March 28, 2019

REMINDERS

- (•) HW 3 due tonight (11:59pm)
- (•) Miniproject report due next Tue (11:59pm)
  - ↳ If you submit your report by tonight, I'll give ~~feedbt~~ feedback by the weekend. Else I'll grade it after due date.

RECAP:

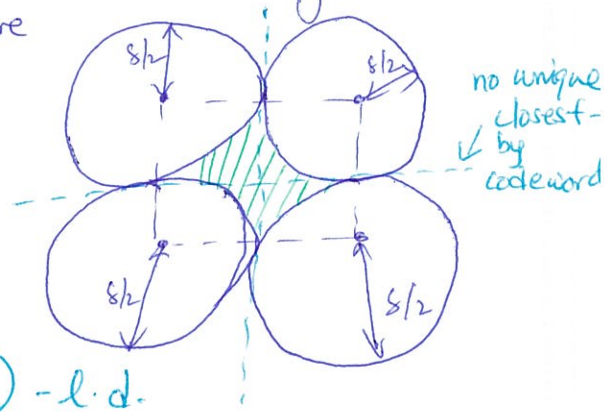
LIST DECODING:

Informally: Allows for outputting a list of codewords with guarantee that transmitted code word is in there

allows for decoding from more error patterns that unique decoding

Formally: $0 \le p \le 1$, $L \ge 1$, $C \subseteq \Sigma^n$ is (p, L) list decodable if $\forall \bar{y} \in \Sigma^n$

$$|C \cap B(\bar{y}, pn)| \le L$$



→ Want $L \le \text{poly}(n)$

→ Any code w/ rel. dist δ is $\left(\frac{\delta}{2}, 1\right)$-l.d.

Q1: Can we get $(p, n^{O(1)})$-l.d. codes for $p > \delta/2$

Q2: Max rate for a $(p, n^{O(1)})$-l.d. code?

TODAY: [Proofs reader: Matt]

- (•) Johnson bound (Ans to Q1 is yes for all codes!)
- (•) List decoding capacity (rate ~~ke~~ $1 - H_q(p) - \varepsilon$ for $(p, O(\frac{1}{\varepsilon}))$ l.d. codes!)
  - ↳ Will not be able to finish this

THM (JOHNSON BOUND): $q \ge 2$, $C \subseteq [q]^n$ with distance d.

If $p < J_q\left(\frac{d}{n}\right) \Rightarrow C$ is (p, qdn)-l.d.

$$J_q(x) = \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{qx}{q-1}}\right)$$

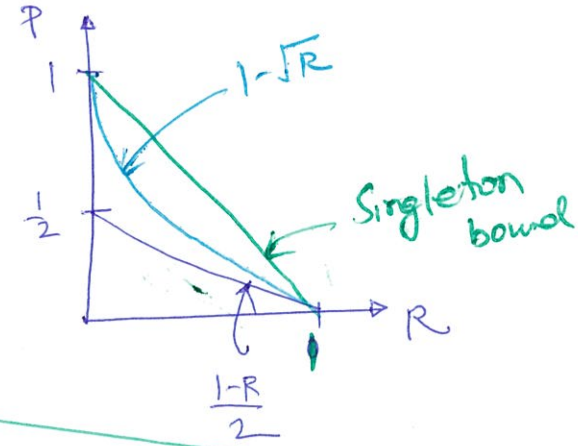
Lemma 1 (pf in book) $\forall q \ge 2$, $0 \le x \le 1 - \frac{1}{q}$

$$J_q(x) \ge 1 - \sqrt{1 - x} > \frac{x}{2}$$

$\Rightarrow$ Any $(n,k,d)_q$ code is $\left(\frac{e}{n}, qdn\right)$-l.d. $\quad e < n - \sqrt{n(n-d)}$

Assume C is MDS ie $\delta = 1 - R$

$\Longrightarrow$ Johnson bound ~~impl~~ $\quad p \leq 1 - \sqrt{1-(1-R)} = 1 - \sqrt{R}$



Q: Is the Johnson bound tight?
$(p \leq 1 - \sqrt{1-\delta})$

YES: $\exists$ code s.t for $p > J_q(\delta)$
$\Rightarrow$ super poly codewords

NO: Random codes do better

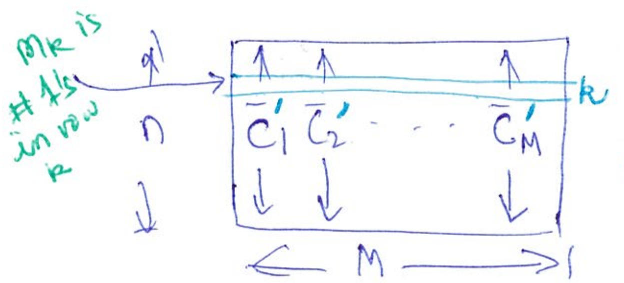
Pf of Johnson bound $(q=2)$

Proof technique: Double counting. Come up with some quantity S.
then show by (approx counting / analyzing) S:
(i) $S \leq U$ (ii) $S \geq L$ $\Rightarrow$ $L \leq U$ $\xrightarrow{\text{(somehow)}}$ get your result.

Goal: $\forall\, C \subseteq \{0,1\}^n$ has dist $d = \delta n$.
$\Rightarrow \forall\, \bar{y} \in \{0,1\}^n, \quad |B(\bar{y}, e) \cap C| \leq 2dn$

$e = pn$ s.t
$$p < \left(1 - \frac{1}{2}\right)\left(1 - \sqrt{1 - \frac{2\delta}{2-1}}\right) = \frac{1}{2}\left(1 - \sqrt{1-2\delta}\right)$$

fix $C \subseteq \{0,1\}^n$ with dist d
$\bar{y} \in \{0,1\}^n$
Let $B(\bar{y}, e) \cap C = \{\bar{c}_1, \ldots, \bar{c}_M\}$
$\Rightarrow M \leq 2dn.$



Define $\bar{c}_i' = \bar{c}_i - \bar{y}$

$$S = \sum_{i<j} \Delta(\bar{c}_i', \bar{c}_j')$$

$\Rightarrow$ (i) $wt(\bar{c}_i') = \Delta(\bar{c}_i, \bar{y}) \leq e$
(ii) $\Delta(\bar{c}_i', \bar{c}_j') = \Delta(\bar{c}_i, \bar{c}_j) \geq d$.

Lower bound: By (ii) $\quad S \geq \sum_{i<j} d = \binom{M}{2} d = \frac{M(M-1)}{2} d.$

Upper bound: $\quad S = \sum_{k=1}^{n} m_k (M - m_k) \rightarrow$ # ~~unordered~~ unordered pairs i, j s.t. $(\bar{c}_i'[k], \bar{c}_j'[k]) = (0,1)$ or $(1,0)$

$$S' = \sum_{k=1} m_k (M - m_k) \qquad \bar{e} = \sum_{k=1}^{n} \frac{m_k}{M}$$

$$\sum_{k=1}^{n} m_k = \sum_{j=1}^{M} wt(\bar{c}_j) \leq \sum_{j=1}^{M} e = eM$$

$$\Rightarrow \boxed{\bar{e} \leq e}$$

Cauchy - Schwartz lemma: $\bar{x}, \bar{y} \in \mathbb{R}^n \qquad \langle \bar{x}, \bar{y} \rangle^2 \leq \|\bar{x}\|^2 \|\bar{y}\|^2$

$$\bar{x} = (m_1, \ldots, m_n), \quad \bar{y} = \left(\tfrac{1}{n}, \ldots, \tfrac{1}{n}\right)$$

$$\langle \bar{x}, \bar{y} \rangle^2 = \left(\frac{\sum_{k=1}^{n} m_k}{n}\right)^2 \leq \left(\sum_{k=1}^{n} m_k^2\right) \underbrace{\left(\sum_{k=1}^{n} \frac{1}{n^2}\right)}_{=\frac{1}{n}}$$

$$\Rightarrow \boxed{\left(\sum_{k=1}^{n} m_k^2\right) \geq \frac{\left(\sum_{k=1}^{n} m_k\right)^2}{n}}$$

Going back to S

$$S = \sum_{k=1}^{n} m_k (M - m_k) = M \sum_{k=1} m_k - \sum_{k=1} m_k^2$$

$$\leq M \cdot \left(\sum_{k=1}^{n} m_k\right) - \frac{1}{n} \left(\sum_{k=1}^{n} m_k\right)^2$$

def of $\bar{e}$ $\rightarrow$ $= M \cdot M\bar{e} - \frac{1}{n} M^2 (\bar{e})^2$

$$= M^2 \left(\bar{e} - \frac{(\bar{e})^2}{n}\right)$$

Combing lower + upper bound ons:

$$M^{\cancel{2}} \left(\bar{e} - \frac{(\bar{e})^2}{n}\right) \geq \frac{\cancel{M}(M-1)\,d}{2}$$

$$\Rightarrow 2M \left(n\bar{e} - (\bar{e})^2\right) \geq (M-1)\,dn$$

$$\Rightarrow M \left(dn - 2n\bar{e} + 2(\bar{e})^2\right) \leq dn$$

$$\Rightarrow M \leq \frac{dn}{dn - 2n\bar{e} + 2(\bar{e})^2} \ \cdots \leq 2dn.$$

$$\cdots = \frac{2dn}{\underbrace{(n - 2\bar{e})^2 - n(n-2d)}_{\geq 1}}$$

by The Johnson bound ub.

LIST Decoding Capacity

<u>So far:</u> tradeoff b/w p & δ?

<u>Big Q:</u> R vs p

<u>THM:</u> $q \geq 2$, $0 \leq p < 1 - \frac{1}{q}$, $\varepsilon > 0$. Following are true for large ~~as~~ enough n:

1. If $R \leq 1 - H_q(p) - \varepsilon$, $\exists$ $(p, O(\frac{1}{\varepsilon}))$ - l.d code of rate R
2. If $R > 1 - H_q(p) + \varepsilon$, every (p, L) - l.d code of rate R has $L \geq q^{\Omega(n)}$.

"List decoding capacity" $= 1 - H_q(p) =$ capacity of qSC_p
(for $q \geq 2^{\Omega(1/\varepsilon)}$, ~~q~~ $p \geq 1 - R - \varepsilon$)

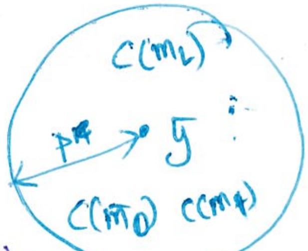
(Pf ~~idea~~)

1. By prob. method. random code C of rate $1 - H_q(p) - \frac{1}{L}$ for $L \geq 1$

$\Longrightarrow$ (p, L) - l.d. $\qquad L = \lceil \frac{1}{\varepsilon} \rceil$

Analyze the prob of a "bad event"

$\exists\ \bar{m}_0, \ldots, \bar{m}_L \in [q]^k$ s.t $\Delta(C(\bar{m}_i), \bar{y}) \leq pn$ $\forall\ 0 \leq i \leq L$



~~for~~ a fixed $\bar{m}_i$

$$\Delta(C(\bar{m}_i), \bar{y}) \leq pn = \frac{Vol_q(pn, n)}{q^n} \leq \frac{q^{H_q(p)n}}{q^n} = q^{-n(1 - H_q(p))}$$

Since $C(\bar{m}_i)$ is independent for each ~~i~~ $\bar{m}_i$,

$$\Pr[\underbrace{\forall 0 \leq i \leq L,\ \Delta(C(\bar{m}_i), \bar{y}) \leq pn}] \leq \left(q^{-n(1 - H_q(p))}\right)^{L+1}$$

Prob $\exists\ \bar{y}, \bar{m}_0, \ldots, \bar{m}_L$ s.t $\quad \underset{\text{union}}{\leq} q^n (q^{k})^{L+1} \cdot q^{-n(L+1)(1 - H_q(p))}$

$k = Rn$

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

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

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

$$= q^{-\frac{n}{L}} \longrightarrow 0 \quad \text{as } n \to \infty$$

$\Rightarrow$ wp $\geq 1 - q^{-n/L}$, $\nexists$ $\bar{y}, \bar{m}_0, \ldots, \bar{m}_L$ s.t

$\forall_{0 \leq i \leq L}$ $\Delta(C(\bar{m}_i), \bar{y}) \leq pn$

$\Rightarrow$ C is (p, L) l.d. ∎