=: Trade-off b/w Rate & Distance- III :=

1. Asymptotic vesion of Hamming bound.

In Thm2, we have stated upper bound on k in terms of n, q & d. Here, we convert this into a relation on R vs δ.

Consider any $(n,k,d)_q$ code with rate $R = \frac{k}{n}$ & relative distance $\delta = \frac{d}{n}$.

$$\text{Thm2} \Rightarrow \quad R = \frac{k}{n} \leq 1 - \frac{\log_q Vol_q\left(\lfloor \frac{d-1}{2} \rfloor, n\right)}{n}$$

From Proposition 1, $Vol_q\left(\lfloor \frac{d-1}{2} \rfloor, n\right) \geq q^{H_q(\delta/2)n - o(n)}$

$$\Rightarrow \log_q Vol_q\left(\lfloor \frac{d-1}{2} \rfloor, n\right) \geq H_q(\delta/2)n - o(n)$$

$$\Rightarrow \frac{\log_q Vol_q\left(\lfloor \frac{d-1}{2} \rfloor, n\right)}{n} \geq H_q(\delta/2) - o(1)$$

$$\Rightarrow R \leq 1 - H_q(\delta/2) + o(1)$$

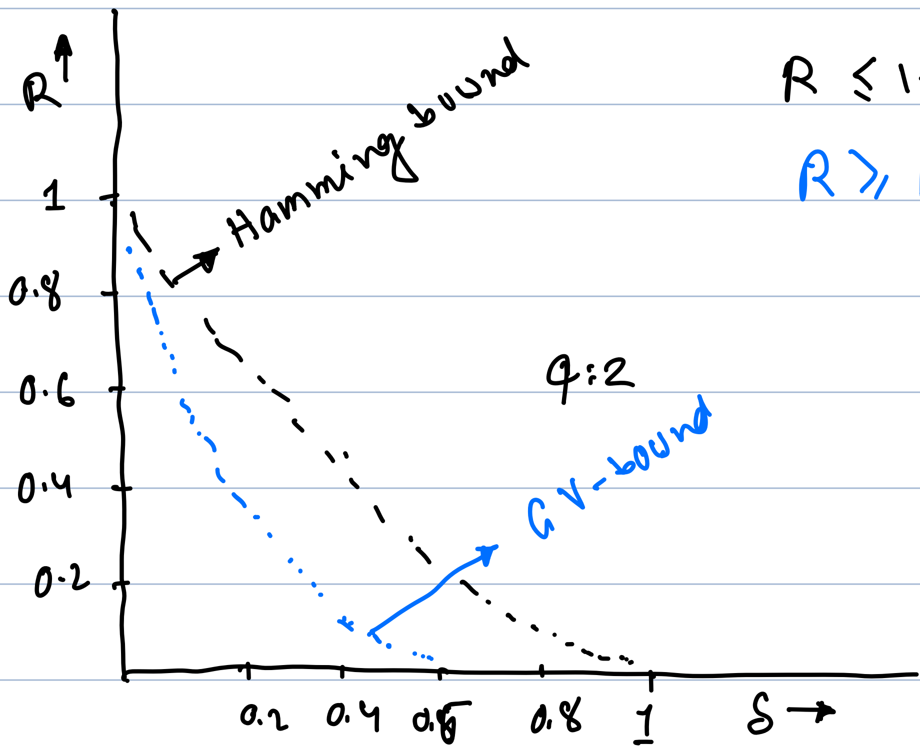
As $n \to \infty$, $o(1) \to 0$. Thus, for a family of codes C, taking limit as $n \to \infty$, we have the following asymptotic Hamming bound.

Theorem 1: (Asymptotic Hamming Bound): Let C be family of q-ary code with relative distance δ & rate R,

$$R \leq 1 - H_q(\delta/2).$$

Gilbert-Varshamov bound (GV-Bound):

Theorem 2: Let $q \in \mathbb{Z}_{\geq 2}$. Then, $\forall \delta \in [0, 1-1/q]$, $\exists$ a q-ary code with rate $R \geq 1 - H_q(\delta)$ & relative distance δ. If q is a prime power, $\exists$ such a q-ary family linear codes. Furthermore, $\forall\, \varepsilon \in [0, 1-H_q(\delta)]$, & $n \in \mathbb{N}$, if we randomly & uniformly pick a generator matrix of code length n & rate $1-H_q(\delta)-\varepsilon$, then code has relative distance $\geq \delta$ w.p. $> 1 - q^{-\varepsilon n}$



$R \leq 1 - H_2(\delta/2)$

$R \geq 1 - H_2(\delta)$

- $\varepsilon = 0 \Rightarrow$ the first part of the thm.

Remark: Theorem 1 & Theorem 2 $\Rightarrow$

for a fixed constant $q \in \mathbb{Z}_{\geq 2}$ & $\delta \in [0, 1-\frac{1}{q}]$ a q-ary code family C with rate R & relative dist δ.

$$1 - H_q(\delta) \leq R \leq 1 - H_q(\delta/2)$$

Question 1: Does $\exists$ asymptotically good a q-ary code family for $\delta > 1 - \frac{1}{q}$?

Question 2: for $\delta \in [0, 1-\frac{1}{q}]$, does $\exists$ a q-ary code family C with rate R & relative distance δ. s.t. $R > 1 - H_q(\delta)$?

First, we see a greedy construction of code, may not be linear, that satisfies GV-bound. Then,

Greedy construction:

Σ - alphabet of size q.

Input: $n, q, d = \delta n > 0$

Output: $(n, k, d)_q$ code C with $R = \frac{k}{n} \geq 1 - H_q(\delta)$.

1. $C \leftarrow \emptyset$
2. while $\exists$ a $v \in \Sigma^n$ s.t. $\Delta(v, c) \geq d$ $\forall c \in C$. Do
3. Add $v \in C$.
4. Return C.

Stops in finite time — [Explain]

Time-Complexity: $q^{O(n)}$ → [Explain]

Claim: On the termination of the algorithm,

$$\bigcup_{c \in C} B_q(c, d-1) = \Sigma^n$$ → [Explain Proof]

Claim ⟹ $$\left| \bigcup_{c \in C} B_q(c, d-1) \right| = q^n$$

$$\Rightarrow \sum_{c \in C} |B_q(c,d-1)| \geq \left| \bigcup_{c \in C} B_q(c,d-1) \right| = q^n$$

$$\Rightarrow \quad |C| \cdot Vol_q(d-1, n) \geq q^n$$ [Complete the rest of the proof]

Existence of Linear Code satisfying GV-bound!

- Set up: $\Sigma = \mathbb{F}_q$; $\delta \in [0, 1-\frac{1}{q}]$; $\varepsilon \in [0, 1-H_q(\delta)]$; $k = (1 - H_q(\delta) - \varepsilon)n$;
- Goal: For $G \in_r \mathbb{F}_q^{k \times n}$, G is a generator matrix of $[n, k, d]_q$ with $d \geq \delta n$

Need to show that for $G \in_r \mathbb{F}_q^{k \times n}$ w.p. $\geq 1 - q^{-\varepsilon n}$,

- distance of code generated by G is $\geq \delta n$
- $\text{rank}(G) = k$

⇕ [Explain]

$$\boxed{\forall x \in \mathbb{F}_q^n \setminus \{0\},\ wt(xG) \geq \delta n}$$

Fix a $\underline{\text{non zero}}$ $m = (m_1, m_2, \ldots, m_k) \in \mathbb{F}_q^k$.

$\mathbb{F}_q^{k \times n}$ $\qquad\qquad$ $\mathbb{F}_q^{n}$

uniformly at random $\qquad\qquad$ uniformly at random

$$G \xmapsto{\;m \cdot G\;} b = (b_1, b_2, \ldots, b_n)$$

[Explain]

$$\Pr[\mathrm{wt}(xG) < \delta n] \leq \frac{\mathrm{Vol}_q(\delta n, n)}{q^n} \leq q^{H_q(\delta)n - n}$$

$\Downarrow$ [Union-bound]

$$\Pr[\exists \text{ non-zero } x \in \mathbb{F}_q^k \text{ s.t. } \mathrm{wt}(xG) < \delta] \leq (q^k - 1) \cdot q^{H_q(\delta)n - n}$$

$$= (q^k - 1) \cdot q^k \cdot q^{-\varepsilon n}$$

$\Rightarrow$ G is a generator matrix of our desired code is $\geq 1 - q^{-\varepsilon n}$.