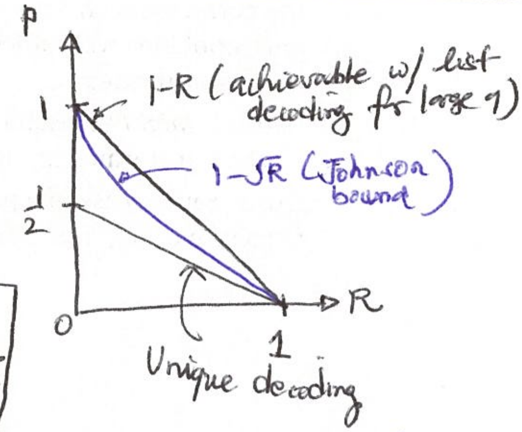
Apr 4

REMINDERS

(•) HW 4 is due by 11:59pm Wed
↳ See piazza post on some suggestions / hints on HW 4
(•) HW 5 (2nd Last HW!) out by 11:59pm Wed

RECAP



Def: A code $C \subseteq [q]^n$ is (p,L)-list decoding if $\forall\ \bar{y} \in [q]^n$,
$$|C \cap B(\bar{y}, pn)| \le L.$$

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

$$\boxed{\begin{array}{l}\text{Technical statement: } p \le J_q(\delta) \\ \left\{ J_q(\delta) = \left(1-\frac{1}{q}\right)\left(1-\sqrt{1-\frac{q\delta}{q-1}}\right)\right\} \\ \Rightarrow (p, qdn)\text{ l.d.}\end{array}}$$

List decoding ~~capa~~ capacity: $q \ge 2$, $0 \le p < 1-\frac{1}{q}$. Following is true for small enough ε & large enough n:
(i) $\exists$ code of rate $R \le 1 - H_q(p) - \varepsilon$ s.t. it is $(p, O(\frac{1}{\varepsilon}))$-l.d.
(ii) For every ~~code~~ (p,L)-l.d. code of rate $\ge 1-H_q(p)+\varepsilon \Rightarrow L \ge q^{\Omega(\varepsilon n)}$

TODAY

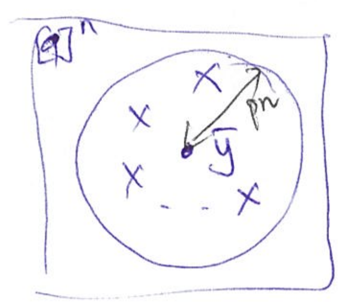
(•) Proof readers: Shiva Kumar, Ryan
(•) Pf of l.d. capacity thm
(•) [If there is more time] Back to R vs. δ (for a little bit)

Pf of (i) of LD capacity By prob method.
(General) random code C of rate $R = 1 - H_q(p) - \frac{1}{L} \Rightarrow C$ is (p,L)-l.d.
($\Rightarrow$ get rate $1 - H_q(p) - \varepsilon$ with list size $\lceil \frac{1}{\varepsilon} \rceil$)

Goal: Show prob random code of rate R is NOT (p,L)-l.d. is $\ll 1$

Witness: $\exists\ \bar{y} \in [q]^n$, $\exists\ \bar{m}_1, \ldots, \bar{m}_{L+1}$ s.t. $\Delta(\bar{y}, C(\bar{m}_i)) \le pn$.
$\iff$ C is NOT (p,L) l.d.

fix. $\bar{y} \in [q]^n$, $\bar{m}_1, \ldots, \bar{m}_{L+1} \in \mathbb{F}_q^{\,R}$
$$\Pr\left[\forall\ 1 \le i \le L+1,\ \Delta(\bar{y}, C(\bar{m}_i)) \le pn\right]$$



/

fix i ($\bar{m}_i$)

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

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

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

choice of each $C(\bar{m}_i)$ is independent.

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

union bound

$$\le \sum_{\bar{y}} \sum_{\bar{m}_1,\dots,\bar{m}_{L+1}} \Pr[\forall i\ \Delta(\bar{y}, C(\bar{m}_i)) \le pn]$$

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

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

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

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

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

$\to 0$ as $n \to \infty$ ■

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

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

Fix $C \subseteq [q]^n$ be (p,L) l.d. code of rate $1-H_q(p)+\varepsilon$

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

We'll use the prob. method.

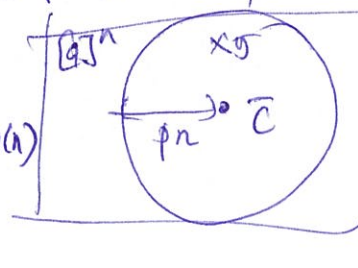
Pick $\bar{y} \in [q]^n$ uniformly at random

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

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

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

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



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

$\mathbb{E}[\mathbb{1}_{P(x)}] = \Pr[P(x) \text{ is true}]$

lin of exp. $\longrightarrow$

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

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

$$= \sum_{\bar{c}\in C}\frac{Vol_q(pn,n)}{q^n}$$

$$(*) \longrightarrow = |C|\cdot\frac{Vol_q(pn,n)}{q^n} \ge q^{-n(1-H_q(p))-o(n)}$$

$$\ge q^{Rn}\cdot q^{-n(1-H_q(p))-o(n)}$$

$$= q^{\cancel{(1-H_q(p))n}+\varepsilon n-\cancel{n(1-H_q(p))}-o(n)}$$

$$= q^{\varepsilon n-o(n)} \ge q^{\Omega(\varepsilon n)}$$

$\blacksquare$

<u>COR:</u> (from $*$) $\exists\ \bar{y}'\in[q]^n$ s.t. $|B(\bar{y}',pn)\cap C| \ge |C|\cdot\frac{Vol_q(pn,n)}{q^n}$.

List decoding capacity: $1-H_q(p) \approx 1-p-\varepsilon$ if $q\ge 2^{\Omega(1/\varepsilon)}$

$\equiv\ p\approx 1-R-\varepsilon$

$q\ge q^{\Omega(1/\varepsilon)}$

<u>Q1:</u> Explicit code that achieves l.d. capacity? $\Leftrightarrow p\approx 1-R-\varepsilon$?

<u>Q2:</u> ____________________ with efficient encoding + list decoding algs

<u>Q3:</u> Above with $p=1-\sqrt{R}$?
$\uparrow$ RS

<u>Ans:</u> Yes!

Back R vs δ

Elias-Bassalygo bound:

q-ary code rate R, rel. dist δ

$$R \le 1 - H_q(J_q(\delta)) + o(1)$$