| Feb 15 | 1 Min Checkin

(•) HW0 (optional) is due by 11:59pm tonight

(•) Team registration is due by 11:59pm tonight ← If you miss this deadline you lose 50% of your total grade

(As of ~~1~~ 2pm ~~yesterday~~ today, ~~ ~~ 39 students have registered)

RECAP

(•) A field $\mathbb{F}_q = (S, +, \cdot)$ when we can add/mult/subtract/divide and stay in S

(•) Finite field $|\mathbb{F}|$ $(= |S|)$ is finite

(•) Finite field only exist for sizes p^s; $p \to$ prime, $s \geq 1$ int

(•) Unique finite field (up to isomorphism) for a given prime power q $(\mathbb{F}_q)$

(•) $\mathbb{F}_p = (\{0, 1, \ldots, p-1\}, +_{\text{mod } p}, \cdot_{\text{mod } p})$

(•) A linear code $C \subseteq \mathbb{F}_q^n$ is a linear subspace

(•) $S \subseteq \mathbb{F}_q^n$ is a linear subspace if

(i) $\forall \bar{x}, \bar{y} \in S$, $\bar{x} + \bar{y} \in S$

(ii) $\forall a \in \mathbb{F}_q, \bar{x} \in S$, $a \cdot \bar{x} \in S$ [Note: always $\bar{0} \in S$]

(•) $S_1 = \{(0,0,0), (1,1,1), (2,2,2), (3,3,3), (4,4,4)\}$ $\subseteq \mathbb{F}_5^3$

$S_2 = \{(0,0,0), (1,0,1), (2,0,2), (0,1,1), (0,2,2), (1,1,2), (2,2,1), (1,2,0), (2,1,0)\}$ $\subseteq \mathbb{F}_3^3$

(•) $\text{span}(\{\bar{u}_1, \ldots, \bar{u}_k\}) = \left\{ \sum_{i=1}^{k} a_i \cdot \bar{u}_i \;\middle|\; a_i \in \mathbb{F}_q \; \forall i \in [k] \right\}$ $u_i \in \mathbb{F}_q^n$

Ex. $\text{span}(\{(1,1,1)\}) = S_1$ (over $\mathbb{F}_5$)

$\text{span}(\{(1,0,1), (0,1,1)\}) = S_2$ (over $\mathbb{F}_3$)

PLAN for TODAY

(•) Some fundamental results/concepts for linear subspace (AND $\Rightarrow$ for linear codes)

(•) (If there is time) More on distance of linear code

<u>Def</u> (linear independence) $\bar{u}_1, \ldots, \bar{u}_k \in \mathbb{F}_q^n$ are linearly independent if $\forall i \in [k]$ $\bar{u}_i \notin \text{span}\{\bar{u}_1, \ldots, \bar{u}_{i-1}, \bar{u}_{i+1}, \ldots, \bar{u}_k\}$

$\forall i$ $\{1, \ldots, k\}$

$\equiv$ cannot express $\bar{u}_i$ as a linear combination of

O/w they are linearly dependent.

Ex: Over $\mathbb{F}_3$: $(1,0,1)$ & $(0,1,1)$ are linearly independent.

$(1,0,1)$ is lin de o $(0,1,1)$

$\Leftrightarrow$

$(1,0,1) = a\cdot(0,1,1)$

$\Rightarrow = (0,a,a)$

cannot happen since $\neq$

$(0,1,1)$ is lin dep on $(1,0,1)$

$\Leftrightarrow \exists b$ s.t $(0,1,1) = b(1,0,1)$

$= (b,0,b)$

$\neq$

But

$(1,0,1)$ $(0,1,1)$ $(2,2,1)$ are lin depent over $\mathbb{F}_3$

$2\cdot(1,0,1) + 2(0,1,1)$

$= (2,0,2) + (0,2,2)$

$= (2,2,4 \bmod 3) = (2,2,1)$

Def (rank) Rank of a matrix $M \in \mathbb{F}_q^{k\times n}$ is the largest number of linearly independent rows/columns.

$$\underbrace{k\Big\updownarrow\left(\;\;\in \mathbb{F}_q\;\;\right)}_{\longleftarrow n \longrightarrow}$$

Ex rank $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 2 & 1 \end{pmatrix} = 2$ over $\mathbb{F}_3$ rank $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3$

Matrix ~~has~~ $M \in \mathbb{F}_q^{k\times n}$ has full rank if $\operatorname{rank}(M) = \min\{k,n\}$

$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ full rank over any $\mathbb{F}_q$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ full rank over any $\mathbb{F}_q$

THM (Standard in linear algebra) ← see book for proof.

$S \subseteq \mathbb{F}_q^n$ be a ~~k linear~~ linear subspace $\Rightarrow$

(i) $|S| = q^k$ for some integer $k \geq 0$ $\quad k \to$ dimension of S

$\to C \subseteq \mathbb{F}_q^n \quad \dim(C) = \log_q |C| = \log_q q^k = k$

(ii) [for rest assume $\dim(S) = k$]

(ii) $\exists\ \bar{u}_1, \dots, \bar{u}_k \in \mathbb{F}_q^n$ that are linearly independent (basis of S)

s.t. $\bar{x} \in S$

$$\bar{x} = a_1 \bar{u}_1 + a_2 \bar{u}_2 + \cdots + a_k \bar{u}_k \;; \quad a_i \in \mathbb{F}_q \ \forall i \in [k]$$

$$\equiv \bar{x} = (a_1 \ a_2 \ \cdots \ a_k) \underbrace{\begin{array}{c} \\ \begin{pmatrix} \leftarrow \bar{u}_1 \rightarrow \\ \vdots \\ \leftarrow \bar{u}_i \rightarrow \\ \vdots \\ \leftarrow \bar{u}_k \rightarrow \end{pmatrix} \end{array}}_{n} \updownarrow k$$

Generator matrix G of S

Note: G is full rank

G_{Ham}

$[7,4,3]_2 \quad C_H(\bar{x}) = \underbrace{(x_1 \ x_2 \ x_3 \ x_4)}_{\text{all vectors are row vectors}} \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix} \updownarrow 4$, width 7

($n = 7$, $k = 4$)

$S_1: \ G_1 = (1 \ 1 \ 1)$

$S_2: \ G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

(iii) $\exists$ a full rank $(n-k) \times n$ matrix $H \in \mathbb{F}_q^{(n-k)\times n}$

s.t. $\forall\ \bar{x} \in S, \quad H \bar{x}^T = \bar{0}$

H ← parity check matrix

$$\begin{array}{c} n-k \updownarrow \end{array} \underbrace{\begin{pmatrix} \quad H \quad \end{pmatrix}}_{n} \begin{pmatrix} \\ \bar{x}^T \\ \\ \end{pmatrix} \updownarrow n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \updownarrow n-k$$

$S_1: \ H_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ over $\mathbb{F}_5$

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \\ 4 \end{pmatrix} = \left(\begin{matrix} 5 \cdot 4 \\ 5 \cdot 4 \\ 5 \cdot 4 \end{matrix} \bmod 5 \right) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$S_2: \ H_2 = \underbrace{(1 \ 1 \ 2)}_{\leftarrow 7 \rightarrow}$ over $\mathbb{F}_3$

$$(1 \ 1 \ 2) \underbrace{\begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}}_{\in S} = \left\{ \begin{matrix} 1 \cdot 2 + 1 \cdot 2 \\ + 2 \cdot 1 \\ = 6 \bmod 3 \\ = 0 \end{matrix} \right.$$

$$H_{Ham} = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix} \updownarrow 3$$

$n-k = 7-4 = 3$