3|2|2021

Lecture 8 (Bounds on parameters of codes)

Recap

Standard array decoding → Coset leaders are the correctable error patterns
Syndrome decoding ↗

There is a one-to-one mapping between syndromes and coset leaders.

Hamming bound for linear codes

For any (n, k, d) linear code.

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

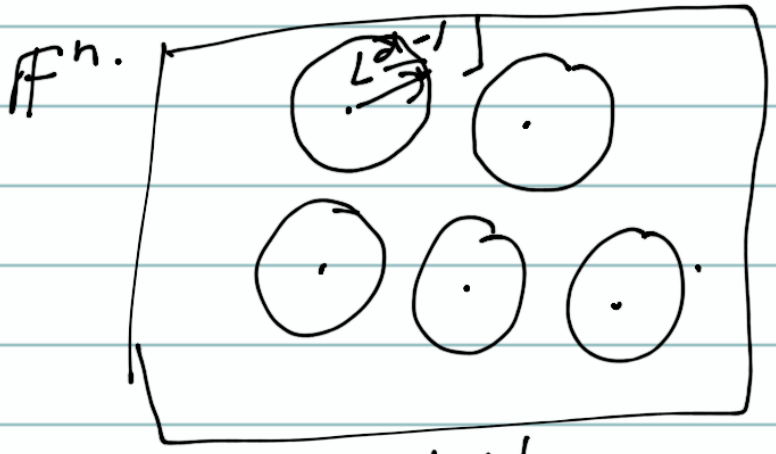
Sphere Packing Bound.

Generalization of the Hamming bound to general block codes. (n, M, d) over $\mathbb{F}$ $|\mathbb{F}| = q$.

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq \frac{q^n}{M}$$

Proof:-

Hamming balls of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ around each codeword.



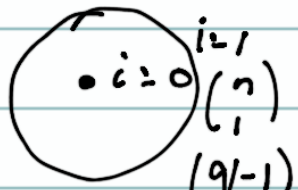
All the Hamming balls are disjoint

How many Hamming balls are there?

$$M \cdot \sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i \leq q^n.$$

$i=0 \rightarrow$ includes the codewords.

$$\sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i \leq \frac{q^n}{M}.$$



$$M \leq \frac{q^n}{\sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i}$$

2 1 1 0 2.

5 → 1 or 0

1 1 1 0 2

0 1 1 0 2

2 2 1 0 2

2 0 1 0 2.

Example: What is the largest no. of codewords in a single-error correcting binary block code of length 6?

$M \leq 9$. ✓

$(6, 10, 3)$ does not exist follows from sphere packing bound ✓

$(6, 9, 3)$ over $\mathbb{F}_2$. $d_{min} \geq 3$ ← It is possible to show by some other means that $(6, 9, 3)$

$(6, 8, 3)$ Code exists over $\mathbb{F}_2$.

$(6, 3, 3)$ ← linear code $k = 3$, $q^k = 8$.

↑ name of a person.

Singleton Bound

statement of Singleton bound for linear codes.

For any (n, k, d) code over $\mathbb{F}_q$;

$$d \leq n - k + 1$$

Proof: We had a lemma relating the parity check matrix to the minimum distance.

Let s denote the largest integer such that any s columns of H are linearly independent.

Then $s = d - 1$.

$s \leq n - k$ (Because size of matrix H is $(n-k) \times n$)

$$(d-1) \leq n-k$$

$$\boxed{d \leq n-k+1}.$$

Singleton bound for general block codes

For any (n, M, d) code over $\mathbb{F}$:

$$\boxed{d \leq n - \lceil \log_q M \rceil + 1}$$

For linear code, $M = q^k$.

$$d \leq n - \lceil \log_q q^k \rceil + 1 = n-k+1.$$

→ Proof:- Say $l = \lceil \log_q M \rceil - 1$

$$l < \log_q M \Rightarrow q^l < M.$$

Consider first l coordinates of codewords in the code.

In how many ways can we fill the first l coordinates → q^l ways.

But there are M codewords in the code where $M > q^l$.

.

.

$\exists$ at least two codewords which have the same entries in the first l coordinates.

Let the two codewords be $\underline{c}$ and $\underline{c}'$.

$$d \leq d_H(\underline{c}, \underline{c}') \leq n - l$$

$$= n - \lceil \log_q M \rceil + 1$$

$$\boxed{d \leq n - \lceil \log_q M \rceil + 1}$$

Defn:- A (n, k, d) linear code which satisfies singleton bound with equality i.e., $d = n - k + 1$, then the code is called a Maximum Distance Separable Code (MDS Codes).

Examples of MDS Codes

① $(n, 1, n)$ repetition code over $\mathbb{F}_2$.

$$d = n - k + 1$$

$$n = n - 1 + 1.$$

② $(n, n-1, 2)$ Simple parity check code over $\mathbb{F}_2$.

$$d = n - k + 1, \quad 2 = n - (n-1) + 1$$

Repetition Code & simple parity check Code are duals of each other.

→ Dual of an MDS is also an MDS Code.

→ Over $\mathbb{F}_2$, the above shown examples are the only possible MDS Codes. (Requires a proof; part of Assgn 4)

Popular class of MDS Codes over finite fields are Reed Solomon Codes.

Plotkin Bound for General Block Codes

For an (n, M, d) block code over F,

$$\boxed{M \leq \frac{d}{d - \theta n}} \quad \text{for} \quad \boxed{d > \theta n.}$$

$$\theta = 1 - \frac{1}{q}.$$

For the case of linear codes

$$q^k \leq \frac{d}{d - \theta n} = \frac{d}{d - \left(1 - \frac{1}{q}\right) n}.$$

$\Downarrow$

can be rewritten as

$$d \leq \frac{n\left(q^k - q^{k-1}\right)}{q^k - 1}$$

Proof of Plotkin Bound

$\mathbb{C}$ (n, M, d) block code over $\mathbb{F}$

$$S = \sum_{\underline{u} \in \mathbb{C}} \sum_{\underline{v} \in \mathbb{C}} d_H(\underline{u}, \underline{v}).$$

$$\underline{u} \neq \underline{v}.$$

How many terms in the sum?

$$= M(M-1).$$

$$d_H(\underline{u}, \underline{v}) \geq d.$$

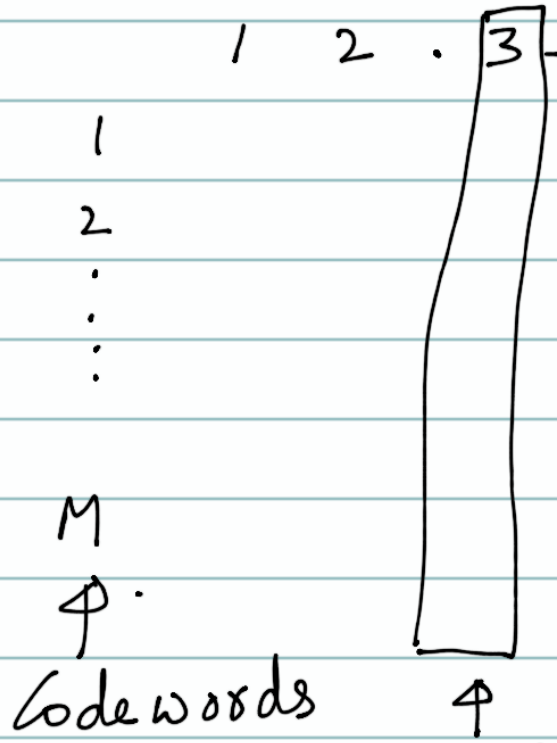
We can lower bound S as

$$\boxed{S \geq M(M-1)d.}$$

In the next part of the proof, we will derive an upper bound on S in terms of θ, n.

To get the upper bound, first get an alternate expression for S in terms of m_j.

m_j is the no. of times symbol $j \in \mathbb{F}$ appears in a particular column



All the codewords in the code can be arranged in the form of an array.

$m_{i,1}, \ldots, m_{i,q}$: $\sum_{j \in \mathbb{F}} m_{i,j} = M$

$d_H(\underline{u}, \underline{v})$

$$S = \sum_{\underline{u} \in C} \sum_{\substack{\underline{v} \in C \\ \underline{u} \neq \underline{v}}} d_H(\underline{u}, \underline{v}).$$

$$\Pi(u_i \neq v_i) = \begin{cases} 1 & \text{if } u_i \neq v_i \\ 0 & \text{if } u_i = v_i \end{cases}$$

$$= \sum_{\underline{u} \in C} \sum_{\substack{\underline{v} \in C \\ \underline{u} \neq \underline{v}}} \sum_{i=1}^{n} \Pi(u_i \neq v_i)$$

$$= \sum_{i=1}^{n} \left[\sum_{\underline{u} \in C} \sum_{\substack{\underline{v} \in C \\ \underline{u} \neq \underline{v}}} \Pi(u_i \neq v_i) \right]$$

Internal Summation corresponding to one column is given by

$$\sum_{\substack{\underline{u} \in \mathbb{C} \\ \underline{u} \neq \underline{v}}} \sum_{\underline{v} \in \mathbb{C}} \mathbb{I}(u_i \neq v_i) = \sum_{j \in \mathbb{F}} m_j (M - m_j).$$

$$S = \sum_{i=1}^{n} \sum_{j \in \mathbb{F}} m_j (M - m_j).$$

$$= \sum_{i=1}^{n} \left[M \sum_{j \in \mathbb{F}} m_j - \sum_{j \in \mathbb{F}} m_j^2 \right]$$

$$= \sum_{i=1}^{n} \left(M^2 - \sum_{j \in \mathbb{F}} m_j^2 \right).$$

Need a upper bound on S

$\Rightarrow$ Need a lower bound on $\sum_{j \in \mathbb{F}} m_j^2$.

What is the minimum value $\sum_{j \in \mathbb{F}} m_j^2$ will take subject to $\sum_{j \in \mathbb{F}} m_j = M$.

Guess the choice of m_j which will give the min. value

$$m_j = \frac{M}{q} \quad \forall j$$

Min value of $\sum_{j \in \mathbb{F}} m_j^2 = \frac{M^2}{q^2} \cdot q = \frac{M^2}{q}$.

$$S \leq \sum_{i=1}^{n} \left(M^2 - \frac{M^2}{q} \right) = n\left(1 - \frac{1}{q}\right) M^2 = n\theta M^2.$$

Putting the upper bound and lower bound.

$$M(M-1)d \leq S \leq n\theta M^2$$

$$\boxed{M(M-1)d \leq n\theta M^2}$$

$$M^2(d - \theta n) \leq dM$$

$$\Downarrow$$

$$\boxed{M \leq \frac{d}{d - \theta n}} \quad \text{for } d > \theta n.$$

Next time: Gilbert-Varshamov Bound (Guarantees Existence of linear codes)