01204211 Discrete Mathematics
Lecture 9a: Spans and Vector Spaces

Jittat Fakcharoenphol

August 30, 2022

Review: Linear combinations

Definition

For any scalars

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

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

Review: Span

Definition

A set of all linear combination of vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ is called the **span** of that set of vectors.
It is denoted by $\mathrm{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m\}$.

Example 1

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

Example 2

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

Example 3

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

Elements in a vector

- 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.

2×2 Lights out

Can you solve 2×2 Lights out?

Let $\boldsymbol{u}_1 = [1, 1, 1, 0]$, $\boldsymbol{u}_2 = [1, 1, 0, 1]$, $\boldsymbol{u}_3 = [1, 0, 1, 1]$, and $\boldsymbol{u}_4 = [0, 1, 1, 1]$.

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

$$a_1 \cdot \boldsymbol{u}_1 + a_2 \cdot \boldsymbol{u}_2 + a_3 \cdot \boldsymbol{u}_3 + a_4 \cdot \boldsymbol{u}_4 = \boldsymbol{b}?$$

Same question: Is $\mathrm{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4\} = GF(2)^4$?

Can you solve 2×2 Lights out?

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

$$a_1 \cdot \boldsymbol{u}_1 + a_2 \cdot \boldsymbol{u}_2 + a_3 \cdot \boldsymbol{u}_3 + a_4 \cdot \boldsymbol{u}_4 = \boldsymbol{b}?$$

Can you solve 2×2 Lights out?

Since

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

and

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

what can we say about $\text{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4\}$?

Generators

Definition

Let $\mathcal{V}$ be a set of vectors. Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$.
If $\mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\} = \mathcal{V}$, we say that

- $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ is a **generating set** for $\mathcal{V}$
- vectors $\boldsymbol{u}_1, \boldsymbol{u}_2 \ldots, \boldsymbol{u}_n$ 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 $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4$.

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

Generators and spans

Lemma 1

Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. *If* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ *are generators for* $\mathcal{V}$, *and for each* i,

$$\boldsymbol{v}_i \in \mathrm{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\},$$

we have that $\mathcal{V} \subseteq \mathrm{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$.

Adding a vector into a span

Lemma 2

Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$. *If* $\boldsymbol{v} \in \mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$, *then*

$$\mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n, \boldsymbol{v}\} = \mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$$

Geometry of spans: in $\mathbb{R}^2$

Geometry of spans: in $\mathbb{R}^3$

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
- if $\boldsymbol{u}$ and $\boldsymbol{v}$ are in the objects, $\boldsymbol{u} + \boldsymbol{v}$ is also in the objects.

Vector spaces

Definition

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

- (V1) $\mathbf{0} \in \mathcal{V}$,
- (V2) for any $\boldsymbol{u} \in \mathcal{V}$,
$$\alpha \cdot \boldsymbol{u} \in \mathcal{V}$$
  for any $\alpha \in \mathbb{F}$, and
- (V3) for any $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}$,
$$\boldsymbol{u} + \boldsymbol{v} \in \mathcal{V}.$$

Span of vectors is a vector space

Consider n-vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$,

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

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 $\mathcal{S}$ of all n-vectors in the form $[x_1, x_2, \ldots, x_n]$ where

$$\begin{aligned}
a_{11} \cdot x_1 + a_{12} \cdot x_2 + \cdots + a_{1n} \cdot x_n &= 0 \\
a_{21} \cdot x_1 + a_{22} \cdot x_2 + \cdots + a_{2n} \cdot x_n &= 0 \\
\vdots &= \vdots \\
a_{m1} x \cdot_1 + a_{m2} \cdot x_2 + \cdots + a_{mn} \cdot x_n &= 0
\end{aligned}$$

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

Dot product

Definition

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

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

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

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

and we know that $\mathcal{S}$ is a vector space.

Parity-check code

From message $\boldsymbol{a} = [a_1, a_2, a_3, a_4]$, we compute (in $GF(2)$) the parity check bit

$$b = a_1 + a_2 + a_3 + a_4.$$

Now our encoded message becomes

$$[a_1, a_2, a_3, a_4, a_5],$$

where $a_5 = b = a_1 + a_2 + a_3 + a_4$. It can detects a single-bit error.

What can we say about the condition on a_5?
It is in fact a homogeneous linear equation (in $GF(2)$):

$$a_1 + a_2 + a_3 + a_4 + a_5 = 0$$

Now, what is the set of all possible codewords?

Hamming code

You can detect and correct more errors with Hamming codes. In this version called a $[7, 4]$ Hamming code, you encode 4-bit data $[a_1, a_2, a_3, a_4]$ into a 7-bit codeword $[a_1, a_2, a_3, a_4, a_5, a_6, a_7]$. Using the formula:

$$\begin{aligned} a_5 &= a_1 + a_2 + a_4 \\ a_6 &= a_1 + a_3 + a_4 \\ a_7 &= a_2 + a_3 + a_4 \end{aligned}$$

Let's see how this works.

Parity check

Let

$$\begin{aligned} s_1 &= a_1 + a_2 + a_4 + a_5 \\ s_2 &= a_1 + a_3 + a_4 + a_6 \\ s_3 &= a_2 + a_3 + a_4 + a_7 \end{aligned}$$

Given a codewords $\boldsymbol{w} = [c_1, c_2, \ldots, c_7]$, if we compute s_1, s_2, s_3, we would get all zero's.

What if there is an error? Let's try.

Codewords from Hamming code

Turning the formula for a_5, a_6, a_7 around, we have 3 homogeneous linear equations:

$$\begin{aligned} a_1 + a_2 + a_4 + a_5 &= 0 \\ a_1 + a_3 + a_4 + a_6 &= 0 \\ a_2 + a_3 + a_4 + a_7 &= 0 \end{aligned}$$

and again the set of all possible codewords $\mathcal{W}$ forms a vector space over $GF(2)$.

An object not passing through the origin: 2 dimensions

An object not passing through the origin: 3 dimensions

Translation

If we have a line or a plane passing through a vector $\boldsymbol{a}$, but not through the origin, how can we represent it?

- Translate the object so that it passes through the origin.
- We obtain a vector space $\mathcal{V}$.
- Then we translate it back so that it passes through $\boldsymbol{a}$.
- We get the set
$$\mathcal{A} = \{\boldsymbol{a} + \boldsymbol{u} : \boldsymbol{u} \in \mathcal{V}\}$$

- *Question:* Is $\mathcal{A}$ a vector space?
- We also write it as $\boldsymbol{a} + \mathcal{V}$.

Affine spaces

Definition

If $\boldsymbol{a}$ is a vector and $\mathcal{V}$ is a vector space, then

$$\boldsymbol{a} + \mathcal{V}$$

is an **affine space**.

An affine space and convex combination: 2 dimensions

An affine space and convex combination: 3 dimensions

Affine combination

Definition

For any scalars $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that

$$\alpha_1 + \alpha_2 + \ldots + \alpha_m = 1$$

and vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$, we say that a linear combination

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

is an **affine combination** of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$.

Definition

The set of all affine combinations of vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ is called the **affine hull** of $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$.

Convex combination: review

Definition

For any scalars $\alpha_1, \alpha_2, \ldots, \alpha_m \geq 0$ such that

$$\alpha_1 + \alpha_2 + \ldots + \alpha_m = 1$$

and vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$, we say that a linear combination

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

is a **convex combination** of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$.

Definition

The set of all convex combinations of vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ is called the **convex hull** of $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$.

Writing an affine space using a span

An affine space

An affine space passing through $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ is

$$\boldsymbol{u}_1 + \mathrm{Span}\,\{\boldsymbol{u}_2 - \boldsymbol{u}_1, \boldsymbol{u}_3 - \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n - \boldsymbol{u}_1\}.$$

Non-homogeneous linear system

Two linear systems:

$$\begin{array}{rcl} \boldsymbol{a_1} \cdot \boldsymbol{x} & = & b_1 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} & = & b_2 \\ & \vdots & \\ \boldsymbol{a_m} \cdot \boldsymbol{x} & = & b_m \end{array} \qquad\qquad \begin{array}{rcl} \boldsymbol{a_1} \cdot \boldsymbol{x} & = & 0 \\ \boldsymbol{a_2} \cdot \boldsymbol{x} & = & 0 \\ & \vdots & \\ \boldsymbol{a_m} \cdot \boldsymbol{x} & = & 0 \end{array}$$

What can you say about the solution sets of these two related linear systems?
$\mathbf{0}$ is always a solution to the linear system on the right.
Note: A linear equation whose right-hand-side is zero is called a **homogeneous linear equation**. A system of linear homogeneous equations is called a **homogeneous linear system**.

Solutions of the two systems

Recall that if $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ are both solutions to the non-homogeneous linear system, we have that for any i

$$\boldsymbol{a}_i\boldsymbol{u}_1 - \boldsymbol{a}_i\boldsymbol{u}_2 = b_i - b_i = 0 = \boldsymbol{a}_i(\boldsymbol{u}_1 - \boldsymbol{u}_2).$$

This implies that $\boldsymbol{u}_1 - \boldsymbol{u}_2$ is a solution to the homogeneous linear system.

Suppose that $\mathcal{W}$ is the set of all solution to the non-homogeneous linear system, i.e.,

$$\mathcal{W} = \{\boldsymbol{x} : \boldsymbol{a}_i \boldsymbol{x} = b_i, \text{ for } 1 \leq i \leq m\},$$

and let $\boldsymbol{u} \in \mathcal{W}$ be one of the solutions, we have that

$$\{\boldsymbol{v} - \boldsymbol{u} : \boldsymbol{v} \in \mathcal{W}\}$$

is a vector space, because

$$\{\boldsymbol{v} - \boldsymbol{u} : \boldsymbol{v} \in \mathcal{W}\} = \{\boldsymbol{x} : \boldsymbol{a}_i \boldsymbol{x} = 0, \text{ for } 1 \leq i \leq m\}$$

In other words,

$$\begin{aligned} \mathcal{W} &= \boldsymbol{u} + \{\boldsymbol{v} - \boldsymbol{u} : \boldsymbol{v} \in \mathcal{W}\} \\ &= \boldsymbol{u} + \{\boldsymbol{x} : \boldsymbol{a}_i \boldsymbol{x} = 0, \text{ for } 1 \leq i \leq m\}, \end{aligned}$$

i.e., $\mathcal{W}$ is an affine space.

Solutions to a non-homogeneous linear system

Lemma 3

If the solution set of a linear system is not empty, it is an affine space.