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

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

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 $GF(2)$?

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.

$$\begin{gathered} 0 + 0 = 0 \\ 0 + 1 = 1 + 0 = 1 \\ 1 + 1 = 0 \end{gathered}$$

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.

$$
\begin{gathered}
0 + 0 = 0 \\
0 + 1 = 1 + 0 = 1 \\
1 + 1 = 0
\end{gathered}
$$

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

$$
\begin{gathered}
0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \\
1 \cdot 1 = 1
\end{gathered}
$$

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

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

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

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

and

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

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

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 $\mathcal{V}$

Generators

Definition

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

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 $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4$.

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

Theorem 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,

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

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

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.

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?

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

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

is a vector space.

Span of vectors is a vector space

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

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

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

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

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

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

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.