01204211 Discrete Mathematics
Lecture 10b: Dimensions

Jittat Fakcharoenphol

September 6, 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 $\mathrm{Span}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m\}$.

Review: 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 $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}$,
  $$\boldsymbol{u} + \boldsymbol{v} \in \mathcal{V}.$$

Review: 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.

(Another) Definition

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

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

is

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

Review: 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

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

Lemma 1 (Superfluous Vector Lemma)

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*

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

Lemma 2

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

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

Lemma 3 (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* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$*.*

Examples in $\mathbb{R}^2$ and $\mathbb{R}^3$

Examples in $GF(2)$ - Vector spaces from graphs

Examples in $GF(2)$ - Cycles

Examples in $GF(2)$ - Basis

Number of vectors in bases

- We have an observation that for a vector space $\mathcal{V}$, every basis has the same size.
- This is not a coincident.
- In this course, we will see two proofs.
- Remark: there are vector spaces whose basis has infinite size, but we are not dealing with those vector spaces in this course.

Theorem 4 (Main Theorem)

If $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ *and* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ *are bases for vector space* $\mathcal{W}$*, then* $n = m$*.*

Exchange Lemma

We will prove the main theorem using the "exchange" lemma.

Lemma 5 (Simplified Exchange Lemma)

Consider a set of vectors S *and let* $\boldsymbol{z}$ *be a non-zero vector in* $\text{Span } S$*. There is a vector* $\boldsymbol{w} \in S$ *such that* $\text{Span } (S \cup \{\boldsymbol{z}\} - \{\boldsymbol{w}\}) = \text{Span } S$*.*

Lemma 6 (Exchange Lemma)

Consider a set of vectors S *and its subset* A*. Let* $\boldsymbol{z}$ *be a non-zero vector in* $\text{Span } S$ *such that* $A \cup \{\boldsymbol{z}\}$ *is linearly independent. There is a vector* $\boldsymbol{w} \in S - A$ *such that* $\text{Span } (S \cup \{\boldsymbol{z}\} - \{\boldsymbol{w}\}) = \text{Span } S$*.*

Lemma 7 (Morphing Lemma)

If a set of vectors S spans a vector space $\mathcal{W}$ and B is a linearly independent set of vectors in $\mathcal{W}$, then $|B| \leq |S|$.

Proof.

Let $B = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$. We show how to construct $S_1, \ldots, S_n$ such that for each i, $|S_i| = |S|$, $\mathrm{Span}\ S_i = \mathrm{Span}\ S$, and

$$\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i\} \subseteq S_i.$$

Let $S_0 = S$. We construct S_i from S_{i-1}. Note that since B is linearly independent, $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}\} \subseteq S_{i-1}$ is also linearly independent. We can use the Exchange Lemma to state that there exist $\boldsymbol{w} \in S_{i-1} - \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}\}$ such that

$$\mathrm{Span}\ (S_{i-1} \cup \{\boldsymbol{u_i}\} - \{\boldsymbol{w}\}) = \mathrm{Span}\ S_{i-1}.$$

We then let $S_i = S_{i-1} \cup \{\boldsymbol{u_i}\} - \{\boldsymbol{w}\}$. (You can check that S_i has the properties as claimed above.)

Since $|S_n| = |S|$ and $B \subseteq S_n$, we have that $|B| \leq |S|$. $\square$

Morphing Lemma $\Rightarrow$ Main Theorem

Theorem 8 (Main Theorem)

If $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ *and* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ *are bases for vector space* $\mathcal{W}$*, then* $n = m$*.*

Proof.

Since $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$ is a basis, it spans $\mathcal{W}$. Also, vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ are linearly independent because they also form a basis. Thus, from the Morphing Lemma, $m \leq n$.
We can reverse the roles of $\boldsymbol{u}_i$'s and $\boldsymbol{v}_i$'s to obtain that $n \leq m$.
Therefore, $n = m$. $\square$

Proof of the Simplified Exchange Lemma.

Let $S = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n\}$. Since $\boldsymbol{z} \in \mathrm{Span}\ S$, we note that $\mathrm{Span}\ S = \mathrm{Span}\ (S \cup \{\boldsymbol{z}\})$. We can also write

$$\boldsymbol{z} = \alpha_1 \boldsymbol{u}_1 + \alpha_2 \boldsymbol{u}_2 + \ldots + \alpha_n \boldsymbol{u}_n.$$

Because $\boldsymbol{z}$ is non-zero, there exists some non-zero α_i. We can rewrite the above equation as

$$\alpha_i \boldsymbol{u}_i = \boldsymbol{z} - \alpha_1 \boldsymbol{u}_1 - \ldots - \alpha_{i-1} \boldsymbol{u}_{i-1} - \alpha_{i+1} \boldsymbol{u}_{i+1} - \cdots - \alpha_n \boldsymbol{u}_n,$$

or

$$\boldsymbol{u}_i = \left(\frac{1}{\alpha_i} \boldsymbol{z} - \frac{\alpha_1}{\alpha_i} \boldsymbol{u}_1 - \ldots - \frac{\alpha_{i-1}}{\alpha_i} \boldsymbol{u}_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} \boldsymbol{u}_{i+1} - \cdots - \frac{\alpha_n}{\alpha_i} \boldsymbol{u}_n \right),$$

i.e., $\boldsymbol{u}_i \in \mathrm{Span}\ (S \cup \{\boldsymbol{z}\})$. In this case, we can remove $\boldsymbol{u}_i$, i.e.,

$$\mathrm{Span}\ (S \cup \{\boldsymbol{z}\} - \{\boldsymbol{u}_i\}) = \mathrm{Span}\ (S \cup \{\boldsymbol{z}\}) = \mathrm{Span}\ S.$$

Therefore we can let $\boldsymbol{w} = \boldsymbol{u}_i$ and the lemma follows. $\square$

How can we prove the full lemma?

Dimensions

Definition

The **dimension** of a vector space $\mathcal{V}$ is the size of its basis.
The dimension of $\mathcal{V}$ is written as $\dim \mathcal{V}$.