01204211 Discrete Mathematics Lecture 9a: Spans and independence

Jittat Fakcharoenphol

August 30, 2022

Review: Linear combinations

Definition

For any scalar

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

and vectors

$$\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m,$$

we say that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_m \boldsymbol{u}_m$$

is a linear combination of u_1, \ldots, u_m .

Review: Span

Definition

A set of all linear combination of vectors $m{u}_1, m{u}_2, \dots, m{u}_m$ is called the span of that set of vectors.

It is denoted by $Span\{u_1, u_2, \dots, u_m\}$.

Example 1

Is Span $\{[1,2],[2,5]\} = \mathbb{R}^2$?

Example 2

Is Span $\{[1,0,1],[1,1,0],[2,3,4]\} = \mathbb{R}^3$?

Example 3

Is Span $\{[1,0,1],[1,1,0],[4,2,2]\} = \mathbb{R}^3$?

Elements in a vector

- \blacktriangleright We see examples of vectors over \mathbb{R} .
- However, elements in a vector can be from other sets with appropriate property. (I.e., they should behave a real numbers.)
- ▶ What do we want from an element in a vector?
 - We should be able to perform addition, subtraction, multiplication, and division.
 - Operations should be commutative and associative.
 - Additive and multiplicative identity should exist.
 - Addition and multiplication should have inverses.
- We refer to a set with these properties as a **field**.

A field

Definition

A set \mathbb{F} with two operations + and \times (or \cdot) is a **field** iff these operations satisfy the following properties:

- (Associativity): (a+b)+c=a+(b+c) and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- ► (Commutativity): a + b = b + a and $a \cdot b = b \cdot a$
- ▶ (Identities): There exist two elements $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$ such that a+0=a and $a\cdot 1=a$
- ▶ (Additive inverse): For every element $a \in \mathbb{F}$, there is an element $-a \in \mathbb{F}$ such that a + (-a) = 0
- ▶ (Multiplicative inverse): For every element $a \in \mathbb{F} \setminus \{0\}$, there is an alement a^{-1} such that $a \cdot a^{-1} = 1$
- ▶ (Distributive): $a \cdot (b+c) = a \cdot b + a \cdot c$

Another useful field: GF(2)

 $GF(2) = \{0,1\}$. I.e., it is a "bit" field. What are + and \cdot in GF(2)?

▶ We define $b_1 + b_2$ to be XOR.

$$0+0=0$$

 $0+1=1+0=1$
 $1+1=0$

▶ We define $b_1 \cdot b_2$ to be standard multiplication.

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$$

 $1 \cdot 1 = 1$

You can check that GF(2) satisfies the axioms of fields.



Can you solve 2×2 Lights out?

Let
$$u_1 = [1, 1, 1, 0]$$
, $u_2 = [1, 1, 0, 1]$, $u_3 = [1, 0, 1, 1]$, and $u_4 = [0, 1, 1, 1]$.

Given ${m b}=[b_1,b_2,b_3,b_4]$, can you always find $a_1,a_2,a_3,a_4\in GF(2)$ such that

$$a_1 \cdot u_1 + a_2 \cdot u_2 + a_3 \cdot u_3 + a_4 \cdot u_4 = b$$
?

Same question: Is Span $\{u_1, u_2, u_3, u_4\} = GF(2)^4$?

Can you solve 2×2 Lights out?

Let's try with an example. Let $\mathbf{b} = [1, 0, 0, 0]$. Can you find $a_1, a_2, a_3, a_4 \in GF(2)$ such that

$$a_1 \cdot u_1 + a_2 \cdot u_2 + a_3 \cdot u_3 + a_4 \cdot u_4 = b$$
?

Can you solve 2×2 Lights out?

Since

$$[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1] \in \mathrm{Span} \ \{\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,\boldsymbol{u}_4\},$$
 and

Span
$$\{[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]\} = GF(2)^4$$
,

what can we say about Span $\{u_1, u_2, u_3, u_4\}$?

Generators

Definition

Let $\mathcal V$ be a set of vectors. Consider vectors u_1,u_2,\ldots,u_n . If $\mathrm{Span}\ \{u_1,u_2,\ldots,u_n\}=\mathcal V$, we say that

- $lackbox{} \{oldsymbol{u}_1,oldsymbol{u}_2,\ldots,oldsymbol{u}_n\}$ is a **generating set** for $\mathcal V$
- lacktriangle vectors $oldsymbol{u}_1, oldsymbol{u}_2 \ldots, oldsymbol{u}_n$ are **generators** for $\mathcal V$

Examples

Standard generators

Note that $\{[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]\}$ are generators for $GF(2)^4$. Why?

They are called **standard generators** for $GF(2)^4$, written as e_1, e_2, e_3, e_4 .

For \mathbb{R}^n , we also have $[1,0,0,\dots,0],[0,1,0,\dots,0],\dots,[0,0,0,\dots,1]$ as standard generators.

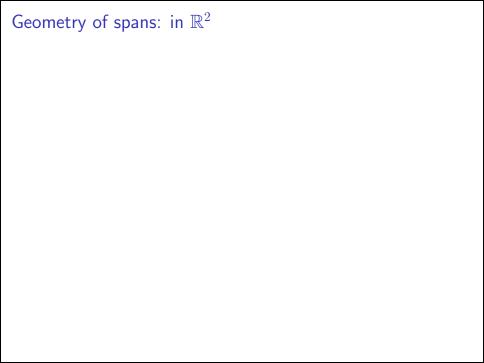
Generators and spans

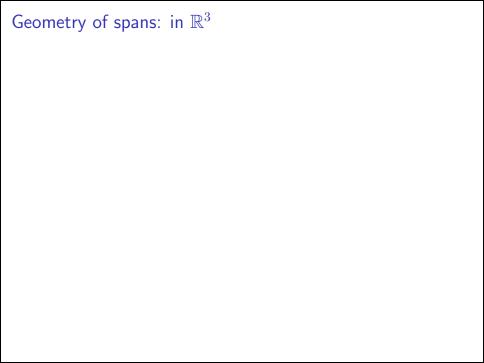
Theorem 1

Consider vectors u_1, u_2, \dots, u_n . If v_1, v_2, \dots, v_k are generators for V, and for each i,

$$v_i \in \text{Span } \{u_1, u_2, \dots, u_n\},\$$

we have that $V \subseteq \operatorname{Span} \{u_1, u_2, \dots, u_n\}$.





Two representations

There are two ways to represent a line, a plane, and a (hyper)plane, passing through the origin:

- ► as a span of vectors
- ▶ as solutions of a system of homogeneous linear equations.

What are common properties of these geometric objects?

- they pass through the origin,
- ▶ if vector \boldsymbol{u} is in the objects, $\alpha \boldsymbol{u}$ for any scalar α is also in the objects, and
- ightharpoonup if u and v are in the objects, u+v is also in the objects.

Vector spaces

Definition

A set \mathcal{V} of vectors over \mathbb{F} is a **vector space** iff

- ightharpoonup (V1) $\mathbf{0} \in \mathcal{V}$,
- ightharpoonup (V2) for any $u \in \mathcal{V}$,

$$\alpha \cdot \boldsymbol{u} \in \mathcal{V}$$

for any $\alpha \in \mathbb{F}$, and

ightharpoonup (V3) for any $u,v\in\mathcal{V}$,

$$u + v \in \mathcal{V}$$
.

Span of vectors is a vector space

Consider n-vectors u_1, u_2, \ldots, u_m ,

Span
$$\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_m\}$$

is a vector space.

Let's check if properties V1, V2, and V3 are satisfied.

Solutions to homogeneous linear equations is a vector space

Consider a set S of all n-vectors in the form $[x_1, x_2, \ldots, x_n]$ where

$$a_{11} \cdot x_1 + a_{12} \cdot x_2 + \dots + a_{1n} \cdot x_n = 0$$

$$a_{21} \cdot x_1 + a_{22} \cdot x_2 + \dots + a_{2n} \cdot x_n = 0$$

$$\vdots = \vdots$$

$$a_{m1}x \cdot_1 + a_{m2} \cdot x_2 + \dots + a_{mn} \cdot x_n = 0$$

Let's check if properties V1, V2, and V3 are satisfied.

Dot product

Definition

For n-vectors $u = [u_1, u_2, \dots, u_n]$ and $v = [v_1, v_2, \dots, v_n]$, the **dot product** of u and v, denoted by $u \cdot v$, is

$$u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_n \cdot v_n$$

Using dot products, the previous set ${\mathcal S}$ can be written as

$$\{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}_1 \cdot \boldsymbol{x} = 0, \boldsymbol{a}_2 \cdot \boldsymbol{x} = 0, \dots, \boldsymbol{a}_m \cdot \boldsymbol{x} = 0\}$$

and we know that S is a vector space.