Feb 14

REMINDERS

- (•) HW 0 (optional) due 11:59pm on Wed
- (•) ! IMPORTANT ! Project group composition form due 11:59 pm on Wed (Google form linked from course webpage)

RECAP

- (•) A field $\mathbb{F} = (S, +, \cdot)$ when one can add / mult / subtract / Divide & stay in S.
- (•) Finite field: $|\mathbb{F}|$ $(= |S|)$ is finite
- (•) Only field sizes are p^s for prime p, int $s \geq 1$
- (•) Unique 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 $C \subseteq \mathbb{F}_q^n$ ($q \to$ prime power) is a linear subspace.
- (•) $S \subseteq \mathbb{F}_q^n$ is a linear subspace if
  - (i) $\forall\ \bar{x}, \bar{y} \in S, \quad \bar{x} + \bar{y} \in S$ component-wise add in $\mathbb{F}_q$
  - (ii) $\forall\ a \in \mathbb{F}_q, \bar{x} \in S, \quad a \cdot \bar{x} \in S$ mult each entry in $\bar{x}$ by a (mult over $\mathbb{F}_q$)

  [Note $\Rightarrow \bar{0} \in S$

Proof readers for today: Connor, Yaswanth

PLAN for TODAY:

(1) Some fundamental concepts in linear subspaces

(2) Some consequences / properties for linear subspaces / codes.

Def: A linear ~~code~~ $(n, k, d)_q$ will be denoted as $[n, k, d]_q$ or even $[n, k]_q$ code.

Ex 1: Subspace of $\mathbb{F}_5^3$

$$S_1 = \{(0,0,0), (1,1,1), (2,2,2), (3,3,3), (4,4,4)\}$$

→ (i) $(1,1,1) + (3,3,3) = (4,4,4) \in S_1$

(ii) $2 \cdot (4,4,4) = (8,8,8) \bmod 5 = (3,3,3) \in S_1$

Ex2: Subspace over $\mathbb{F}_3^3$

$S_2 = \{(0,0,0), (1,0,1), (2,0,2), (0,1,1), (0,2,2),$
$(1,1,2), (2,2,1), (1,2,0), (2,1,0)\}$

→ (i) $(0,2,2) + (2,2,1) = (2,4,3) \bmod 3 = (2,1,0) \in S_2$

Def (span) $B = \{\bar{u}_1, \dots, \bar{u}_k\}$ $\bar{u}_i \in \mathbb{F}_q^n$

$$\text{span}(B) = \left\{ \sum_{i=1}^{k} a_i \cdot \bar{u}_i \;\middle|\; a_i \in \mathbb{F}_q \right\}$$

Over $\mathbb{F}_5$: $\text{span}\{(1,1,1)\} = S_1$

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

Def (linear independence) $\{\bar{u}_1, \dots, \bar{u}_k\} \subseteq \mathbb{F}_q^n$ are linearly independent if $\forall i \in [k] \rightsquigarrow \{1, \dots, k\}$

$u_i \notin \text{span}\{\bar{u}_1, \dots, \bar{u}_{i-1}, \bar{u}_{i+1}, \dots, \bar{u}_k\}$

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

But $\{(1,0,1), (0,1,1), (1,1,2)\}$ are NOT linearly independent

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

→ M has full rank if it's rank $= \min(k, n)$

Eg: $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ has full rank over $\mathbb{F}_3$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ has full rank over any $\mathbb{F}_q$.

THM (Standard in linear algebra)

$S \subseteq \mathbb{F}_q^n$ is a linear subspace $\Rightarrow$

(i) $|S| = q^k$, $0 \le k \le n$ is an integer (k: dimension of S)

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

s.t $\forall\ \bar{X} \in S$

$$\bar{X} = a_1 \bar{u}_1 + a_2 \bar{u}_2 + \cdots + a_k \bar{u}_k \ ; \ a_i \in \mathbb{F}_q$$

$$\equiv \bar{X} = (a_1 \ a_2 \ \ a_k) \cdot \begin{pmatrix} \leftarrow \bar{u}_1 \rightarrow \\ \leftarrow \bar{u}_2 \rightarrow \\ \vdots \\ \leftarrow \bar{u}_k \rightarrow \end{pmatrix}$$

↪ generator matrix $G \in \mathbb{F}_q^{k \times n}$

(full rank)

$[7,4,3]_2$ C_H

$$C_H = (X_1 \ X_2 \ X_3 \ X_4) \; {\scriptstyle \updownarrow 4} \overset{\longleftarrow 7 \longrightarrow}{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}} \leftarrow G_{Ham}$$

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

s.t $\forall\ \bar{X} \in S$ $\quad H X^T = \bar{0} \in \mathbb{F}_q^{n-k}$

parity check matrix

$$\underset{\leftarrow n \rightarrow}{{\scriptstyle n-k \updownarrow} \left(\quad H \quad \right)} \left(\; \right) {\scriptstyle \updownarrow n} = \left(\; \right) {\scriptstyle \updownarrow n-k}$$

(iv) G & H are orthogonal

$$G \cdot H^T = 0$$

$$\underset{\leftarrow n \rightarrow}{{\scriptstyle k \updownarrow} \left(\quad G \quad \right)} \quad \underset{\leftarrow n-k \rightarrow}{\left(\; H^T \; \right) {\scriptstyle \updownarrow n}}$$

S_1: $G_1 = (1 \ 2 \ 1 \ 1)$ $\quad H_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ over $\mathbb{F}_5$.

S_2 = $G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ $\quad H_2 = (1 \ 1 \ 2)$ over $\mathbb{F}_3$

$$H_{Ham} = {\scriptstyle 3 \updownarrow} \underset{\longleftarrow 7 \longrightarrow}{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}} \qquad [7,4,3]_2$$

Lemma: G is a generator matrix for S_1

H is a parity check matrix for S_2

If $G \cdot H^T = 0 \Rightarrow S_1 = S_2$

Properties of linear codes

Prop 1: Any $[n,k]_q$ code can be represented with $\min(nk, (n-k)n)$ symbols from $\mathbb{F}_q$

Prop 2: Any $[n,k]_q$ code can be encoded in $O(kn)$ operations over $\mathbb{F}_q$ $C: \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$

Prop 3: Any $[n,k]_q$ code we can do error detection with $O((n-k)n)$ operations over $\mathbb{F}_q$