Module 7: Linear Algebra I

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 18, 2024

Outline

Today:

- Vector spaces and subspaces
- Linear independence and bases
- Linear maps, null space, range

Vector spaces & subspaces

Definition

We call V a **vector space** if the following hold:

(A) *Commutativity in addition:* $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ for all $\mathbf{u}, \mathbf{v} \in V$

(B) *Associativity in addition:* $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$

(C) *Existence of a neutral element, addition:* There exists a vector $\mathbf{0}$ such that for any $\mathbf{v} \in V$, $\mathbf{0} + \mathbf{v} = \mathbf{v}$

(D) *Additive inverse:* For every $\mathbf{v} \in V$, there exists another vector, which we denote $-\mathbf{v}$, such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$. ← At this point, we are not sure $(-1) \times v = -v$

(E) *Existence of a neutral element, multiplication:* For any $\mathbf{v} \in V$, $\overset{\in \mathbb{F}}{1} \times \mathbf{v} = \mathbf{v}$

(F) *Associativity in multiplication:* Let $\alpha, \beta \in \mathbb{F}$. For any $\mathbf{v} \in V$, $(\alpha\beta)\mathbf{v} = \alpha(\beta\mathbf{v})$

(G) Let $\alpha \in \mathbb{F}, \mathbf{u}, \mathbf{v} \in V$. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$.

(H) Let $\alpha, \beta \in \mathbb{F}, \mathbf{v} \in V$. $(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$.

$\mathbb{F}$ = field $\mathbb{R}$ or $\mathbb{C}$

Elements of the vector space are called vectors.
Most often we will assume $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$.

Example

The following are vector spaces:

- $\mathbb{R}^n$
- $\mathbb{C}^n$
- $C(\mathbb{R};\mathbb{R})$, continuous functions from $\mathbb{R}$ to $\mathbb{R}$
- $M_{n\times m}$, matrices of size $n \times m$
- $\mathbb{P}_n$ (polynomials of degree n, $p(x) = a_0 + a_1 x + \ldots + a_n x^n$).

Lemma

For every $\mathbf{v} \in V$, $0\mathbf{v} = \mathbf{0}$.

Proof.

Using (H), $0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v$.

By (D), there exists addition inverse of $0 \cdot v$.

So, $0 = 0 \cdot v + (-0 \cdot v) = (0 \cdot v + 0 \cdot v) + (-0 \cdot v)$

By (B) $\longrightarrow = 0 \cdot v + (0 \cdot v + (-0 \cdot v))$

By (D) $= 0 \cdot v + 0$

By (C) $= 0 \cdot v$.

$\square$

Lemma

For every $\mathbf{v} \in V$, we have $-\mathbf{v} = (-1) \times \mathbf{v}$.

Proof.

We want to show $v + (-1) \cdot v = 0$ (due to definition of $-v$)

By (E), $v = 1 \cdot v$.

Thus $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v$

$= (1 + (-1)) \cdot v$ by (H)

$= 0 \cdot v$

$= 0$ by the previous lemma. $\square$

Statistical Sciences
UNIVERSITY OF TORONTO

a vector space.

Definition

A subset U of V is called a **subspace** of of V if U is also a vector space (using the same addition and scalar multiplication as on V).

Proposition

A subset U of V is a subspace of V if and only if U satisfies the following three conditions:

1. $\mathbf{0} \in U$
2. Closed under addition: $\mathbf{u}, \mathbf{v} \in U$ implies $\mathbf{u} + \mathbf{v} \in U$
3. Closed under scalar multiplication: $\alpha \in \mathbb{F}$ and $\mathbf{u} \in U$ implies $\alpha\mathbf{u} \in U$

Proof. ($\Rightarrow$) Suppose U is a subspace.

Then U is also a vector space

Therefore 1 ~ 3 must hold.

($\Leftarrow$) Suppose (1 ~ 3) hold.

Only prove (1) (rest omitted)

For any $v \in U$, we need to show the existence of additive inverse.

By 3), $(-1) \times v \in U$.

Since V is a vector space. $(-1) \times v = -v$ in V.

Thus $v + (-v) = 0$

Since $-v = (-1) \times v \in U$, we know that $(-1) \times v$ is an additive inverse in U

Linear (in)dependence and bases

Linear combinations

Definition

A linear combination of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of vectors in V is a vector of the form

$$\alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n = \sum_{k=1}^{n} \alpha_k \mathbf{v}_k$$

where $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$.

Span

Definition

The set of all linear combinations of a list of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ in V is called the **span** of $\mathbf{v}_1, \dots, \mathbf{v}_n$, denoted $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. In other words,

$\langle v_1, \dots, v_n \rangle$

$$\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\alpha_1 \mathbf{v}_1 + \dots + \alpha_m \mathbf{v}_n : \alpha_1, \dots, \alpha_n \in \mathbb{F}\}$$

The span of the empty list is defined to be $\{\mathbf{0}\}$.

Basis

Definition

A system of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is called a basis (for the vector space V) if any vector $\mathbf{v} \in V$ admits a unique representation as a linear combination

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n = \sum_{k=1}^{n} \alpha_k \mathbf{v}_k. \quad \in \langle v_1, \ldots, v_n \rangle$$

Example $\mathbb{R}^n$ or $\mathbb{C}^n$

- For $\mathbb{F}^n$, $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$ is a basis
- The monomials $1, x, x^2, \ldots, x^n$ form a basis for $\mathbb{P}_n$.

Polynomials of degree $\leq n$.

Statistical Sciences
UNIVERSITY OF TORONTO

Linear independence

If $v_1, \ldots, v_n$ are linearly dependent,

$\exists\ \alpha_k \neq 0$ s.t. $\sum_{i=1}^{n} \alpha_i v_i = 0$

$\alpha_k v_k = - \sum_{i \neq k} \alpha_i v_i$

Definition

A system of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in V is called *linearly independent* if

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

implies $\alpha_i = 0$ for all $i = 1, \ldots, n$.

Otherwise, we call the system *linearly dependent*.

$\therefore\ v_k = - \sum_{i \neq k} \frac{\alpha_i}{\alpha_k} v_i$

v_k is a linear combination of the rest of v_i's.

Linear combinations $\alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n$ such that $\alpha_k = 0$ for every k are called trivial.

Spanning set

Definition

A system of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in V is called *spanning* if any vector in V can be written as a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_n$. In other words,

$$V = \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}. \left(= \langle v_1, \cdots, v_n \rangle \right)$$

Such a system is also often called generating or complete. The next proposition relates spanning and linearly independent to a basis.

Proposition

A system of vectors $\mathbf{v}_1, \ldots \mathbf{v}_n \in V$ is a basis if and only if it is linearly independent and spanning.

Proof. ($\Rightarrow$)

Suppose $v_1, \cdots, v_n$ is a basis of V.

By definition $V = \langle v_1, \cdots, v_n \rangle$.

Suppose $\sum_{i=1}^{n} \alpha_i v_i = 0$

two representations of 0.

Note that $\sum_{i=1}^{n} 0 \cdot v_i = 0$

By the uniqueness of the representation, we must have $\alpha_i = 0$.

Thus $v_1, \cdots, v_n$ are linearly independent

Statistical Sciences
UNIVERSITY OF TORONTO

($\Leftarrow$) Suppose $V = \langle v_1, \dots, v_n \rangle$ and v_i's are linearly indepet.

We only need to show linear representation by v_i's is always unique.

Suppose. $\sum \alpha_i v_i = \sum \beta_i v_i$.

$$\Leftrightarrow \sum_i (\alpha_i - \beta_i) \cdot v_i = 0.$$

Since v_i's are linearly independent, $\alpha_i - \beta_i = 0$ for $\forall i$. //

Proposition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ be spanning. Then $\mathbf{v}_1, \ldots, \mathbf{v}_n$ contains a basis.

Sketch of proof.

Define $E_1 = \{v_1\}$.

If $v_2 \in \langle v_1 \rangle$, then ignore v_2.

If $v_2 \notin \langle v_1 \rangle$, then let $E_2 = \{v_1, v_2\}$.

Repeat this operation until v_n. and we have E_φ.

In the end, we have E_φ spanning V

and vector v_i's in E_φ are linearly independent

Definition

An $\mathbb{F}$-vector space V is called *finite dimensional* if there exists a finite list of vectors that span it, i.e. there exist $n \in \mathbb{N}$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ such that $V = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Otherwise, we call V *infinite dimensional*.

Example

- $\mathbb{F}^n$, $M_{m\times n}$, $\mathbb{P}_n$ are examples of finite dimensional vector spaces
- The $\mathbb{F}$-vector space $\mathbb{P} = \{\sum_{i=1}^{n} \alpha_i x^i \ : \ n \in \mathbb{N}, \alpha_i \in \mathbb{F}, i = 1, \ldots, n\}$ is infinite dimensional.

allowing degree to be arbitrarily large.

Corollary

Every finite dimensional vector space has a basis.

This follows from the fact that every spanning set for a vector space contains a basis.

finite.

This can also be extended to infinite dimensional vector spaces, i.e. when we do not assume that there exists a finite spanning set. However, this relies on the Axiom of Choice and is beyond the scope of this course.

Proposition

Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.

Proof. Let $u_1, \cdots, u_n$ be linearly independent vectors.

Set $E_0 = \{u_1, \cdots, u_n\}$.

Let $v_1, \cdots, v_m$ be a basis of V.

If $v_1 \notin \langle E_0 \rangle$, then $v_1 \in E_1$.

If $v_1 \in \langle E_0 \rangle$, then $v_1 \notin E_1$ and check if $v_2 \notin \langle E_0 \rangle$.

continue till you find the first v_i s.t. $v_i \notin \langle E_0 \rangle$

and let $v_i \in E_1$

Continues until the end.

Dimension

Proposition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis for V. Then $m = n$.

The proof is omitted,. It relies on the fact that the number of elements in linearly independent systems are always less than or equal to the number of elements in spanning systems.

Definition

Let V be a finite dimensional $\mathbb{F}$-vector space. The number of elements in a basis of V is called the *dimension* of V and is denoted $\dim(V)$.

By the previous ~~definition~~, the notion of dimension is well-defined.

proposition

Dimension

Example

- $\dim(\mathbb{F}^n) =$ n
- $\dim(\mathbb{P}_n) =$ $n+1$
- $\dim\{\mathbf{0}\} =$ 0

Linear maps

Linear Maps

Definition

A map from a vector space U to a vector space V is **linear** if

$$T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}) \quad \text{for any } \mathbf{u}, \mathbf{v} \in V,\ \alpha, \beta \in \mathbb{F}$$

Notation: $\mathcal{L}(U, V)$ is the set of all linear maps from $\mathbb{F}$-vector space U to $\mathbb{F}$-vector space V

Example

- Zero map

  $0 : U \to V$ by $0(\vec{u}) = 0$

- Identity map

  $Id : V \to V$ $Id(v) = v$

- Differentiation $\mathbb{P}(\mathbb{R}) \to \mathbb{P}(\mathbb{R})$

  $x^n \to n \cdot x^{n-1}$

Statistical Sciences
UNIVERSITY OF TORONTO

Theorem

Suppose $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is a basis for U and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis for V. Then there exists a unique linear map $T : U \to V$ such that $T\mathbf{u}_j = \mathbf{v}_j$ for $j = 1, \ldots, n$.

Proof in book.

Theorem

Let $S, T \in \mathcal{L}(U, V)$ and $\alpha \in \mathbb{F}$. $\mathcal{L}(U, V)$ is a vector space with addition defined as the sum $S + T$ and multiplication as the product αT.

The proof follows from properties of linear maps and vector spaces. Note that the additive identity is the zero map.

Lemma

Let $T \in \mathcal{L}(U, V)$. Then $T(\mathbf{0}) = \mathbf{0}$. $\iff 0 \in \ker T$

Proof.

$$T(0) = T(1 \cdot 0 + 1 \cdot 0)$$
$$= 1 \cdot T(0) + 1 \cdot T(0)$$
$$= T(0) + T(0)$$
$$\therefore \quad T(0) = 0$$

Null space and range

Definition

Let $T: U \to V$ be a linear transformation. We define the following important subspaces:

ker T

- *Kernel or null space*: null $T = \{\mathbf{u} \in U : T\mathbf{u} = 0\}$
- *Range*: range $T = \{\mathbf{v} \in V : \exists \mathbf{u} \in U$ such that $\mathbf{v} = T\mathbf{u}\}$ = Im(T)

The dimensions of these spaces are often called the following:

- *Nullity*: nullity$(T) = \dim(\text{null}(T))$ = dim(ker T)
- *Rank*: rank$(T) = \dim(\text{range}(T))$ = dim(Im(T))

Statistical Sciences
UNIVERSITY OF TORONTO

Proposition

Let $T: U \to V$. The null space of T is a subspace of U and the range of T is a subspace of V.

Proof. (i) the null space of T is a subspace of U

kernel

1) $0 \in \ker T$ is already proved.

2) Let $u, v \in \ker T$.

Then $Tu = Tv = 0$

Thus $T(u+v) = Tu + Tv = 0 + 0 = 0$.

Thus $u + v \in \ker T$.

3) Let $\alpha \in \mathbb{F}$ and $v \in \ker T$.

Then $T(\alpha v) = \alpha Tv = \alpha \cdot 0 = 0$, thus $\alpha v \in \ker T$.

(ii) the range of T is a subspace of V

1) $0 \in \operatorname{Im} T$ is already proved.

2) Let $v_1, v_2 \in \operatorname{Im} T$.

$\exists\, u_1, u_2$ s.t. $Tu_1 = v_1$ and $Tu_2 = v_2$

$v_1 + v_2 = Tu_1 + Tu_2 = T(u_1 + u_2)$

Thus $v_1 + v_2 \in \operatorname{Im} T$

3) Let $v \in \operatorname{Im} T$, $\alpha \in \mathbb{F}$.

$\exists\, u \in U$ s.t. $Tu = v$.

Thus $T(\alpha u) = \alpha T u = \alpha v$. Therefore $\alpha v \in \operatorname{Im}(T)$

Example

Zero map from a vector space U to a vector space V:

- The null space is U
- The range is $\{0\}$

Differentiation map from $\mathbb{P}(\mathbb{R})$ to $\mathbb{P}(\mathbb{R})$:

- The null space is constants
- The range is $\mathbb{P}(\mathbb{R})$

In other words
$u \neq v$ implies $Tu \neq Tv$

Definition (Injective and surjective)

Let $T : U \to V$. T is *injective* if $T\mathbf{u} = T\mathbf{v}$ implies $\mathbf{u} = \mathbf{v}$ and T is *surjective* if $\forall \mathbf{v} \in V$, $\exists \mathbf{u} \in U$ such that $\mathbf{v} = T\mathbf{u}$, i.e. if range $T = V$.

Theorem

$T \in \mathcal{L}(U, v)$ is injective if and only if null T $= \{\mathbf{0}\}$.

$= \ker T$

Proof. ($\Rightarrow$) Suppose T is injective.

Let $v \in \ker T$

Then we have $Tv = 0 = T \cdot 0$

Since T is injective, $v = 0$

($\Leftarrow$) Suppose $\ker T = \{0\}$.

Let $Tu = Tv$.

Then $T(u-v) = 0$. That means $u - v \in \ker T$.

However, we assumed $\ker T = \{0\}$.

Therefore $u - v = 0 \Leftrightarrow u = v$.

Theorem (Rank Nullity Theorem)

Let $T : U \to V$ be a linear transformation, where U and V are finite-dimensional vector spaces. Then

$$\text{rank } T + \text{nullity } T = \dim U.$$

$$\dim(\text{Im } T) + \dim(\ker T) = \dim U$$

Proof in the lecture notes (pg. 35).

References

Axler S. *Linear Algebra Done Right*. 3rd ed. Undergraduate Texts in Mathematics. Springer, 2015. Available from: https://link.springer.com/book/10.1007/978-3-319-11080-6

Treil S. *Linear Algebra Done Wrong*. 2017. Available from: https://www.math.brown.edu/streil/papers/LADW/LADW.html