantitative

(•) List Decoding (if there is time)

Average error $\leq 2^{-\delta' n}$ $\xRightarrow{\text{strategically drop half the msgs.}}$ max error $\leq 2 \cdot 2^{-\delta' n} = 2^{-\delta n}$

$\delta = \delta' - \frac{1}{n}$

as $n \to \infty$, $\delta = \theta(\delta') = \theta(\varepsilon^2)$

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

s.t $P_i = E_{RR}^{E}(\bar{m}_i)$

s.t $P_1 \leq P_2 \leq \cdots \leq P_{2^k}$

note: $\frac{1}{2^k}\sum_{i=1}^{2^k} P_i \leq 2^{-\delta' n}$

Then: $P_{\frac{2^k}{2}} \leq 2 \cdot 2^{-\delta' n}$ (Claim: $q_1 \leq \cdots \leq q_m \Rightarrow q_{\frac{m}{2}} \leq \frac{1}{2m}\sum_{i=1}^{m} q_i$)

Final code: just use E w/ $\bar{m}_1, \ldots, m_{\frac{2^k}{2}}$

$\xRightarrow{\text{claim}}$ max dec. error prob $\leq 2 \cdot 2^{-\delta' n} = 2^{-\delta n}$ done!

($k \to k-1$, $R \to R - \frac{1}{n}$, $R = 1 - H(p+\varepsilon)$)

Shannon's capacity Thm $\Rightarrow$ for BSC_p cap $= 1 - H(p)$.

for qSC_p, cap $= 1 - H_q(p)$

BEC_α, cap $= 1 - \alpha$ (Ex 6.7 in book)

$\rightarrow$ Our proof shows $\exists$ general codes that achieves BSC_p cap.

Q: Can ~~linear~~ linear codes achieve the cap?

A: Yes (Ex 6.4 in book)

Two issues with Shannon's result (even w/ linear codes)

($\rightarrow$) Decoding time is exponential

($\rightarrow$) Codes are not "explicit"

(Def) (Linear) code C is explicit, if $\exists$ an algo given (k, n) computes a generator matrix G in poly time.

(Def) Linear code C is strongly explicit if $\exists$ an algo that given $k, n, \forall (i,j) \in [k] \times [n]$ can compute $G[i,j]$ in poly $(\log n)$ time.

$$\begin{array}{cc} & j \\ i \rightarrow & \begin{bmatrix} & G & \end{bmatrix} \end{array}$$

$\hookrightarrow$ RS codes are strongly explicit

$$\begin{array}{cc} & j \\ i \rightarrow & \begin{pmatrix} \alpha_j^i \end{pmatrix} \end{array}$$

compute in poly$(\log q)$ operation time

eval pts $\alpha_1, \ldots, \alpha_n$

(Next) Big Q: Can we get (strongly) explicit linear codes with poly time decoding (+encoding) that achieves BSC_p capacity?

see in class

near linear $\leftarrow$ (Somewhat) recently can get near linear as well

(Polar codes) [Chap 12]

(Weaker Q): Above w/ $R > 0$, $p > 0$ (Ex 6.13 in book)

Hamming vs Shannon (Qualitative)

Hamming	Shannon
Focus on codewords	~~Deals~~ deals directly encoding/dec
Explicit codes	Not explicit at all!
R vs. δ	R vs "error param"
Worst-case errors	memoryless stochastic errors

Ham's lemma: If a code C can handle $(p+\varepsilon)$-frac of worst-case errors $\Rightarrow$ use C for reliable comm. over BSC_p

dec. error $2^{-\Omega(\varepsilon^2 n)}$

$\Rightarrow$ By Chernoff's bound prob $> (p+\varepsilon)n$ errors $\leq 2^{-\varepsilon^2 n/2}$

Converse: If you can achieve exp. small dec error prob with code $C \Rightarrow C$ has rel dist $\Omega(1)$