Apr 1

REMINDERS

(∘) Will try & finish grading project reports ≤ 1 week

(∘) Fill in the AV questionnaire by Sunday if you want + can

RECAP:

(∘) $C \subseteq \Sigma^n$ if (p, L)-l.d. (dist decodable) if $\forall \bar{y} \in \Sigma^n$,

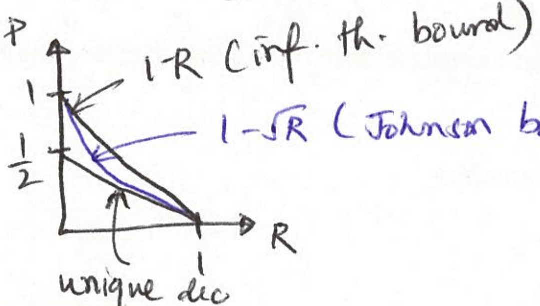
$$|\{\bar{c} \in C \mid \Delta(\bar{y}, \bar{c}) \leq pn\}| \leq L$$

(∘) JOHNSON BOUND: $q \geq 2$, $C \subseteq [q]^n$ with dist $d = \delta n$

If $p < J_q(\delta) \Rightarrow C$ is (p, qnd)-l.d.

$$J_q(\delta) = \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{q\delta}{q-1}}\right) \left[\geq 1 - \sqrt{1-\delta} > \frac{\delta}{2}\right]$$

(∘) Bounds



TODAY:

(∘) Proof readers: Siddhesh, Jiawei, Frank

(∘) Prove Johnson bound

(∘) List decoding capacity

Proof technique: Double counting. (∘) S $\left\{ \begin{array}{l} (\circ)\ S \leq U \\ (\circ)\ L \leq S \end{array} \right. \Rightarrow L \leq U$

Pf of Johnson bound for $q = 2$

Goal: $\forall C \subseteq \{0,1\}^n$ w/ dist $d = \delta n$ $\quad e = pn$ s.t.

$\forall \bar{y} \{0,1\}^n \quad |B(\bar{y}, pn) \cap C| \leq 2dn \quad p < \left(1 - \frac{1}{2}\right)\left(1 - \sqrt{1 - 2\delta}\right)$

$= \frac{1}{2}\left(1 - \sqrt{1 - 2\delta}\right)$

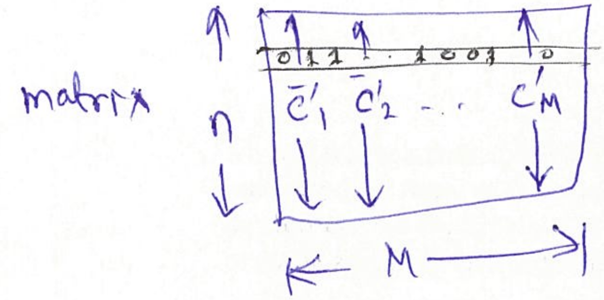
---

fix $C \subseteq \{0,1\}^n$ w/ dist $d = \delta n$

fix $\bar{y} \in \{0,1\}^n$

Let ~~BCP~~ $C \cap B(\bar{y}, \underbrace{pn}_{e}) = \{\bar{c}_1, \ldots, \bar{c}_M\}$

$\Rightarrow$ show $M \leq 2dn$



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

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

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

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

$$\text{(II)} \Rightarrow S \geq \sum_{i<j} d = \binom{M}{2} d = \frac{M(M-1)}{2} d \quad \text{—(*)}$$

Upper bound: $k \in [n]$, m_k = # 1s in row k of matrix

$$S = \sum_k (\text{\# pairs in row } k \text{ that differ})$$

$$= \sum_k m_k (M - m_k) \longrightarrow \text{Goal: upper bound this}$$

Aside: (1) $\bar{e} = \dfrac{\sum_{k=1}^{n} m_k}{M} = \dfrac{1}{M} \sum_{k=1}^{M} wt(\bar{c}'_i) \leq \dfrac{1}{M} \sum_k e = \dfrac{1}{M} \cdot Me = e.$ —(#)

Aside (2) Cauchy-Schwartz inequlity $\bar{x}, \bar{y} \in \mathbb{R}^N$

$$\langle \bar{x}, \bar{y} \rangle^2 \leq \|x\|^2 \|y\|^2 \equiv \|x\|^2 \geq \frac{\langle \bar{x}, \bar{y} \rangle^2}{\|y\|^2}$$

Going back to S

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

$$\xrightarrow{\text{Def of } \bar{e}} = M \cdot M \cdot \bar{e} - \sum_k m_k^2$$

$$\xrightarrow{\text{by (\#)}} \leq M^2 \bar{e} - \sum_k m_k^2$$

Aside (III) Applying Cauchy-Schwartz, $\bar{x} = (m_1, \ldots, m_n)$ $\bar{y} = (\frac{1}{n}, \ldots, \frac{1}{n})$

$\Rightarrow$ By Cauchy-Schwartz $\displaystyle \sum_k m_k^2 \geq \frac{\left(\sum_k m_k \cdot \frac{1}{n}\right)^2}{\sum_{k=1}^{n} \left(\frac{1}{n}\right)^2} = \frac{(\sum m_k)^2 / n^2}{n \cdot \frac{1}{n^2} = \frac{1}{n}}$

$$= \frac{\left(\sum_k m_k\right)^2}{n}$$

$$\Rightarrow S \le M^2\bar{e} - \frac{\left(\sum_k m_k\right)^2}{n} = M^2\bar{e} - \frac{(M\bar{e})^2}{n} = M^2\left(\bar{e} - \frac{(\bar{e})^2}{n}\right)$$

By combining u.b. & l.b. on S,

we get $\frac{\cancel{M}(M-1)}{2} d \le M^{\cancel{2}}\left(\bar{e} - \frac{(\bar{e})^2}{n}\right)$

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

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

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

Uses the fact that $\bar{e} \le e$

$$\le 2dn.$$

List decoding capacity

So far: tradeoff b/w p & δ? (poly(n) list size)

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

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

1. If $R \le 1 - H_q(p) - \varepsilon$, $\exists$ $(p, O(\frac{1}{\varepsilon}))$ l.d. code of rate R
2. If $R \ge 1 - H_q(p) + \varepsilon$, $\forall$ (p, L) l.d. codes of rate R, $L \ge q^{\Omega(n)}$

"list decoding capacity" $= 1 - H_q(p) =$ capacity of qSC_p

$\Rightarrow$ Hamming meets Shannon!

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