Feb 24

REMINDERS

(1) Video topic due (via Google form) by 11:59pm Wed.
↳ If you miss this deadline, ZERO ON REST of the project.

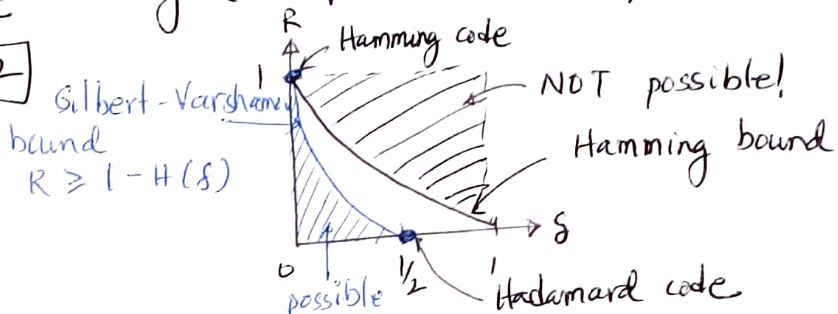
(2) New piazza response time policy

(3) Please ask Q if you do not understand something
↳ Asking Qs on the day HW is due is TOO LATE!

(4) Yunus OH changes forthcoming

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

→ $\boxed{q=2}$



→ Greedy construction (Gilbert) $R \geq 1 - H_q(\delta)$ not necessarily linear code

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

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

PLAN for TODAY / MONDAY

(•) Q1 : Can we achieve GV bound with linear code?

(•) Q2 : Can we have $(q=2)$ $R > 0$, $\delta > \frac{1}{2}$? $\left[\delta > 1 - \frac{1}{q}\right]$ Is inherently necessary or just a technical assumption

(•) Q3 : Other upper bounds?

(•) Q4 : Can we make the 'gap' space smaller?

Order of coverage: Q1, Q3, Q2+Q4

PROOF READER for today: Any volunteer? Phil

Varshamov construction: Linear codes achieve GV bound

∃ ~~linear~~ linear code w/ rel. dist δ & $R \geq 1 - H_q(\delta)$

Probabilistic method:

$R = (1 - H_q(\delta) - \varepsilon)n$

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

↑ By picking a random $G \in \mathbb{F}_q^{k \times n}$

$= \Pr[$ ______ ~~does NOT~~ has dist $< \delta] < 1$

Probability Lemmas:

(◦) Lemma 1: Let $\bar m \in \mathbb{F}_q^k$ be non-zero. Let $G \in \mathbb{F}_q^{k\times n}$ be chosen uniformly at random. $\Rightarrow$ $\bar m G$ is uniformly random over $\mathbb{F}_q^n$.

(◦) Union bound: $\Pr\left[\bigvee_{i=1}^{m} E_i\right] \le \sum_{i=1}^{m} \Pr[E_i]$

$E_i \in \{0,1\}$

Let $G \in \mathbb{F}_q^{k\times n}$ be a uniformly random matrix.

$k = \lfloor (1-H_q(\delta)-\varepsilon)n \rfloor$

We want to show that $\forall\, \bar m \in \mathbb{F}_q^k\setminus\{\bar 0\}$, $wt(\bar m G) \ge \delta n$

(negate $\exists\, \bar m \in \mathbb{F}_q^k\setminus\{\bar 0\}$, $wt(\bar m G) < \delta n$)

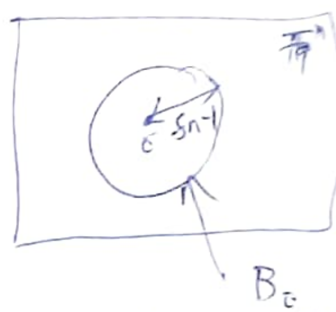
We'll show

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

$$\overset{\text{union bound}}{\le} \boxed{\sum_{\bar m \in \mathbb{F}_q^k\setminus\{\bar 0\}} \underbrace{\Pr[wt(\bar m G) < \delta n]}_{\text{bound this terms } < \frac{1}{q^k-1}}} \quad @$$

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

By Lemma 1 $\bar m G$ is uniformly random over $\mathbb{F}_q^n$



$$\Pr[wt(\bar m G) < \delta n] = \Pr[\text{random vector from } \mathbb{F}_q^n \text{ falls in } B_0]$$

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

$$\Rightarrow @ \le \sum_{\bar m \in \mathbb{F}_q^k\setminus\{\bar 0\}} q^{-n(1-H_q(\delta))} = (q^k-1)\, q^{-n(1-H_q(\delta))}$$

$$< q^k \cdot q^{-n(1-H_q(\delta))} \le q^{(1-H_q(\delta)-\varepsilon)n} \cdot q^{-n(1-H_q(\delta))}$$

$$= q^{-\varepsilon n} \underset{\varepsilon \ge 0}{\le} 1 \quad (<< 1 \text{ if } \varepsilon > 0).$$

∎

Still need to argue that $\dim(C) = k$ ($C \equiv G$ has full rank)

<u>Option 1:</u> With high probability G has full rank.

<u>Option 2:</u> w.p $> 1 - q^{-\varepsilon n}$, C has dist $d \geq 1$

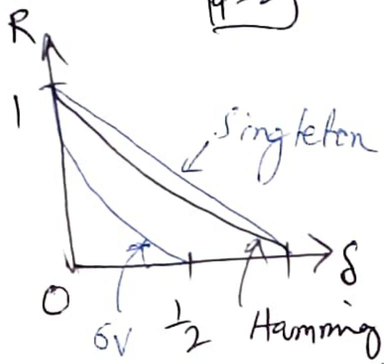
$\Rightarrow$ all messages are mapped to distinct codewords

$\Rightarrow G$ has full rank.

<u>Singleton bound</u> <u>THM:</u> For any $(n,k,d)_q$ code

$k \leq n-d+1 \equiv R < 1-\delta+o(1)$

$\boxed{q=2}$



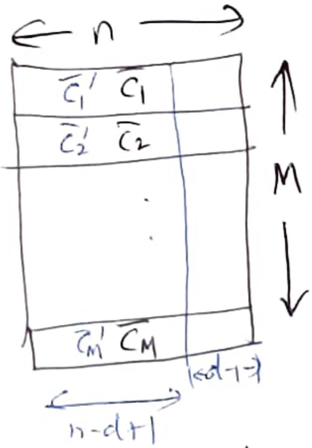
$\rightarrow q=2$, worse than Hamming

$\rightarrow$ show later as $q \to \infty$ (q depends on n)

Singleton bound is tight.

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

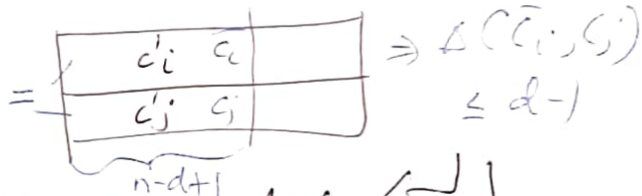
<u>Pf:</u> $C = \{\bar{c}_1, \dots, \bar{c}_M\}$ $M = q^k$



$\bar{c}_i'$ is $\bar{c}_i$ projected down to first $n-d+1$ position.

<u>Claim:</u> $\forall i \neq j$ $\bar{c}_i' \neq \bar{c}_j'$

Pf: If not $\bar{c}_i' = \bar{c}_j'$



C has dist $< d$ ✗ $\Leftarrow\!\!\lrcorner$

$C' = \{\bar{c}_i' \mid i \in [M]\}$

$\Rightarrow M = |C| = |C'|$

OTOH $|C'| \leq q^{n-d+1}$

$\Rightarrow q^k \leq q^{n-d+1} \Rightarrow k \leq n-d+1$ ∎