01204211 Discrete Mathematics
Lecture 9c: Linear Independence and Bases

Jittat Fakcharoenphol

November 3, 2024

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

Previous Lemmas

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

Lemma 2

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

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

Proof: Consider $w \in \operatorname{Span}\{u_1, \ldots, u_n, v\}$, i.e., there exist $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta$ such that

$$w = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n + \beta v. \quad \text{— (1)}$$

Also since $v \in \operatorname{Span}\{u_1, \ldots, u_n\}$, there exist $\gamma_1, \gamma_2, \ldots, \gamma_n$ s.t.

$$v = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_n u_n. \quad \text{— (2)}$$

Plug in (2) to (1),

$$w = \alpha_1 u_1 + \cdots + \alpha_n u_n + \beta(\gamma_1 u_1 + \cdots + \gamma_n u_n)$$
$$= (\alpha_1 + \beta\gamma_1) u_1 + (\alpha_2 + \beta\gamma_2) u_2 + \cdots + (\alpha_n + \beta\gamma_n) u_n$$
$$\Rightarrow w \in \ldots$$

Lemma 2

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

$$\text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n, \boldsymbol{v}\} = \text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$$

Lemma 3

Consider vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$. *If* $\boldsymbol{u}_n \in \text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_{n-1}\}$, *then*

$$\text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_{n-1}\} = \text{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n\}$$

Proof of Lemma 2.

Since $\boldsymbol{v}$ can be written as a linear combination of other vectors, there exist $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$\boldsymbol{v} = \alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_n \boldsymbol{u}_n.$$

Consider any vector $\boldsymbol{w} \in \mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n, \boldsymbol{v}\}$; thus, we can write

$$\boldsymbol{w} = \beta_0 \boldsymbol{v} + \beta_1 \boldsymbol{u}_1 + \beta_2 \boldsymbol{u}_2 + \cdots + \beta_n \boldsymbol{u}_n.$$

Plugging in $\boldsymbol{v}$, we get that

$$\begin{aligned}\boldsymbol{w} &= \beta_0 \left(\alpha_1 \boldsymbol{u}_1 + \cdots + \alpha_n \boldsymbol{u}_n\right) + \beta_1 \boldsymbol{u}_1 + \beta_2 \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k \\ &= (\beta_0 \alpha_1 + \beta_1) \boldsymbol{u}_1 + (\beta_0 \alpha_2 + \beta_2) \boldsymbol{u}_2 + \cdots + (\beta_0 \alpha_n + \beta_n) \boldsymbol{u}_n,\end{aligned}$$

implying that $\boldsymbol{w} \in \mathrm{Span}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$.

$\square$

Linearly independence

Definition

Vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ are **linearly independent** if no vector $\boldsymbol{u}_i$ can be written as a linear combination of other vectors.

u_1, u_2, u_3, u_4, u_5

$u_1 = [1, 0, 0, 0, 0]$

$u_2 = [0, 1, 0, 0, 0]$

$u_3 = [2, 2, 1, 1, 1]$

$u_4 = [0, 0, 0, 1, 1]$

$u_5 = [1, 1, 1, 1, 1]$

Can you write u_5 as a linear combination of u_1, u_2, u_3, u_4 ?

$[0, 0, 1, 1, 1]$

$\shortparallel$

$(u_3 - 2u_1 - 2u_2) + u_1 + u_2$

$= u_3 - u_1 - u_2 = (-1)u_1 + (-1)u_2 + u_3 + 0 \cdot u_4$

Linearly independence

$u_1, u_2, \dots, u_{n-1}, u_n$

$0 = \cancel{u_n - u_n} = \underline{\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_{n-1} u_{n-1} - u_n}$

Definition

Vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ are **linearly independent** if no vector $\boldsymbol{u}_i$ can be written as a linear combination of other vectors.

(Another) Definition

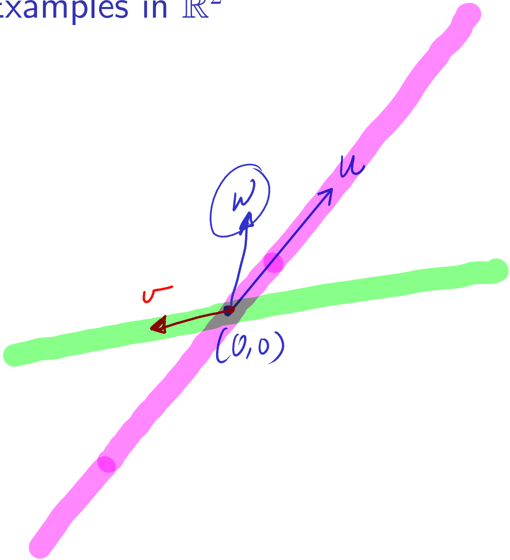
→ Vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_n$ are **linearly independent** if the only solution of equation

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \dots + \alpha_n \boldsymbol{u}_n = \boldsymbol{0}$$

is

$$\alpha_1 = \alpha_2 = \dots = \alpha_n = 0.$$

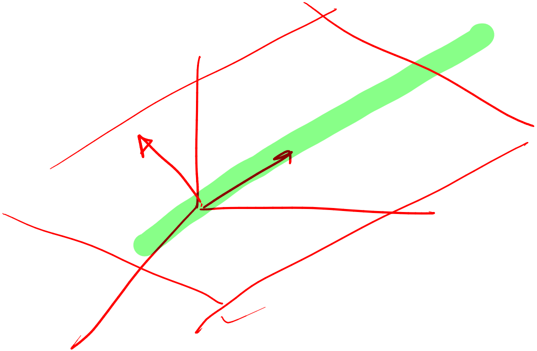
Examples in $\mathbb{R}^2$



$\mathrm{Span}\{u,v\} = \mathbb{R}^2$

$\nexists\, w \in \mathbb{R}^2$, s.t. $w \notin \mathrm{Span}\{u,v\}$

Examples in $\mathbb{R}^3$



Examples in $GF(2)$

Examples in linear systems

Subset of linearly independent vectors

Lemma 4

If $A = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ be a set of linearly independent vectors, then any $B \subseteq A$ is also a set of linearly independent vectors.

Proof.

We prove by contradiction. Assume that B is **not** linearly independent. Without loss of generality, assume that $B = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ where $k \leq n$.

Subset of linearly independent vectors

Lemma 4

If $A = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ *be a set of linearly independent vectors, then any* $B \subseteq A$ *is also a set of linearly independent vectors.*

Proof.

We prove by contradiction. Assume that B is **not** linearly independent. Without loss of generality, assume that $B = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ where $k \leq n$. This means that there exists $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k = \boldsymbol{0},$$

and some α_i's is nonzero.

Subset of linearly independent vectors

Lemma 4

If $A = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ be a set of linearly independent vectors, then any $B \subseteq A$ is also a set of linearly independent vectors.

Proof.

We prove by contradiction. Assume that B is **not** linearly independent. Without loss of generality, assume that $B = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ where $k \leq n$. This means that there exists $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that

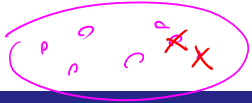
$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k = \mathbf{0},$$

and some α_i's is nonzero. If we let $\alpha_{k+1} = \alpha_{k+2} = \cdots = \alpha_n = 0$, we have that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_n \boldsymbol{u}_n = \mathbf{0},$$

with some α_i's being nonzero as well.

Subset of linearly independent vectors



Lemma 4

If $A = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ be a set of linearly independent vectors, then any $B \subseteq A$ is also a set of linearly independent vectors.

Proof.

We prove by contradiction. Assume that B is **not** linearly independent. Without loss of generality, assume that $B = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ where $k \leq n$. This means that there exists $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k = \mathbf{0},$$

and some α_i's is nonzero. If we let $\alpha_{k+1} = \alpha_{k+2} = \cdots = \alpha_n = 0$, we have that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_n \boldsymbol{u}_n = \mathbf{0},$$

with some α_i's being nonzero as well. This implies that vectors in A are not linearly independept; leading to a contradiction. $\square$

Bases

Definition

A set of vectors $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ is a **basis** for vector space $\mathcal{V}$ if

- $\text{Span}\ \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\} = \mathcal{V}$, and
- $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ are linearly independent.

Examples 1: $\mathbb{R}^2$ and $\mathbb{R}^3$

Examples 2

Lemma 5 (Unique representation)

Let $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ *be a basis for vector space* $\mathcal{V}$. *For any* $\boldsymbol{v} \in \mathcal{V}$, *there is a unique way to write* $\boldsymbol{v}$ *as a linear combination of* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$.

Proof of unique representation lemma.

We prove by contradiction.

Proof of unique representation lemma.

We prove by contradiction. Assume that there exists a vector $\boldsymbol{v} \in \mathcal{V}$ with more than one ways to be written as linear combinations of the basis. Thus, there exist

$$\alpha_1, \alpha_2, \ldots, \alpha_k,$$

and

$$\beta_1, \beta_2, \ldots, \beta_k,$$

that are not equal (i.e., there exists i where $\alpha_i \neq \beta_i$) such that $\boldsymbol{v} = \alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k$ and $\boldsymbol{v} = \beta_1 \boldsymbol{u}_1 + \beta_2 \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k$.

Proof of unique representation lemma.

We prove by contradiction. Assume that there exists a vector $\boldsymbol{v} \in \mathcal{V}$ with more than one ways to be written as linear combinations of the basis. Thus, there exist

$$\alpha_1, \alpha_2, \ldots, \alpha_k,$$

and

$$\beta_1, \beta_2, \ldots, \beta_k,$$

that are not equal (i.e., there exists i where $\alpha_i \neq \beta_i$) such that $\boldsymbol{v} = \alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k$ and $\boldsymbol{v} = \beta_1 \boldsymbol{u}_1 + \beta_2 \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k$. This implies that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k = \boldsymbol{v} = \beta_1 \boldsymbol{u}_1 + \beta \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k,$$

and

$$(\alpha_1 - \beta_1)\boldsymbol{u}_1 + (\alpha_2 - \beta_2)\boldsymbol{u}_2 + \cdots + (\alpha_k - \beta_k)\boldsymbol{u}_k = 0.$$

Proof of unique representation lemma.

We prove by contradiction. Assume that there exists a vector $\boldsymbol{v} \in \mathcal{V}$ with more than one ways to be written as linear combinations of the basis. Thus, there exist

$$\alpha_1, \alpha_2, \ldots, \alpha_k,$$

and

$$\beta_1, \beta_2, \ldots, \beta_k,$$

that are not equal (i.e., there exists i where $\alpha_i \neq \beta_i$) such that $\boldsymbol{v} = \alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k$ and $\boldsymbol{v} = \beta_1 \boldsymbol{u}_1 + \beta_2 \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k$. This implies that

$$\alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \cdots + \alpha_k \boldsymbol{u}_k = \boldsymbol{v} = \beta_1 \boldsymbol{u}_1 + \beta \boldsymbol{u}_2 + \cdots + \beta_k \boldsymbol{u}_k,$$

and

$$(\alpha_1 - \beta_1)\boldsymbol{u}_1 + (\alpha_2 - \beta_2)\boldsymbol{u}_2 + \cdots + (\alpha_k - \beta_k)\boldsymbol{u}_k = 0.$$

Since $\alpha_i \neq \beta_i$, we have that at least one of the coefficients is non-zero, implying that $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ are not linearly independent. This contradicts the assumption that $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ form a basis. $\square$