Apr 7

1 min checkin

REMINDERS

(•) HW 5 due by 11:59 pm Wed
(•) Video due in ~5.5 weeks (last Sunday of semester)
↳ NO extension to the deadline (please plan in advance)

RECAP

(•) $C \subseteq \Sigma^n$ is (p, L)-l.d. if $\forall \bar{y} \in \Sigma^n$, $|\{\bar{c} \in C \mid \Delta(\bar{c}, \bar{y}) \le pn\}| \le L$
(•) code with rel. dist δ is $(< \frac{\delta}{2}, 1)$-l.d.

Plan for today (•) Johnson bound

Q1: Can we correct $> \frac{\delta}{2}$ errors with poly(n) list size?

Q2: What is the optimal tradeoff b/w R & p $(p, \text{poly}(n))$-l.d code?

A1: Yes! $\forall$ codes! (Johnson bound)

THM (Johnson bound) $q \ge 2$, $C \subseteq [q]^n$ with dist. d,

If $p \le J_q(\frac{d}{n}) \Rightarrow C$ is $(p, \underbrace{qdn}_{\text{is poly(n) if } q \text{ is poly(n)}})$-l.d

$\frac{d}{n} = \delta$

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

$0 \le x \le 1 - \frac{1}{q}$

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

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

$\Rightarrow J_q(\delta) > \frac{\delta}{2}$!

$\Rightarrow$ Any $(n, k, d)_q$ code is $(\frac{e}{n}, qdn)$-l.d from $e \le n - \sqrt{n(n-d)}$ errors

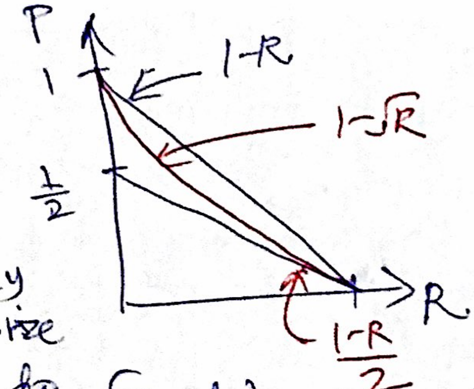
$\equiv \frac{e}{n} < 1 - \sqrt{\frac{n(n-d)}{n^2}} = 1 - \sqrt{1 - \frac{d}{n}} = 1 - \sqrt{1-\delta}$

C is MDS $\Rightarrow \delta = 1 - R$

$\Rightarrow$ Johnson bound $p \le 1 - \sqrt{1-(1-R)} = 1 - \sqrt{R}$

Hamming setting (unique) dec $p \le \frac{\delta}{2} = \frac{1-R}{2}$

~~Pf~~ Is JB tight?



Yes! $\exists$ some code C w/ rel. dist δ, st $p > 1-\sqrt{1-\delta} \Rightarrow$ super poly list size

No: Random codes do (much) better!

Pf of Johnson bound $(q=2)$

Proof technique Double counting (to prove an inequality)

1. Come up with some quantity S
2. Show by (approx) counting that
   (i) $S \le U$ (ii) $S \ge L$

   } double counting

   $\Rightarrow L \le U$
3. ~~Sto~~ (Somehow) $\downarrow$ to prove the desired inequality (generally algebraic manipulation)

Goal: $\forall C \subseteq \{0,1\}^n$ w/ $d = \delta n$, $\forall \bar{y} \in \{0,1\}^n$ $\boxed{e = pn}$

$$|B(\bar{y}, pn) \cap C| \le 2dn \qquad p < \left(1-\tfrac{1}{2}\right)\left(1-\sqrt{1-\tfrac{2\delta}{2-1}}\right) = \tfrac{1}{2}\left(1-\sqrt{1-2\delta}\right)$$

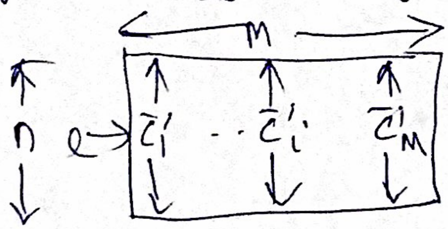
---

fix $C \subseteq \{0,1\}^n$ w/ rel. dist δ

$y \in \{0,1\}^n$ Let $B(\bar{y}, \underset{e}{\underset{\parallel}{pn}}) \cap C = \{\bar{c}_1, \ldots, \bar{c}_M\}$ for some M

Goal: $\boxed{M \le 2dn}$

$\forall i \in [M]$ $\quad \bar{c}_i' = \bar{c}_i - \bar{y}$



$\Rightarrow$ (I) $wt(\bar{c}_i') = \Delta(\bar{c}_i, y) \le e$

(II) $\Delta(\bar{c}_i', \bar{c}_j') = \Delta(\bar{c}_i, \bar{c}_j) \ge d$

$\bar{c}_i'[\ell] = c_i[\ell] - y[\ell]$

$c_j'[\ell] = c_j[\ell] - y[\ell]$

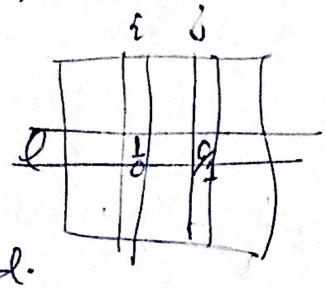
Def: $S = \sum_{i<j} \Delta(\bar{c}_i', \bar{c}_j')$

$$\text{II} \Rightarrow S = \sum_{i<j} \Delta(\bar{c}_i, \bar{c}_j) \geq \sum_{i<j} d = \binom{M}{2} d$$

$$= \frac{M(M-1)}{2} \cdot d \quad \text{(\#)}$$

Upper bound: $\ell \in [n]$ $m_\ell \overset{\text{def}}{=}$ # 1s in ℓ'th row

$$S = \sum_{\ell=1}^{n} (\text{\# pairs in } \ell^{th} \text{ row that differ})$$



$$= \sum_{\ell=1}^{n} m_\ell (M - m_\ell)$$

← Goal: upper bound.

$$= M \sum_{\ell=1}^{n} m_\ell - \sum_{\ell=1}^{n} m_\ell^2$$

Aside (i) $\bar{e} \overset{\text{def}}{=} \dfrac{\sum_{\ell=1}^{n} m_\ell}{M} = \dfrac{\sum_{i \in [M]} wt(\bar{c}_i)}{M} \leq \dfrac{\sum_{i \in M} e}{M} = \dfrac{eM}{M} = e$

Aside (ii) Cauchy-Schwartz $\bar{x}, \bar{y} \in \mathbb{R}^N$

$\langle \bar{x}, \bar{y} \rangle = \sum_{i=1}^{N} x_i y_i$ $\qquad \langle \bar{x}, \bar{y} \rangle^2 \leq \|x\|^2 \|y\|^2$

$\|\bar{x}\|^2 = \langle \bar{x}, \bar{x} \rangle = \sum_{i=}^{n} x_i^2$ $\qquad \equiv \|x\|^2 \geq \langle \bar{x}, \bar{y} \rangle^2 / \|y\|^2$

Going back to S $\qquad S = M \sum_{\ell=1}^{n} m_\ell - \sum_{\ell=1}^{n} m_\ell^2$

$\bar{x} = (m_\ell)_{\ell=1}^{n}$, $\bar{y} = (\frac{1}{n}, \frac{1}{n}, \dots \frac{1}{n})$ Cauchy-Schwatrz → $\cancel{\geq} \; M \cdot M \bar{e} - \dfrac{(\sum_\ell m_\ell)^2}{n}$

⋮

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

⋮

$$M \leq 2dn$$