Apr 10 — 1 min checkin

REMINDERS

(•) HW 5 due by 11:59 pm Wed.
↳ If you have not submitted any of HW 1-4 submit BOTH HW 5 & 6
↳ Conversely, if you did well on Hws 1-4, you can not submit HW 5 or 6

(•) Video due by 11:59 pm on Sun, May 14
↳ REMEMBER: Everyone submit PDF individually

(•) Report has been graded
↳ See piazza post for important instructions

RECAP

(•) A code $C \subseteq \Sigma^n$ is (p, L)-l.d. if $\forall \bar{y} \in \Sigma^n$ $|C \cap B(\bar{y}, pn)| \leq L$

(•) Johnson bound: Any code w/ rel. dist is (p, qdn)-l.d. for any $p \leq J_q(\delta) \overset{\text{def}}{=} \left(1 - \frac{1}{q}\right)\sqrt{1 - \frac{q\delta}{q-1}}$

q is poly(n)

$\Rightarrow$ COROLLARY: Every MDS code of rate R is $(1 - \sqrt{R}, \text{poly}(n))$-l.d.

Plan for today: List decoding capacity

So far: tradeoff between p & δ (poly(n) list size)

Big Q: R vs p? (poly(n) list size)

THM: $q \geq 2$, $0 \leq p < 1 - \frac{1}{q}$, $\varepsilon > 0$ small enough. Following holds for large enough n:

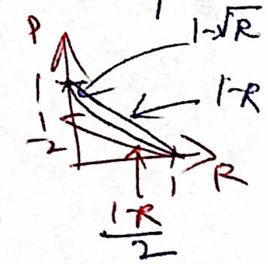
(i) If $R \leq 1 - H_q(p) - \varepsilon$, $\exists$ $(p, O(\frac{1}{\varepsilon}))$-l.d. code of rate R.

(ii) If $R \geq 1 - H_q(p) + \varepsilon$, $\forall$ (p, L)-l.d. of rate R, $L \geq q^{\Omega(n)}$

$\Rightarrow$ "l.d. capacity" $= 1 - H_q(p)$

aka (capacity of worst-case noise channel with list decoding) $=$ capacity of qSC_p

"Shannon meets Hamming"



Recall: $q \geq 2^{\Omega(1/\varepsilon)}$, $1 - H_q(p) \approx 1 - p - \varepsilon$ $\Rightarrow$ $p \approx 1 - R - \varepsilon$

Pf of (1) The probabilistic method

We'll show (w.h.p.) A (general) random code C of rate $R = 1 - H_q(p) - \frac{1}{L}$ is (p, L)-l.d.

$\Rightarrow$ if $L = \lceil \frac{1}{\varepsilon} \rceil$ this implies $\exists \left(p, \lceil \frac{1}{\varepsilon} \rceil\right)$-l.d code of rate $1 - H_q(p) - \varepsilon$

$\hookrightarrow$ Goal: Prob of random code of rate $R = 1 - H_q(p) - \frac{1}{L}$ is NOT (p, L)-l.d. is $\ll 1$

$\exists \bar{y} \in [q]^n$, $\exists \bar{m}_1, \dots, \bar{m}_{L+1} \in [q]^k$ s.t

$\Delta(\bar{y}, C(\bar{m}_i)) \le pn \quad \forall\, i \in [L+1]$

$\iff C$ is not (p, L)-l.d

Witness: $\bar{y}, \bar{m}_1, \dots, \bar{m}_{L+1}$

Bound: $\Pr[\exists \bar{y}, \bar{m}_1, \dots, \bar{m}_{L+1}, \text{ s.t } \forall i \in [L+1]\ \Delta(\bar{y}, C(\bar{m}_i)) \le pn]$

$$\le \sum_{\bar{y}} \sum_{\bar{m}_1} \sum_{\bar{m}_2} \cdots \sum_{\bar{m}_{L+1}} \Pr[\forall i \in [L+1], \Delta(\bar{y}, C(m_i)) \le pn] < 1$$

union bound

Goal: < 1

fix $\underbrace{\bar{y}}_{\in [q]^n}, \underbrace{\bar{m}_1, \dots, \bar{m}_{L+1}}_{\in [q]^k}$

$\Pr[\forall i \in [L+1], \Delta(\bar{y}, C(\bar{m}_i)) \le pn]$

each m_i has an indep codeword

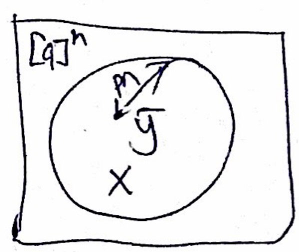
$$= \prod_{i \in 1}^{L+1} \Pr[\Delta(\bar{y}, C(m_i)) \le pn]$$

$$= \left(\frac{Vol_q(pn, n)}{q^n}\right)^{L+1}$$

$$\le \left(\frac{q^{H_q(p) n}}{q^n}\right)^{L+1} = q^{-n(L+1)(1 - H_q(p))}$$

$q^{-n(1-H_q(p))}$

fix $i \in [L+1]$



$\Pr[\Delta(\bar{y}, C(\bar{m}_i)) \le pn] = \frac{Vol_q(pn, n)}{q^n}$

$$\Pr[C \text{ is not } (p,L)\text{-l.d.}] \le \sum_{\underset{q^n}{\bar{y}},\ \underset{(q^{Rn})^{L+1}}{\bar{m}_1,\dots,\bar{m}_{L+1}}} q^{-n(L+1)(1-H_q(p))}$$

$$\le q^n \cdot q^{(Rn)(L+1)} \cdot q^{-n(L+1)(1-H_q(p))}$$

$$= q^{n + n(L+1)R - n(L+1)(1-H_q(p))}$$

$$= q^{-n(L+1)\left(-\frac{1}{L+1} - R + 1 - H_q(p)\right)}$$

$$\le q^{-n(L+1)\left(-\frac{1}{L+1} - \left(1-H_q(p)-\frac{1}{L}\right) + 1 - H_q(p)\right)}$$

$$= q^{-n(L+1)\left(-\frac{1}{L+1} - \cancel{(1-H_q(p))} + \frac{1}{L} + \cancel{1-H_q(p)}\right)}$$

$$= q^{-n(L+1)\left(\frac{1}{L} - \frac{1}{L+1}\right)}$$

$$= q^{-n(L+1)\cdot\frac{1}{L(L+1)}} = q^{-\frac{n}{L}} \to 0$$

as $n \to \infty$. ■

Pf of (ii) $\forall\, C \subseteq [q]^n$ is (p,L) l.d. $R = 1 - H_q(p) + \varepsilon$

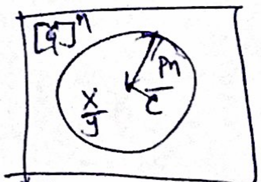
Goal: $L \ge q^{\Omega(\varepsilon n)}$

$\equiv \exists\, \bar{y} \in [q]^n$ s.t. $|B(\bar{y}, pn) \cap C| \ge q^{\Omega(\varepsilon n)}$

Pick: Pick $\bar{y} \in [q]^n$ uniformly at random.

Goal': $\mathbb{E}_{\bar{y}}\left[\,|B(\bar{y},pn) \cap C|\,\right] \ge q^{\Omega(\varepsilon n)}$

$\underset{\text{prob. method}}{\Longrightarrow}$ $\exists\, \bar{y}^*$ s.t. $|B(\bar{y}^*, pn) \cap C| \ge q^{\Omega(\varepsilon n)}$



Fix $\bar{c} \in C$ $\Pr[\Delta(\bar{y},\bar{c}) \le pn]$

$$= \frac{\mathrm{Vol}_q(pn,n)}{q^n} \ge \frac{q^{H_q(p)n - o(n)}}{q^n} = q^{-n(1-H_q(p)) - o(n)}$$

$$\mathbb{E}_{\bar{y}}\left[\,|B(\bar{y},pn) \cap C|\,\right] = \mathbb{E}_{\bar{y}}\left[\sum_{\bar{c}\in C} \mathbb{1}_{\Delta(\bar{y},\bar{c}) \le pn}\right]$$

$$
\begin{aligned}
&= \sum_{\bar{c} \in \mathcal{C}} \mathbb{E}_{y} \left[\mathbb{1}_{\Delta(\bar{y}, \bar{c}) \le pn} \right] \qquad \Pr[\Delta(\bar{y},\bar{c}) \le pn] \cdot 1 + \Pr[\,!\,] \cdot 0 = \Pr[\Delta(\bar{y},\bar{c}) \le pn] \\
&= \sum_{\bar{c} \in C} \Pr\left[\Delta(\bar{y}, \bar{c}) \le pn\right] \\
&= \sum_{\bar{c} \in \mathcal{C}} \frac{\mathrm{Vol}_q(pn, n)}{q^n} \\
&= |C| \cdot \frac{\mathrm{Vol}_q(pn, n)}{q^n} \\
&\ge |C| \cdot q^{-n(1 - H_q(p)) - o(n)} \\
&= q^{Rn} \cdot q^{-n(1 - H_q(p)) - o(n)} \\
&= q^{(\cancel{1 - H_q(p)} + \varepsilon)n \cancel{- n(1 - H_q(p))} - o(n)} \\
&= q^{\varepsilon n - o(n)} \ge q^{\varepsilon n / 2} \\
&= q^{\Omega(\varepsilon n)} \qquad \blacksquare
\end{aligned}
$$