FEB 13

1 MIN CHECKIN

REMINDERS

(•) HW 0 (optional) is due 11:59pm on Wed (see extra hint on piazza)

(•) ! IMPORTANT ! Team Registration due by 11:59pm on Wed
↖ If you miss this deadline you miss 50% of your grade.

(→) If you fill in the form by 5pm on Tue (i.e. tomorrow), I will send you email confirmation by Tue night (30 done as of 2:20pm Sun)

RECAP

(•) A linear code $C \subseteq (\text{"}\{0,..,q-1\}\text{"})^n$ is a linear subspace (q has to be a prime power)

(•) Fields $\mathbb{F} = (S, +, \cdot)$ → add | subtract | mult. | divide & stay within S

PLAN for today

(•) Define fields (•) Define linear subspaces

(•) Some fundamental concepts in linear subspaces

(•) (If there is time) Some consequences for linear subspaces/codes

$\mathbb{F} = (S, +, \cdot)$

$\mathbb{R}, \mathbb{Q}$ are fields

$\mathbb{Z}$ is not (but is a ring)

(•) Closure of + : $\forall\, a, b \in S,\ a+b \in S$

(•) ______ $\cdot$: $\forall\, a, b \in S,\ a \cdot b \in S$

(•) Associativity $+, \cdot$: $\forall\, a, b, c \in S$

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

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(•) Commutativity of $+, \cdot$: $\forall\, a, b \in S$ $\quad a+b = b+a$ $\quad a \cdot b = b \cdot a$

(•) Distributivity property ⇒ $\forall\, a, b, c \in S$

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

(•) Identities : $0 \to +$ $\quad 1 \to \cdot$

$$\forall\, a \in S,\ a+0 = a \qquad a \cdot 1 = a$$

(•) Inverses : $\forall\, a \in S,\ \exists\, -a \in S$ s.t. $a + (-a) = 0$

$\forall\, a \in S \setminus \{0\},\ \exists\, a^{-1} \in S$ s.t. $a \cdot a^{-1} = 1$) X → ring

Finite fields

$|S|$ is finite (Overload $|\mathbb{F}|$ finite)

THM 1: Any finite field has size p^s where $p \to$ prime, $s \geq 1$ int.

Ex:

1. field of size $2 \to \mathbb{F}_2$ ($GF(2)$)

   $(\{0,1\}, \oplus, \times)$

2. field of size $p \to$ prime

   $(\{0,1,\ldots,p-1\}, +_{\text{mod}\,p}, \cdot_{\text{mod}\,p})$

$p = 3$
$\{0,1,2\}$
$\to (2+2) \bmod 3$
$= 4 \bmod 3 = 1$

$\to -2 = 1$ b/c
$2 + (-2) = (2+1) \bmod 3$
$= 3 \bmod 3$
$= 0$

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

$\Rightarrow$ Additive inverse $\%\, p$

$-a \equiv p - a$

$a + (-a) = (a + (p - a)) \bmod p$
$= p \bmod p = 0$

$\Rightarrow$ Multiplicative inverse $\forall\, a \in \{1, \ldots, p-1\}\ \exists\ a^{-1} \in \{1, \ldots, p-1\}$ s.t. $a \cdot a^{-1} = 1 \bmod p$

Isomorphism: $f(a)\ \text{op}\ f(b) = f(a\ \text{op}\ b)$

THM 2: There is a unique finite field of size p^s (up to isomorphism)

$\Rightarrow q$ – prime power $\mathbb{F}_q$

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

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

component-wise + over $\mathbb{F}_q$

(ii) $\forall\, a \in \mathbb{F}_q, \bar{x} \in S \Rightarrow a \cdot \bar{x} \in S$

mult. each entry in $\bar{x}$ by a

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

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

$\rightarrow$ (i) $(1,1,1) + (3,3,3) = (4,4,4) \in S_1$ $1+3 \bmod 5 = 4 \bmod 5 = 4$

$(3,3,3) + (3,3,3) = (1,1,1) \in S_1$ $3+3 \bmod 5 = 6 \bmod 5 = 1$

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

$S_1 = \{b \cdot (1,1,1) \mid b \in \mathbb{F}_5\}$

S_1 is "generated" by $\{(1,1,1)\}$

Ex 2: Subspace $\mathbb{F}_3^3$

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

$\rightarrow$ (i) $(0,2,2) + (2,2,1) = (2,1,0)$

$\rightarrow$ (ii) $2 \cdot (2,2,1) = (1,1,2)$

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

$$\text{Span}(B) = \left\{ \sum_{i=1}^{k} a_i u_i \;\middle|\; a_i \in \mathbb{F}_q \ \forall i \in [k] \right\}$$

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

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