TTIC 31150 / CMSC 31150

Mathematical Toolkit

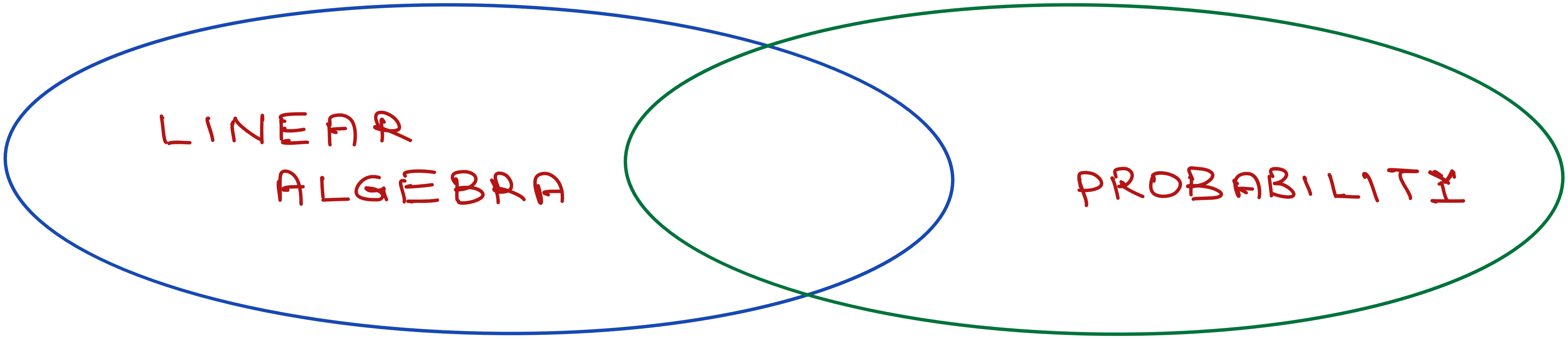
(Things I wish I knew in first year of grad school)

- TAs : Dimitar Chakarov , Keming Ouyang

- Discussion : W 4:30 – 5:30 (Optional)
- Office hours : Th 12:30 – 1:30

- See course page for notes / resources

- 5 Homeworks (60%)
  Midterm (15%)
  Final (25%)



Foundations + Applications

- Abstract treatment of topics
- Emphasis on proofs
- Applications in CS / Math

Linear Algebra

Study of spaces where we can add stuff

Why?

- ML papers (basics)
- Formalism for Physics / Quantum
- CS applications

Fields

Set where we can do arithmetic

- Set $\mathbb{F}$, operations $+ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$ satisfying
  $\cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$

- commutativity: $a + b = b + a$, $a \cdot b = b \cdot a$
- associativity: $(a+b)+c = a+(b+c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- identity: $\exists\, 0_{\mathbb{F}} \in \mathbb{F}$ s.t. $a + 0_{\mathbb{F}} = a \;\; \forall a$

  $\exists\, 1_{\mathbb{F}} \in \mathbb{F}$ s.t. $a \cdot 1_{\mathbb{F}} = a \;\; \forall a$
- inverse: $\forall a\; \exists a'$ s.t. $a + a' = 0_{\mathbb{F}}$, $\forall a \neq 0_F\; \exists a'\;\; a \cdot a' = 1_F$
- distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$

Ex: $a \cdot b = 0_{\mathbb{F}} \Longrightarrow a = 0_{\mathbb{F}}$ or $b = 0_{\mathbb{F}}$

Examples

- $\underbrace{\mathbb{F} = \mathbb{Q}}_{\text{rational numbers}}$, $\underbrace{\mathbb{F} = \mathbb{R}}_{\text{real numbers}}$, $\underbrace{\mathbb{F} = \mathbb{C}}_{\text{complex numbers}}$

- $\mathbb{F} = \mathbb{Q}^2$ with

$$(a,b) + (c,d) = (a+c,\ b+d)$$

?

$$(a,b) \cdot (c,d) = (ac+bd,\ ad + bc)$$

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

$-$

2

3

5

- $\mathbb{F}_p = \{0, 1, \ldots\ldots, p-1\}$ for prime p

(also written as $GF(p)$)

$a + b = a + b \pmod{p}$

$a \cdot b = a \cdot b \pmod{p}$

Ex: Show that above fails when p is not prime (e.g. $p = 6$)

Ex: Show that $\{a + b\sqrt[3]{2} + c\cdot\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

is a field

Vector Spaces

Set of objects we can add and scale

Vector space V over $\mathbb{F}$, associated $+ : V \times V \to V$

$\cdot : \mathbb{F} \times V \to V$

- commutativity: $u + v = v + u$
- associativity of addition: $(u + v) + w = u + (v + w)$
- pseudo-associativity of multiplication: $(a \cdot b) \cdot u$

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

  $a, b \in \mathbb{F},\ u \in V$
- identity: $\exists\, 0_V \qquad 0_V + u = u$

  $1_F \cdot u = u$
- inverse for addition: $\forall u, \exists u' \quad u + u' = 0_V$
- distributivity: $a \cdot (u + v) = a \cdot u + a \cdot v$

Examples

- Any $\mathbb{F}$ is a vector space over itself
- $\mathbb{F}^d$ is a vector space over $\mathbb{F}$ $(d \in \mathbb{N})$
- $\mathbb{R}$ is a vector space over $\mathbb{Q}$
- Polynomials in x with real coefficients

$$\mathbb{R}[x] = \left\{ \sum_{i=0}^{t} c_i x^i \;\middle|\; t \in \mathbb{N},\ c_0, \ldots, c_t \in \mathbb{R} \right\}$$

$\mathbb{R}^{\leq n}[x]$ when degree $\leq n$ $(t \leq n)$

- Continuous functions: $C([0,1], \mathbb{R}) = \{ f : [0,1] \to \mathbb{R} \mid f \text{ is continuous} \}$

vector space over $\mathbb{R}$

Ex: $\text{Fib} = \{ f : \mathbb{N} \to \mathbb{R} \mid f(n) = f(n-1) + f(n-2) \ \forall n \geq 2 \}$

is a vector space over $\mathbb{R}$

Linear Dependence: $S \subseteq V$ is linearly dependent

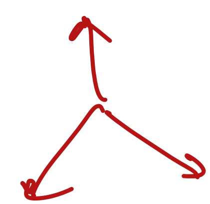
if $\exists\, n \in \mathbb{N}$, $v_1, \ldots, v_n \in S$, $c_1, \ldots, c_n \in \mathbb{F}$ not all zero s.t.

$$\underbrace{c_1 \cdot v_1 + c_2 \cdot v_2 + \cdots + c_n \cdot v_n}_{\text{linear combination of } v_1 \ldots v_n} = 0_{\mathbb{F}}$$

$S \subseteq V$ not linearly dependent $\to$ linearly independent

e.g. Find three linearly dependent vectors in $\mathbb{R}^2$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} \qquad \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$



Examples

- $a_1, \ldots, a_n \in \mathbb{R}$ distinct, $g(x) = \prod_{i=1}^{n} (x - a_i) \in \mathbb{R}^{\leq n}[x]$

$f_i = \frac{g}{x - a_i} = \prod_{j \neq i} (x - a_j)$. $f_1, \ldots, f_n$ LI over $\mathbb{R}$

Proof:

$$c_1 \cdot f_1 + \underbrace{c_2 \cdot f_2}_{0} + \cdots + \underbrace{c_n \cdot f_n}_{0} = 0_V$$

$x = a_1$

$$c_1 \cdot \underbrace{f_1(a_1)}_{\neq 0} = 0 \implies c_1 = 0$$

$c_2 = 0 \quad \ldots \quad c_n = 0$

Ex: $\{1, \sqrt{2}, \sqrt{3}\}$ LI over $\mathbb{Q}$ (but not over $\mathbb{R}$)

Span and Bases

- For $S \subseteq V$, Span(S) $= \left\{ \sum_{i=1}^{n} c_i \cdot v_i \;\middle|\; \begin{array}{l} v_1 \dots v_n \in S \\ c_1 \dots c_n \in \mathbb{F} \end{array} \quad n \in \mathbb{N} \right\}$

- B is a basis for V if
  - B is LI
  - Span$(B) = V$

- (Claim): If B is a basis, then for each $v \in V$ there is a unique choice of $c_1, \dots, c_n \in \mathbb{F}$, $v_1, \dots, v_n \in B$

  s.t. $\quad v = c_1 \cdot v_1 + \dots + c_n \cdot v_n$

Back to polynomials

$a_1, \dots, a_n \in \mathbb{F}$ distinct $\qquad f_i(x) = \prod_{j \neq i} (x - a_j)$

(basis for $\mathbb{F}^{\leq n-1}[x]$) $\qquad f_1, \dots, f_n$ LI over $\mathbb{F}$

Lagrange Interpolation: Unknown $f \in \mathbb{R}^{\leq n-1}[x]$

s.t. $f(a_1) = b_1, \dots, f(a_n) = b_n$

$\exists$ unique $c_1, \dots, c_n$ s.t. $f = c_1 \cdot f_1 + \dots + c_n \cdot f_n$

$b_1 = c_1 \cdot f_1(a_1) \Rightarrow c_1 = \frac{b_1}{f_1(a_1)}$

$c_1 = ?$ $\quad \dots \quad$ $c_n = ?$

$$f = \sum_{i=1}^{n} \frac{b_j}{f_j(a_j)} \cdot f_i(x)$$

Application: Secret Sharing [Shamir 79]

Share secret $s \in [0, M]$ with n people s.t.

- If any d get together, they learn s
- Fewer than d do not get any information

Scheme

- Choose $\mathbb{F}_p$ with $p > \max\{n, M\}$
- Choose (random) $c_1, \ldots, c_{d-1} \in \mathbb{F}_p$ and take

$$Q(x) = s + c_1 \cdot x + \ldots + c_{d-1} \cdot x^{d-1}$$

- Person i gets $(i, Q(i))$ for $i = 1, \ldots, n$