Seminar 1: Vector Spaces

Mou Minghao

SSE, CUHK(SZ)

July 17, 2022

Outline

An interesting figure...

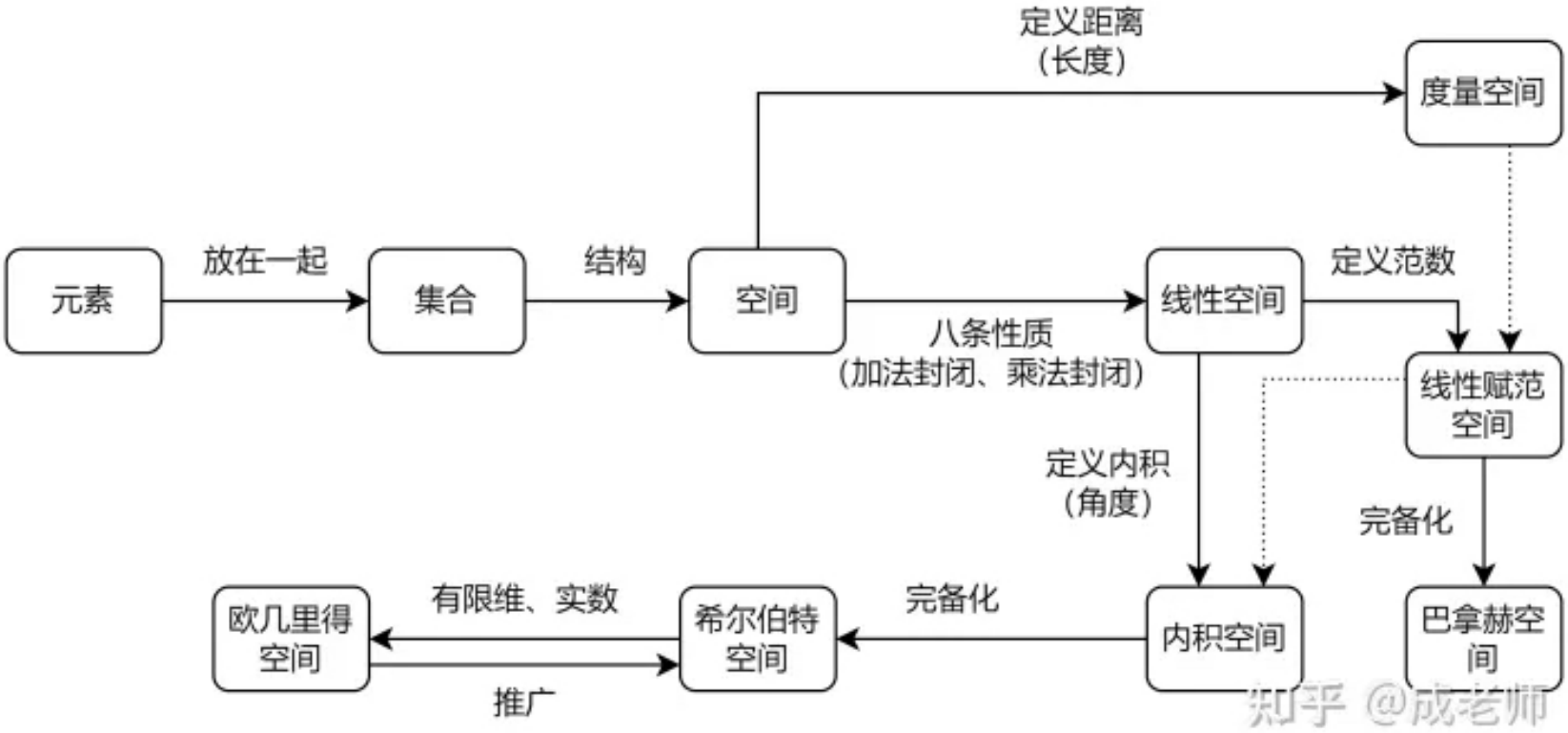

Figure 1: Some spaces appearing in undergraduate level math courses

Vector Space

Definition (Vector Space)

A vector space (also called a $\mathbb{F}$-space, linear space) over a field $\mathbb{F}$ is a nonempty set $\mathcal{X}$ together with two algebraic operations addition $+$ and scalar multiplication $\cdot$ $(+ : \mathcal{X} \times \mathcal{X} \to \mathcal{X}, \cdot : \mathbb{F} \cdot \mathcal{X} \to \mathcal{X})$ such that it satisfies the following axioms:

1. $(\mathcal{X}, +)$ *is an abelian group*
2. $\alpha(\beta x) = (\alpha\beta x)$
3. $\exists 1 \in \mathbb{F}$ *such that* $1x = x$
4. $\alpha(x + y) = \alpha x + \alpha y$
5. $(\alpha + \beta)x = \alpha x + \beta y$

Remark

Usually, $\mathbb{F} = \mathbb{R}, \mathbb{C}$, but we can also take $\mathbb{F}$ as other fields.

Problem

Show that $0x = \theta$ and $\alpha\theta = \theta$, where $\theta \in \mathcal{X}$ is the zero vector.

Examples

Example (1)

$(\mathbb{R}^n, +, \cdot)$

Example (2)

$((\mathcal{M})_{m\times n}(\mathbb{C}), +, \cdot)$

Example (3)

$(C[a, b], +, \cdot)$

Example (4)

l^2: the collection of all real (complex) sequences such that $(\sum_{k=1}^{\infty} |x_k|^2)^{1/2} < \infty$

Subspace

Definition (Subspace)

$\mathcal{Y} \subset \mathcal{X}$ is a subspace of $\mathcal{X}$ if it is itself a vector space under the restricted operations $+_{\mathcal{Y}\times\mathcal{Y}}$ and $\cdot_{\mathbb{F}\times\mathcal{Y}}$. Notation: $\mathcal{Y} \leq \mathcal{X}$.

Example ($\mathcal{V}(n, 2)$)

when we take $\mathbb{F}$ as a finite filed $\mathbb{F}_q$, we denote the vector space as $\mathcal{V}(n, q)$. Let's consider the even weight subspace of $\mathcal{V}(n, 2)$, which is the collection of all n-tuples with 0's and 1's.

1. *$W(v)$ is the weight of a vector v, which is defined to be the number of nonzero entries. (e.g. $W((1, 0, 0, 0)) = 1$)*
2. *CLAIM: E_n, the set of all even weighted vectors is a subspace of $\mathcal{V}(n, 2)$ (Hint: $W(u + v) = W(u) + W(v) - 2W(u \cap v)$)*

Remark

Any subspace of $\mathcal{V}(n, q)$ is called a linear code, which is the most important and widely studied code in cryptography

The Lattice of Subspaces

Problem

Show that if $U, W \leq V$, then $U \cap W \leq V$. Generally, $U \cup W$ is not a subspace of V. Think about under what conditions will $U \cup W \leq V$?

Let $S(V) := \{U | U \leq V\}$. It is a partially ordered set (POS) with the partial order $\subset$. $\{\theta\}$ is the smallest element and V is the largest element.

Definition

if $S, T \in S(V)$, then $GLB(S, T) := S \cap T$ and $LUB(S, T) := S + T$

Theorem

A nontrivial vector space V over an infinite field $\mathbb{F}$ cannot be the union of a finite number of proper subspaces.

The Lattice of Subspaces

Definition (Lattice)

A POS with the property that any pair of elements has a LUB and a GLB is called a lattice

Definition (Complete Lattice)

If a lattice contains a largest and a smallest element and has the property that any collection of elements has a LUB and a GLB is called a complete lattice

Theorem

$S(V)$ is a complete lattice

Span, Linear Combination and Linear Independence

Definition

$\emptyset \neq M \subset \mathcal{X}$, *spanM* (*or* $\langle M \rangle$) $:= \left\{ \sum_{i=1}^{n} \alpha_i x_i | n \in \mathbb{N}, \alpha_i \in \mathbb{F}, x_i \in M \right\}$

Definition (Linear Combination)

$x \in \mathcal{X}$ *is a linear combination of* $M = \{x_1, ..., x_n\}$ *if* $x \in \langle M \rangle$

Definition (Linear Independence)

$\{x_1, .., x_n\}$ *is said to be linearly independent if*

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \text{ iff } \alpha_1 = \cdots \alpha_n = 0.$$

Example

Consider $\mathcal{X} = \mathcal{P}_3(\mathbb{R})$, *show that* $\left\{1, x, x^2\right\}$ *is l.i.*

Basis

Definition (Basis)

A subset $B \subset \mathcal{X}$ is said to be a (Hamel) basis of $\mathcal{X}$ if

1. $\mathcal{X} = \langle B \rangle$ *(if $|B| < \infty$, then $\mathcal{X}$ is finitely-generated)*
2. *B is l.i.*

That is to say, B should be large enough while stay small enough

Example

Show that $\boldsymbol{e} = \{e_1, ..., e_n\}$ is a basis for $\mathbb{R}^n$ and $\mathbb{R}^n = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle$

Proposition

$\forall x \in \mathcal{X}$ can be uniquely represented as a linear combination of B iff B is a basis for $\mathcal{X}$

Basis

Theorem

Every finitely-generated space has a Hamel basis

Corollary

if B spans $\mathcal{X}$, then B can be reduced to a Hamel basis for $\mathcal{X}$

Definition (Dimension)

Given B a basis for $\mathcal{X}$, $|B|$ is defined to be the dimension of $\mathcal{X}$

A natural question is: since $\mathcal{X}$ generally has a lot of bases, does that mean it can have different dimensions? ($\times$)

Example

$dim(\mathbb{R}^n) = n$, $dim(C[a, b]) = \infty$. Try to show by yourself :)

Basis

To answer the question we proposed before, we prove the following theorem

Theorem

All bases of a vector space $\mathcal{X}$ have the same cardinality

proof sketch.

1. assume two bases B_1 and B_2
2. write the longer one as the l.c. of the shorter one
3. construct a matrix A, show it is invertible
4. construct some coefficients to derive a contradiction □

Corollary (Basis Extension)

if $B \subset \mathcal{X}$ is a l.i, it can be extended to a basis of $\mathcal{X}$

Corollary

Given $dim(\mathcal{X}) = n < \infty$, if $B \subset \mathcal{X}$ is l.i., then $|B| \leq n$

Direct Sum

Definition (External Direct Sum)

let $V_1, ..., V_n$ be v.s. over $\mathbb{F}$, the e.d.s. is defined to be

$$V_1 \boxplus \cdots \boxplus V_n := \{(v_1, ..., v_n) | v_i \in V_i, \forall i\}$$

The definition can be generalized to any collection of v.s. by considering any ordered n-tuple $(v_1, ..., v_n)$ as a function $f : \{1, 2, ..., n\} \to \bigcup_i V_i$, where $f(i) \in V_i, \forall i$

Definition (Direct Product)

$\mathcal{F} = \{V_i | i \in K\}$ is a family of v.s. over $\mathbb{F}$. The d.p. is defined to be

$$\prod_{i \in K} V_i := \left\{ f : k \to \bigcup_{i \in K} V_i | f(i) \in V_i \right\}$$

it can be seen as a subspace of $(\bigcup_{i \in K} V_i)^K$

Direct Sum

Definition (Support)

$Supp(f) := \{i \in K | f(i) \neq 0\}$

If |Supp(f)| $< \infty$, f has finite support

Definition (Generalized External Direct Sum)

$$\oplus_{i \in K}^{ext} V_i := \left\{ f : K \to \bigcup_{i \in K} V_i | f(i) \in V_i, \textit{finite support} \right\}$$

if there are only finitely many v.s., it is same as d.p.

Direct Sum

Definition (Internal Direct Sum)

$$V = \oplus_{i \in I} V_i$$

if

1. $V = \sum_{i \in I} V_i$
2. $V_i \bigcap (\sum_{j \neq i} V_j) = \{\theta\}$

if $S \oplus T = V$, then T is called the complement of S in V. (Complement is not unique, consider an example in $\mathbb{R}^2$)
Indeed, external and internal direct sums are the same (equivalent) concepts, isomorphic (NOT proved here)

Theorem

Any subspace of a vector space has a complement

proof sketch

- By basis extension theorem

□

Complexification

if W is a v.s. over $\mathbb{C}$, it can be recasted to a $\mathbb{R}$-space by restricting all scalars to be real numbers.
on ther other hand, to any $\mathbb{R}$-space V, we can associate it with a $V^{\mathbb{C}}$.
This is quite useful in linear transformation theory (e.g. when proving the famous *Cayley-Hamiltion Theorem*)

Definition (Complexification)

if V is a $\mathbb{R}$-space, then the set $V^{\mathbb{C}} = V \times V$ of ordered pairs, with componentwise addition

$$(u, v) + (x, y) := (u + x, v + y)$$

and scalar multiplication

$$(a + bi)(u, v) := (au - bv, av + bu)$$

over $\mathbb{C}$ is called the complexification of V

Complexification

We adopt this notation to resemble the operations between complex numbers:

$$(u, v) \in V^{\mathbb{C}} \to u + vi$$

then the addition and scalar multiplication becomes

$$(u + vi) + (x + yi) = (u + x) + (v + y)i,$$
$$(a + bi)(u + vi) = (au - bv) + (av + bu)i.$$

We consider the map between V and $V^{\mathbb{C}}$

Definition (Complexification Map)

the map $cpx : V \to V^{\mathbb{C}}$ which maps $v \in V$ to $v + 0i \in V^{\mathbb{C}}$ is called the complexification map

Proposition

cpx is a vector space homomorphism. (it is injective but not surjective)

Complexification

It seems to be surprising that V and $V^{\mathbb{C}}$ have the same dimension

Theorem

$dim_{\mathbb{R}}(V) = dim_{\mathbb{C}}(V^{\mathbb{C}})$

proof sketch.

1. let $B \subset V$ be a basis
2. claim that $cpx(B) \subset V^{\mathbb{C}}$ is a basis for $V^{\mathbb{C}}$ $\square$

Appendix

Theorem

if $v_1, ..., v_n$ are l.i. and $s_1, ..., s_m$ spans V, then $m \geq n$

proof sketch.

□

Theorem

If V is a vector space, then any two bases of V have the same size (cardinality)

References I

Roman, S., Axler, S., and Gehring, F. (2005).
Advanced linear algebra, volume 3.
Springer.

[Roman et al., 2005]