# =: Trade-off b/w Distance & Rate - IV :=

## Recap of Last class:

- **Asymptotic Hamming Bound:** For any $q$-ary code family $C$ with Rate $R$ & relative distance $\delta$,
$$R \leq 1 - H_q(\delta/2).$$
- **GV-Bound:** for any $q \in \mathbb{Z}_{\geq 2}$ & $\delta \in [0, 1-\frac{1}{q}]$,
  - $\exists$ a $q$-ary code family with rate $R \geq 1 - H_q(\delta)$ & relative distance $\delta$.
  - if $q$ is a prime power, then $\exists$ a $q$-ary linear code family with $R \geq 1 - H_q(\delta)$ & relative distance $\delta$.

Furthermore, $\forall \varepsilon \in [0, 1 - H_q(\delta)]$ & $n \in \mathbb{Z}_{\geq 1}$, if a matrix $A$ is picked uniformly at random from $\mathbb{F}_q^{k \times n}$ with $k = n(1 - H_q(\delta) - \varepsilon)$, the $A$ generates a radom code of rate $(1 - H_q(\delta) - \varepsilon)$ & relative distance $\geq \delta$ w.p. $> 1 - q^{-\varepsilon n}$

**Q1:** for $q \in \mathbb{Z}_{\geq 2}$ & $\delta \in [0, 1-\frac{1}{q}]$. does $\exists$ a code with
$$1 - H_q(\delta/2) \geq R > 1 - H_q(\delta)$$

**Q2:** Does $\exists$ an asymptotically good $q$-ary code with $\delta > 1 - \frac{1}{q}$?

## Today's Class:

- Complete GV-bound
- Singleton Bound
- Plotkin Bound. (It will answer Q2).

# Discussion on GV-Bound.

- Discuss about the time complexity of constructing a linear code achieving GV-bound.

  Input: $n$, $k = (1 - H_q(\delta) - \varepsilon)n$, $d = \delta n$

  Output: a generator matrix $G$ for $[n, k, d]_q$-code.

The proof of GV-bound gives an algorithm with time complexity $q^{O(kn)}$.

- worse than the greedy algorithm.

Q3: Can we design an algorithm of time complexity $q^{O(n)}$?

**Heart of the Proof:**

fix $\quad m = (m_1, \ldots, m_k) \in \mathbb{F}_q^k \setminus \{0\}$.

$$G \in_r \mathbb{F}_q^{k \times n} \longmapsto m \cdot G \longrightarrow b = (b_1, \ldots, b_n) \in_r \mathbb{F}_q^n$$

In the left hand-side, "amount of randomness we are investing" is $kn$ many independent & uniform random elements from $\mathbb{F}_q$, but on the right side we are getting only $n$ many independent & uniformly chosen random elements. [Massive loss in randomness $kn \to n$]. [Trivial Derandomisation].

Goal: Construct a random matrix $G \in \mathbb{F}_q^{k \times n}$ s.t.

- instead of $kn$ many independent & uniformly chosen random elements, we pick $O(n)$ many elements of $G$ uniformly at random, & other elements are derived from that.

- Fix $m \in \mathbb{F}_q^k \setminus \{0\}$.
  : $m \cdot G = (b_1, \ldots, b_n) \in_r \mathbb{F}_q^n$.

$\Rightarrow$ we have an algorithm of constructing $[n, k, d]_q$ code with $k = (1 - H_q(\delta) - \varepsilon)n$ & $d = \delta n$; & running time is $q^{O(n)}$.

Toeplitz matrix: $M \in \mathbb{F}_q^{k \times n}$ is called Toeplitz matrix if $\forall\ i \in \{2, 3, \ldots, k\}$ & $j \in \{2, 3, \ldots, n\}$

$$M[i, j] = M[i-1, j-1].$$

Example:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 1 & 2 & 3 & 4 & 5 \\ 8 & 7 & 1 & 2 & 3 & 4 \\ 9 & 8 & 7 & 1 & 2 & 3 \end{bmatrix}$$

One can show that if $G$ is a random toeplitz matrix, $\cdot\ mG = (b_1, \ldots, b_n) \in_r \mathbb{F}_q^n$ [Exercise]

[Better than trivial Derandomization].

One can further improve the time complexity to $q^{O(k)}$. [See Exercise 4.8 in Essential Coding Theory].

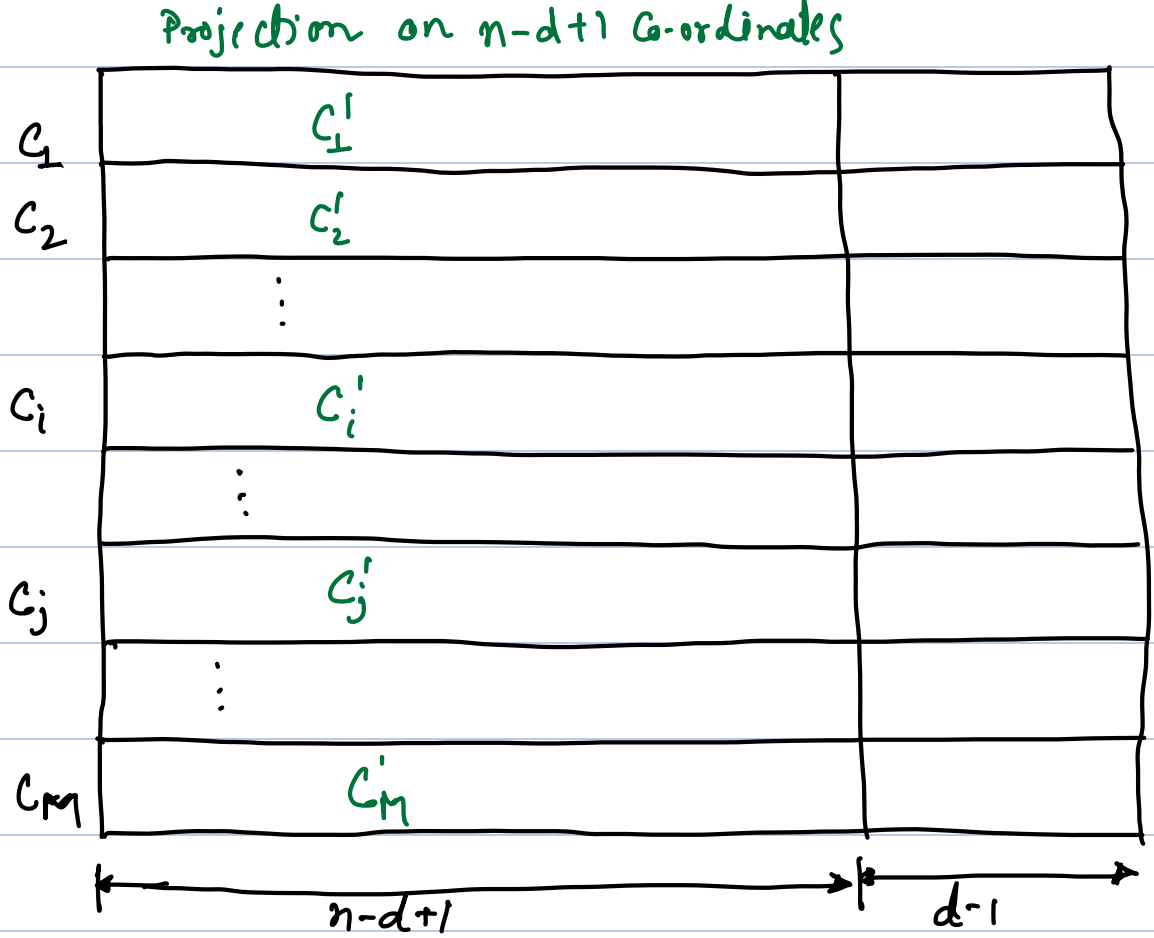
[Much better derandomization when $k = o(n)$].

**Singleton bound:** $\forall$ $(n, k, d)_q$ code

$k \leq n - d + 1$. [negative result].

Consequently, for a code family $C$ with rate $R$ & relative distance $\delta$, $R \leq 1 - \delta$.

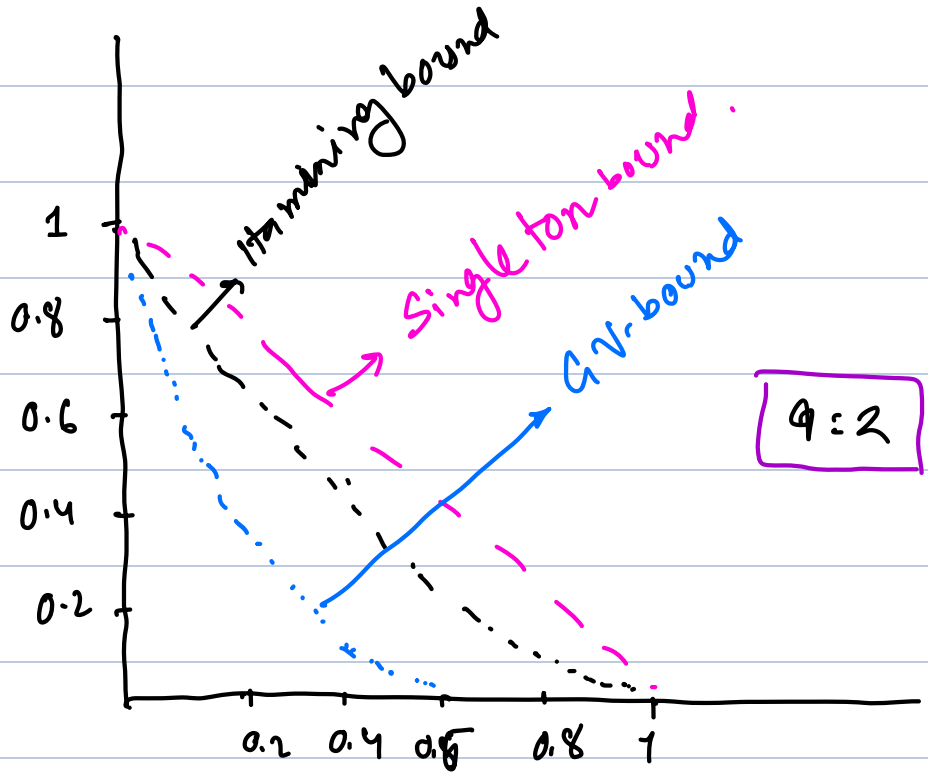
**Proof Idea:** Let $c_1, \ldots, c_M$ be the code words.




$\forall i \neq j \in [M]$, $c_i' \neq c_j' \Rightarrow M \leq q^{n-d+1}$

$\Rightarrow k = \log_q M \leq n - d + 1$

$\Rightarrow R \leq 1 - \delta$




Remarks:
- Independent of alphabet size.
- For $q=2$, Singleton bound is worse than Hamming bound.
- As $q$ becomes larger, singleton bound improves.
- Reed-Solomon codes achieves Singleton bound; but $q \geq n$, i.e., $q \to \infty$ as $n \to \infty$

Q4: Does $\exists$ a $q \in \mathbb{Z}_{\geq 2}$ s.t. $\exists$ a $q$-ary code achieving Singleton bound?

Answer: No!

→ Analytic approach: show $\delta > H_q(\delta/2)$;

→ Coding Theoretic approach via Plotkin approach:

$\forall$ $q$-ary code family $C$ with relative distance $0 \leq \delta \leq 1 - 1/q$ & rate $R$, $R \leq 1 - \left(\frac{q}{q-1}\right)\delta$.

**Theorem 1 (Plotkin bound):** For any code $C \subseteq \Sigma^n$ with $|\Sigma| = q$ & $\text{dist}(C) = d$, the following holds:

i) If $d = (1 - \frac{1}{q})n$, $|C| \leq 2qn$

ii) If $d > (1 - \frac{1}{q})n$, $|C| \leq \frac{qd}{qd - (q-1)n}$

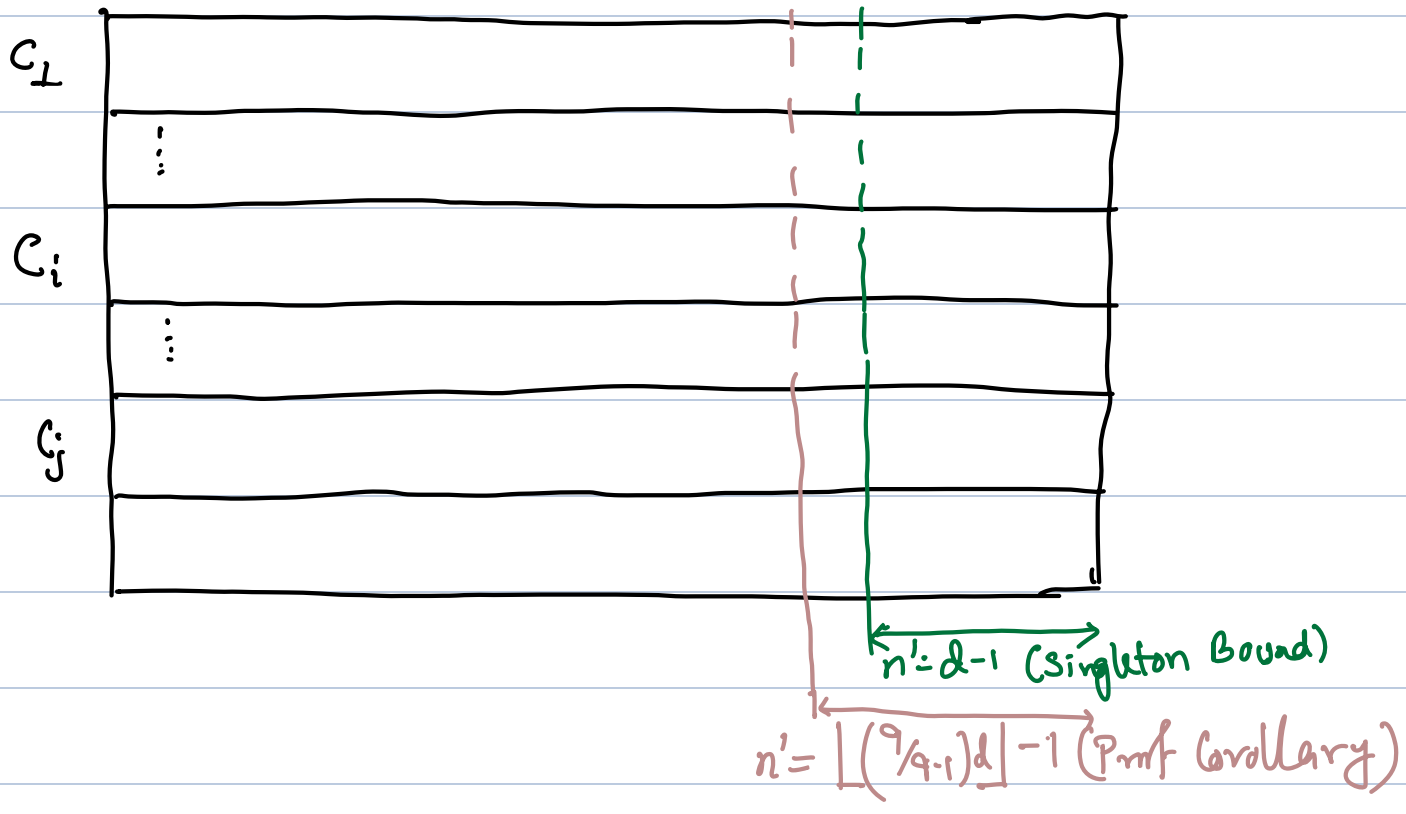
Plotkin bound answers Q2 negatively.

Answering Q4 via Plotkin bound:

**Corollary:** For any $q$-ary code family with relative distance $\delta \in [0, 1 - \frac{1}{q}]$ & rate $R$,

$$R \leq 1 - \left(\frac{q}{q-1}\right)\delta.$$ [improve upon singleton bound].

**Proof Idea:** Fine tuning the proof of Singleton bound.



In Singleton bound, $\forall x \in \Sigma^{n-n'}$

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

$$|C_x| \leq 1 \Rightarrow |C| \leq \sum_{x \in \Sigma^{n-n'}} |C_x| \leq q^{n-n'} = q^{n-d+1}$$

In the proof of Corollary.

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

We show that $C_x$ is a code of block length $n'$ & distance $d$ [Explain].

Additionally, $C_x$ satisfy the hypothesis of plotkin bound [Explain]

$$\Rightarrow |C_x| \leq \frac{qd}{qd - (q-1)n'} \leq qd \leq qn\frac{q-1}{q} = n(q-1)$$

$$\Rightarrow |C| \leq \sum_{x \in \Sigma^{n-n'}} n \cdot q \leq nq\, q^{n-n'+1}$$

$$= n \cdot q^{n-n'+O(\log_q n)}$$

$$= q^{n - \frac{q}{q-1}\delta n + O(\log_q n)}$$

$$= q^{n}$$

$$\Rightarrow \frac{\log_q |C|}{n} \leq 1 - \frac{q}{(q-1)} \cdot \delta, \text{ since } \frac{\log n}{n} \to 0 \text{ as } n \to \infty.$$

# =: Trade-off b/w Distance & Rate - V :=

**Proof of Plotkin bound:** A simple double counting based for the part-II of Plotkin bound is given in the assignment. We see a different proof, more geometric in nature.

We need two lemmas for the proof.

**Lemma 1:** Let $v_1, \ldots, v_m \in \mathbb{R}^N$ be non-zero vectors.

1. if $\langle v_i, v_j \rangle \leq 0 \ \forall\ i \neq j$. then $m \leq 2N$.
2. $\|v_i\|_2 = 1 \ \forall\ i \in [m]$ & $\langle v_i, v_j \rangle \leq -\varepsilon < 0 \ \forall\ i \neq j \in [m]$
   $\Rightarrow m \leq 1 + 1/\varepsilon$.

**Remarks:** Both 1 & 2 are tight in the above lemma.
[Exercise 4.15 & 4.16 of Essential Coding Theory]

The next lemma is about encoding of strings $\Sigma^n$ to real vectors with certain properties useful for proving Plotkin bound.

**Lemma 2:** $\forall\, q, n \in \mathbb{Z}_{\geq 1}$ and a finite set $\Sigma$ with $|\Sigma| = q$

$\exists$ a function $f: \Sigma^n \longrightarrow \mathbb{R}^{nq}$ s.t. $\forall\, c_1, c_2 \in \Sigma^n$,

$$\langle f(c_1), f(c_2) \rangle = 1 - \left(\frac{q}{q-1}\right) \cdot \left(\frac{\Delta(c_1, c_2)}{n}\right) \quad \text{---- (Eqn. 1)}$$

Consequetly, we get

1. $\forall\, c \in \Sigma^n$, $\|f(c)\|_2 = 1$.
2. $\Delta(c_1, c_2) \geq d \Rightarrow \langle f(c_1), f(c_2) \rangle \leq 1 - \left(\frac{q}{q-1}\right)\frac{d}{n}$

**Proof of Plotkin bound using Lemma 1 & Lemma 2:**

Let $C = \{c_1, \ldots\ldots, c_m\}$ & $f: \Sigma^n \longrightarrow \mathbb{R}^{nq}$ be the function promised by Lemma 2.

Then, $\forall\ i \neq j \in [m]$

$$\langle f(c_i), f(c_j) \rangle \leq 1 - \frac{q}{q-1} \cdot \frac{d}{n} = \frac{(q-1)n - qd}{(q-1)n}.$$

$d = (1 - \frac{1}{q})n \Rightarrow qd - (q-1)n = 0$

Therefore, $\langle f(c_i), f(c_j) \rangle \leq 0$

$\Rightarrow m \leq 2qn$ [from Lemma 1].

**Proof of Part - II.** $d > (1 - \frac{1}{q})n$

$\Rightarrow dq - (q-1)n > 0$

Let $\varepsilon = \dfrac{dq - (q-1)n}{(q-1)n}$

$\Rightarrow \langle f(c_i), f(c_j) \rangle \leq -\varepsilon < 0$

$\Rightarrow m \leq 1 + 1/\varepsilon$

$= 1 + \frac{(q-1)n}{dq-(q-1)n} = \frac{dq}{dq-(q-1)n}$ . □ .

**Proof of Lemma 2:** Construct $\Phi : \Sigma \to \mathbb{R}^q$ that satisfies the property in Eqn. 1 (upto scaling) & then essentially we construct desired $f$ for general $n$ by applying $\Phi$ separately to each coordinate.

- **Constructing $\Phi$:** $e_i$ : $i^{th}$ Canonical vector in $\mathbb{R}^q$.

$$\bar{e} = \frac{1}{q} \sum_{i=1}^{q} e_i ;$$

$\forall\, i \in \Sigma = [q]$, , $\Phi(i) = e_i - \bar{e}$

**Observation:** $\|\Phi(i)\|^2 = \frac{q-1}{q}$.

$$\langle \Phi(i), \Phi(j) \rangle = -\frac{1}{q} .$$

$\Rightarrow f : \Sigma \to \mathbb{R}^q$ is defined as follows.

$$f = \sqrt{\frac{q}{q-1}} \cdot \Phi .$$

For general $n$,

$$f(c_1, \ldots, c_n) = \sqrt{\frac{q}{(q-1)n}} \cdot (\Phi(c_1), \ldots, \Phi(c_n)) .$$

**Proof of lemma 1:** $\exists$ a vector $u \in \mathbb{R}^N$ s.t. $\langle u, v_i \rangle \neq 0$

[why? Explain].

$\Rightarrow \exists$ a vector $u \in \mathbb{R}^N$ s.t. for at least half $v_i$'s, $\langle u, v_i \rangle > 0$ [why? Explain].

After relabelling, we can assume that in $v_1, v_2, \ldots, v_\ell$, are the vectors s.t. $\langle u, v_i \rangle > 0 \ \forall i \in [\ell]$.

$\ell \quad \ell \geq m/2$

**Goal:** $v_1, v_2, \ldots, v_\ell$ are linearly independent.

$$\Rightarrow \quad \frac{m}{2} \leq \ell \leq N \Rightarrow m \leq 2N.$$

For the sake of contradiction assume that, $\exists \alpha_1, \ldots, \alpha_\ell$ with at least one $\alpha_i \neq 0$ s.t. $\sum_{i \in [\ell]} \alpha_i v_i = 0$

$\Rightarrow \exists \alpha_1 \ldots, \alpha_\ell$ s.t. $\sum_{i \in [\ell]} \alpha_i v_i = 0$ & $\exists \alpha_i > 0$

after relabelling let $\alpha_1, \dots, \alpha_k > 0$ & $\alpha_{k+1}, \dots, \alpha_\ell < 0$.

$$\Rightarrow w = \sum_{i=1}^{k} \alpha_i v_i = -\sum_{j=k+1}^{\ell} \alpha_j v_j$$

$$\Rightarrow \langle u, w \rangle = \Big(u, \sum_{i=1}^{k} \alpha_i v_i\Big) \geq \alpha_1 \langle u, v_1 \rangle > 0.$$

$$\Rightarrow w \text{ is non-zero.}$$

$$\Rightarrow 0 < \langle w, w \rangle = \Big\langle \sum_{i=1}^{k} \alpha_i v_i, -\sum_{j=k+1}^{\ell} \alpha_j v_j \Big\rangle = -\sum_{i=1, j=k+1}^{k\ \ell} \alpha_i \alpha_j \langle v_i, v_j \rangle \leq 0$$

Contradiction!

Proof of part II: $z = v_1 + \cdots + v_m$

$$\|z\|^2 = \sum_{i=1}^{m} \|v_i\|^2 + 2 \sum_{i<j} \langle v_i, v_j \rangle$$

$$\leq m + 2 \cdot \binom{m}{2} (-\varepsilon)$$

$$= m\left[1 - \varepsilon m + \varepsilon\right]$$

$$\Rightarrow m(1 - \varepsilon m + \varepsilon) \geq 0$$

$$\Rightarrow 1 - \varepsilon m + \varepsilon \geq 0$$

$$\Rightarrow \varepsilon m \leq 1 + \varepsilon$$

$$\Rightarrow m \leq 1 + 1/\varepsilon \qquad \square.$$