5/2/2021

Lecture 9 (Gilbert Varshamov Bound, Finite Fields)

· **Announcements**

1. 2^{nd} Quiz on 14th Feb
2. We will send list of term papers
3. 2 more Assignments coming up

Recap

(Bounds on the parameters of codes)

→ Hamming Bound (Linear)

→ Sphere Packing bound (General).

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

$$\le \frac{q^n}{M}.$$

→ Singleton bound. → Linear $d \le n-k+1$

Nonlinear

$$d \le n - \lceil \log_q M \rceil + 1.$$

→ Plotkin Bound

$$M \leq \frac{d}{d-\theta n}, \quad d > \theta n, \quad \theta = 1 - \frac{1}{q}.$$

Gilbert - Varshamov Bound

Previous bounds are infeasibility results.

→ Achievability

Theorem: Let $\mathbb{F}$ be a field & n, k, d be +ve integers such that

$$\boxed{\sum_{l=0}^{d-2} \binom{n-1}{l} (q-1)^{l} < q^{n-k}.}$$

In that case, there exists a (n, k) linear code over the field $\mathbb{F}$ such that $d_{min} \geq d$.

Proof: Proof by construction.

→ Construct a parity check matrix H. Such that any $(d-1)$ columns of H are linearly independent. $(s \geq d-1) \Rightarrow d_{min} \geq d$.

Recursive procedure to construct H:

① Pick the first column $\underline{h}_1$ to be any nonzero vector in $\mathbb{F}^{n-k}$.

② Pick the second column $\underline{h}_2$ as any nonzero vector in $\mathbb{F}^{n-k}$ which is not a multiple of $\underline{h}_1$.

③ Suppose you have picked $\underline{h}_1 \dots \underline{h}_{i-1}$, pick $\underline{h}_i$ so that it is not contained in the span of any $d-2$ columns of $\underbrace{\underline{h}_1 \dots \underline{h}_{i-1}}$.

Let V_i denote the no. of vectors which are in the span of any $d-2$ columns of $\underline{h}_1 \dots \underline{h}_{i-1}$.

$$V_2 = q-1.$$

$$\boxed{V_i = \sum_{l=0}^{d-2} \binom{i-1}{l} (q-1)^l.}$$

$\underline{\underline{d=5}}$

$$V_2 = 1 + (q-1).$$

If $V_i < q^{n-k}$ (say), there exists a $\underline{h_i}$ to be added in the ith round of your recursion.

In the theorem statement, the condition is

$$\sum_{l=0}^{d-2} \binom{n-1}{l} (q-1)^l < q^{n-k}.$$

$$\underline{\underline{V_n < q^{n-k}}}$$

Based on defn of V_i;

$$V_1 \leq V_2 \leq \dots \leq V_n < q^{n-k}$$

The condition in the theorem statement guarantees that we are execute n rounds of recursion $\Rightarrow$ We can find a H matrix of size $(n-k)\times n$ such that any $d-2$ columns of H are linearly independent.

Finite Fields

(Prime Fields)

$d-1 \le n-k$

Defn:-

A field $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$. with operators of "+" addition & "·" multiplication which satisfy the following conditions:-

(i) $(\mathbb{F}, +) \rightarrow$ Abelian group
- → closure
- → Commutative
- → Associative
- → Existence of identity
- → Existence of inverse

(ii) $\forall\, a, b \in \mathbb{F},\ a.b \in \mathbb{F}$, closure under multiplication

(iii) $a(bc) = (ab)c \rightarrow$ Associative

(iv) Existence of 1, $1.a = a.1 = a$..

(v) Existence of inverse $\longrightarrow a.a^{-1} = a^{-1}.a = 1.$
(non zero elements)

(vi) Distributive law

$$a.(b+c) = a.b + a.c.$$

$$\mathbb{F}$$

$(\mathbb{F}, +)$ Abelian group $(\mathbb{F}^*, \cdot)$ Abelian group

$\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

<u>Examples of fields</u>

$\rightarrow$ $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$

Infinite fields

<u>Defn</u>:- A finite field is a field containing a finite no. of elements i.e., $|\mathbb{F}| < \infty$.

$\mathbb{F}_2$.

Addition Table

$+$	0	1
0	0	1
1	1	0

Multiplication Table.

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{F}_3$.

(mod 3) operations

$2+2 = 1 \pmod 3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2^{-1} = 2$

If p is a prime number; then $(\mathbb{F}_p, +, \cdot)$ is a finite field

under $+$ is $(\bmod\ p)$ addition &

$\cdot$ is $(\bmod\ p)$ multiplication

Every finite field has a size q that is a power of prime $q = p^m$ $m \geq 1$ &

p is a prime number.

$\checkmark 2$ $\checkmark 3$ $\checkmark 4$ $\checkmark 5$ 6 $\checkmark 7$ $\checkmark 8$ $\checkmark 9$ 10

$\checkmark 11$ 12 $\checkmark 13$ 14 15

There does not exist a finite field with

6, 10, 12, 14, 15 · no. of elements.

Prime fields

If $a \in \mathbb{F}_p$, $(-a) = (p - a)$
$a \neq 0$

Existence of multiplicative inverse for every element is a nontrivial property to prove.

① Extended Euclidean division algorithm.
allows you to express the gcd as linear combination of the elements

$a, b \in \mathbb{Z}$ $\quad\quad gcd(a,b) = ax+by$ where $x, y \in \mathbb{Z}$

Since p is a prime;
If $a \in \mathbb{F}_p$, then

$gcd(a,p) = 1$ } are over
$\underline{ax + py = 1}$ } integers.

$a.x \pmod p = 1$

$a^{-1} = x \pmod p$.

<u>Example</u>: $p = 31$, $a = 5$, $(\mathbb{F}_{31}, +, \cdot)$.

$a^{-1} \pmod{31} = 25$

$$\boxed{\begin{array}{l} 25 \cdot 5 = 125 \\ \quad \bmod 31 \\ \quad = 1. \end{array}}$$

$1 \times 31 + 5(-6) = 1.$

<u>Remainders</u>	31	5	Quotient.
31 ←	1	0	
5 ←	0	1	6
1 ←	1	-6	5
0			

Which property of finite field does $\mathbb{F}_6$ not satisfy?

$\gcd(a,p) \neq 1. \Rightarrow$ a may not have any inverse.

$\{0, 1, 2, 3, 4, 5\}$

2 does not have an inverse.

$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$.

$2 = 1+1$

$3 = 1+1+1 \ldots$

$\mathbb{F}_7$

$\mathbb{F}_p = \{0, 3^i, 0 \le i \le 6\}$.

All nonzero elements in the finite field can be expressed as powers of a single element

Primitive element of the finite field.

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 = 2 \pmod 7$

$3^3 = 27 = 6 \pmod 7$

$3^4 = 4$

$3^5 = 5$

$3^6 = 1$