February 21, 2019

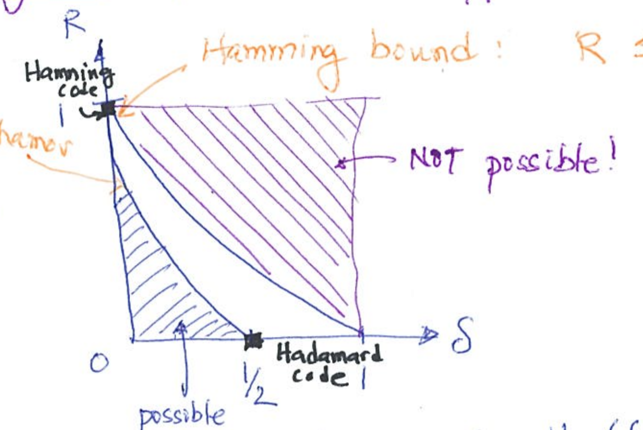
REMINDERS:

- (•) HW 0 due 11:59 pm tonight (NOT graded but light feedback)
- (•) HW 1 out ~~today~~ by tonight + (Make sure you read ALL instructions) Ask if something is not clear
- (•) Video topic + group composition due Tue, Mar 5
- (•) All proof reading for lectures till last week graded
  ↳ ~~Actual score might not show up on grade book but you can see feedback on the actual submission~~

RECAP: Big Q: Optimal tradeoff between R and δ?

→ $\boxed{q=2}$ Hamming bound: $R \le 1 - H_q(\delta)$

Gilbert-Varshamov bound $R \ge 1 - H_q(\delta)$



→ Greedy construction [Gilbert] $(R \ge 1 - H_q(\delta))$ ← NOT necessarily linear code

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

$H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$

→ $q^{H_q(p)n - o(n)} \le Vol_q(pn, n) \le q^{H_q(p)\cdot n}$ if $\boxed{p \le 1 - \frac{1}{q}}$

TODAY

- (•) Q1: Can we achieve GV bound with linear codes?
- (•) Q2: Can we have $R > 0$ and $\delta > \frac{1}{2}$? is inherently necessary or just a technical assumption?
- (•) Q3: Can we make the 'empty' space smaller?
- (•) Q4: Other upper bounds?

Order of coverage of topics:

Q1, Q4, Q2+3

Probability lemmas:

Lemma 1: $\overline{m} \in \mathbb{F}_q^k$ be non-zero. Let $G \in \mathbb{F}^{k \times n}$ be chosen uniformly at random ⇒ $\overline{m}G$ is uniformly random vector in $\mathbb{F}_q^n$

Union bound: $Pr[\bigvee_{i=1}^{m} E_i] \le \sum_{i=1}^{m} Pr[E_i]$

Goal: Show $\exists$ a linear code $\mathcal{C}$ s.t $\mathcal{C}$ has rel dist δ and $R(\mathcal{C}) \geq 1 - H_q(\delta) - \varepsilon$ (any $\varepsilon > 0$)

Probabilistic method:

$\Pr[$ a random linear code of rate $1 - H_q(\delta) - \varepsilon$ has dist $\geq \delta] > 0$

$\equiv \Pr[$ ______________________________ $< \delta] < 1$

Consider a (uniformly) random $G \in \mathbb{F}^{k \times n}$ $\quad (n \to \infty)$

$k = \lfloor (1 - H_q(\delta) - \boxed{\tfrac{\varepsilon}{2}}) n \rfloor \qquad d = \delta \cdot n$

Need to show $\forall\, \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$, $wt(\bar{m} G) \geq \delta n$. (+ show G has full rank)

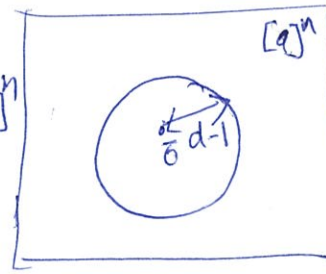
We will show

$(**) \rightarrow \Pr_G [\exists\, \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$ s.t $wt(\bar{m} G) < \delta n] < 1$.

By union bound $(**) \leq \sum_{\bar{m} \in \mathbb{F}_q^k \setminus \{0\}} \Pr[wt(\bar{m} G) < \delta n]$ — (@)

fix $\bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$

By Lemma 1, $\bar{m} G$ is uniformly random in $[q]^n$



$\Rightarrow \Pr[wt(\bar{m} G) < d] = \dfrac{Vol_q(d-1, n)}{q^n}$

$\leq \dfrac{Vol_q(\delta n, n)}{q^n} \leq \dfrac{q^{H_q(\delta) \cdot n}}{q^n} = q^{-n(1-H_q(\delta))}$

$\Rightarrow (@) \leq q^k \cdot q^{-n(1 - H_q(\delta))}$

$= q^{n(1 - H_q(\delta) - \varepsilon) - n(1 - H_q(\delta))}$

$= q^{-n\varepsilon} \ll 1$ ∎

Need to argue $\dim(\mathcal{C}) = k$ (i.e. G has full rank)

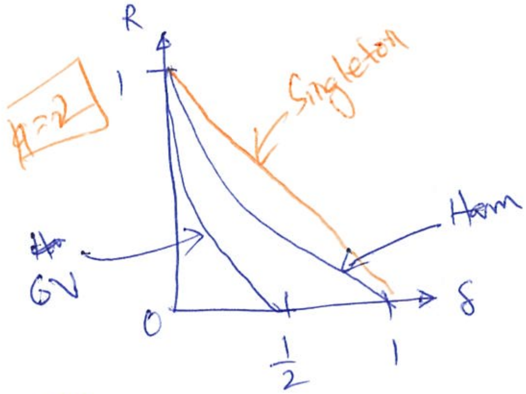
Option 1: Compute prob G is not full rank.

Option 2: wp $\geq 1 - q^{-\varepsilon n}$ $\mathcal{C}$ has dist $d \geq 1 \Rightarrow$ all messages are mapped to distinct codewords $\Rightarrow \dim(\mathcal{C}) = k$.

Singleton bound

THM: For every $(n,k,d)_q$ code C

$\Rightarrow k \le n-d+1 \qquad C \equiv R \le 1-\delta + o(1)$



→ $q=2$, worse than Hamming

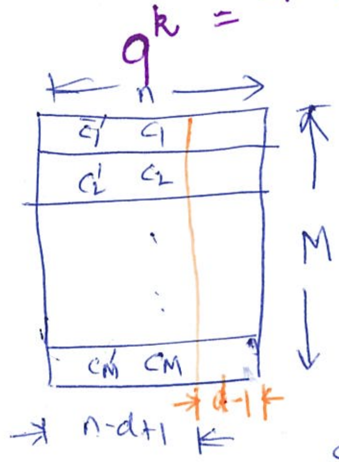
→ Show later as $q \to \infty$ (q depends on n), Singleton bound is tight.

Q5: Can we achieve $R = 1-\delta$ for *fixed* q.

Pf:

$C = \{\bar{c}_1, \dots, \bar{c}_M\}$

Goal $q^k = M \le q^{n-d+1}$



Claim $\forall\, i \ne j \quad \bar{c}_i' \ne \bar{c}_j'$

If not $\exists\, i \ne j \quad \bar{c}_i' = \bar{c}_j'$

$\Delta(\bar{c}_i, \bar{c}_j) = \Delta(\bar{c}_i \setminus \bar{c}_i', \bar{c}_j \setminus \bar{c}_j')$
$\le d-1$

$\Rightarrow$ contradicts that C has dist d.

$\Rightarrow M = |C| = |C'| \qquad C' = \{\bar{c}_i' \mid \bar{c}_i \in C\}$

since C' has length $n-d+1$

$\Rightarrow M = |C'| \le q^{n-d+1}$ ∎

Equivalent reduction: $\underset{(n,k,d)_q}{C} \longrightarrow \underset{(n-d+1,k,1)_q}{C'}$

Q2: Can we get $R>0$, $\delta > \frac{1}{2}$? $(q=2)$

Q3: Tighten gap between upper & lower bounds

Q5: Can we get $R = 1-\delta$ with constant q?

Plotkin bound: Let $C \subseteq [q]^n$ be a code of dist d:

(i) If $d = (1-\frac{1}{q})n \Rightarrow |C| \le 2qn$ [$q=2$, $|C| \le 2n$ tight]

(ii) If $d > (1-\frac{1}{q})n \Rightarrow |C| \le \dfrac{qd}{\underbrace{qd-(q-1)n}_{>0 \text{ \& has to be an int}}} \le qd.$

[$\equiv qd > (q-1)n$]

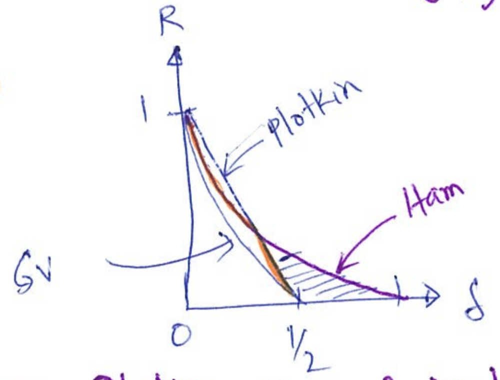
$\Rightarrow$ for $q=2$, $\delta \ge \frac{1}{2}$, $\dim(C)$ is $O(\log n) \Rightarrow R(C) = 0$

↳ NO to Q2.

Cor: Any q-ary code w/ rel. dist δ and rate R

$$R \leq 1 - \left(\frac{q}{q-1}\right)\delta + o(1)$$

$\boxed{q=2}$



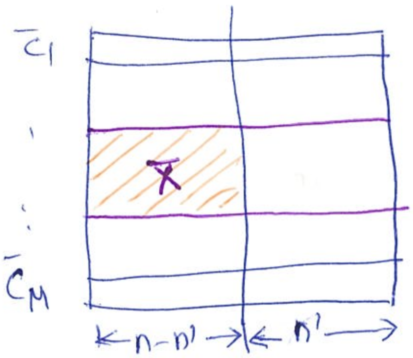
$\boxed{\text{YES to Q3}}$

NO to Q5:
for fixed q.
$R < 1 - \delta$

Assume Plotkin bound is true.

Pf of Corollary:

$$n' = \left\lfloor \frac{qd}{q-1} \right\rfloor - 1$$



$\forall \bar{x} \in [q]^{n-n'}$

$$C_{\bar{x}} = \{ (c_{n-n'+1}, \ldots, c_n) \mid (c_1, \ldots, c_n) \in C, \ (c_1, \ldots, c_{n-n'}) = \bar{x} \}$$

$\forall \bar{x}$, $C_{\bar{x}}$ has dist $\geq d$

block length of $C_{\bar{x}}$ is $n' < \frac{qd}{q-1}$

$\Leftrightarrow qd > n'(q-1)$

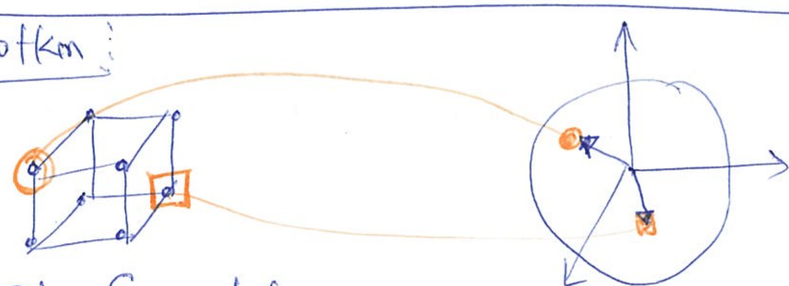
$\Rightarrow$ by (ii) of Plotkin bound, $|C_x| \leq qd$

$$\underset{q^{Rn}}{\overset{\parallel}{M}} = |C| = \sum_{\bar{x} \in [q]^{n-n'}} |C_{\bar{x}}| \leq \sum_{\bar{x} \in [q]^{n-n'}} qd = q^{n-n'} \cdot \underbrace{qd}_{q^{o(n)}}$$

$$\leq q^{n-n'+o(n)} \leq q^{n - \frac{qd}{q-1} + o(n)}$$

$$\Leftrightarrow q^{Rn} \leq q^{n - \left(\frac{q}{q-1}\right)\delta n + o(n)} \Rightarrow R \leq 1 - \frac{q\delta}{q-1} + o(1) \quad \blacksquare$$

Pf overview of Plotkin:



Mapping Lemma:
Rel Ham dist $\geq \left(1 - \frac{1}{q}\right)$
$\Rightarrow$ on sphere vectors are at an obtuse $\angle$.

Geometric Lemma: Cannot have many vectors on unit sphere with obtuse angles.