Linear Algebra

Trivandrum School on Communication, Coding and Networking 2017

Prasad Krishnan

Signal Processing and Communications Research Centre,
International Institute of Information Technology, Hyderabad

January 27-30, 2017

Linear Algebra

- Vector Spaces
  - Definitions : Fields and Vector Space.
  - Linear Combinations.
  - Linear Independence and Dependence.
  - Subspaces
  - Basis and Dimension.
  - Vectors as tuples.
  - Basis change matrix.
- Linear Transformations.
  - Definition.
  - Linear Transformations as Matrices.
  - Similar matrices.
  - Range and Null Space of Linear Transformations.
  - Rank-Nullity Theorem.
  - Eigen values and vectors of a Linear Operator.

General ideas about Math-based Education and Research

- Math is not hard!
- There are only sets and maps (relations between sets).
- Start from basic axioms.
- Connect simple facts to create bigger facts (not always easy!).
- Imagination and Creativity.

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**
- Examples: Number of apples in a basket of infinite apples?

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**
- Examples: Number of apples in a basket of infinite apples? (**No**).
- Temperature (

IIIT, HYDERABAD

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**
- Examples: Number of apples in a basket of infinite apples? (**No**).
- Temperature (**No**).
- Examples : $(\mathbb{R}, +, .)$ (

IIIT, HYDERABAD

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**
- Examples: Number of apples in a basket of infinite apples? (**No**).
- Temperature (**No**).
- Examples : $(\mathbb{R}, +, .)$ (**Yes**)
- $(\mathbb{F}_p, + \ (mod \ p), x \ (mod \ p))$ (integers modulo p). (

IIIT, HYDERABAD

Field - A rough definition

- *Fields (Scalars)* : A set which is closed under addition (and subtraction), multiplication (and division by non-zeros) - **How much?**
- Examples: Number of apples in a basket of infinite apples? (**No**).
- Temperature (**No**).
- Examples : $(\mathbb{R}, +, .)$ (**Yes**)
- $(\mathbb{F}_p, + \ (mod \ \ p), x \ (mod \ \ p))$ (integers modulo p). (**Yes**)

IIIT, HYDERABAD

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of ‘coordinate-tuples’].

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$

Vector Spaces over fields - A rough definition

- Space $=$ set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).

Vector Spaces over fields - A rough definition

- Space $=$ set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$

IIIT, HYDERABAD

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),
- Set of finite energy signals over $\mathbb{R}$.

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),
- Set of finite energy signals over $\mathbb{R}$. **(Yes!)**

Vector Spaces over fields - A rough definition

- Space $=$ set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),
- Set of finite energy signals over $\mathbb{R}$. **(Yes!)**
- $\mathbb{F}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{F}\}$ over $\mathbb{F}$.

IIIT, HYDERABAD

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),
- Set of finite energy signals over $\mathbb{R}$. **(Yes!)**
- $\mathbb{F}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{F}\}$ over $\mathbb{F}$. **(Yes!)**
- Set of locations within a room, over $\mathbb{R}$

IIIT, HYDERABAD

Vector Spaces over fields - A rough definition

- Space = set.
- *Vector space V over a field of scalars* $\mathbb{F}$: A set closed under addition, scalar multiplication [A set of 'coordinate-tuples'].
- Examples: $\{(a, b) : a, b \in \mathbb{Z}\}$ over $\mathbb{R}$ (**No!**).
- Examples: $\{(a, b) : a, b \in \mathbb{R}\}$ over $\mathbb{R}$ (**Yes!**),
- Set of finite energy signals over $\mathbb{R}$. **(Yes!)**
- $\mathbb{F}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{F}\}$ over $\mathbb{F}$. **(Yes!)**
- Set of locations within a room, over $\mathbb{R}$ **(No!)**

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

- For $\boldsymbol{x} = x(t)$, $\boldsymbol{y} = y(t)$ (complex-valued functions), define

$$< \mathbf{x}, \mathbf{y} >= \int_{-\infty}^{\infty} x(t) y^*(t) dt \in \mathbb{C}.$$

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

- For $\boldsymbol{x} = x(t)$, $\boldsymbol{y} = y(t)$ (complex-valued functions), define

$$< \mathbf{x}, \mathbf{y} >= \int_{-\infty}^{\infty} x(t) y^*(t) dt \in \mathbb{C}.$$

- *Energy* of the signal $x(t)$, $||\mathbf{x}||^2 =< \mathbf{x}, \mathbf{x} >$.
- If $||\mathbf{x}|| < \infty$, then signal $x(t)$ has finite energy.

Need for Linear Algebra in Communications and Coding

- For $\boldsymbol{x} = x(t)$, $\boldsymbol{y} = y(t)$ (complex-valued functions), define

$$< \mathbf{x}, \mathbf{y} >= \int_{-\infty}^{\infty} x(t) y^*(t) dt \in \mathbb{C}.$$

- *Energy* of the signal $x(t)$, $||\mathbf{x}||^2 =< \mathbf{x}, \mathbf{x} >$.
- If $||\mathbf{x}|| < \infty$, then signal $x(t)$ has finite energy.

Theorem

Finite-energy signals form a vector space over $\mathbb{C}$.

Need for Linear Algebra in Communications and Coding

- For $\boldsymbol{x} = x(t)$, $\boldsymbol{y} = y(t)$ (complex-valued functions), define

$$< \mathbf{x}, \mathbf{y} >= \int_{-\infty}^{\infty} x(t)y^*(t)dt \in \mathbb{C}.$$

- *Energy* of the signal $x(t)$, $||\mathbf{x}||^2 =< \mathbf{x}, \mathbf{x} >$.
- If $||\mathbf{x}|| < \infty$, then signal $x(t)$ has finite energy.

Theorem

Finite-energy signals form a vector space over $\mathbb{C}$.

Proof:

- If $x(t)$ is finite-energy, then so is $cx(t)$ for any $c \in \mathbb{C}$.
- To show : If $x(t), y(t)$ are finite-energy, then so is $x(t) + y(t)$.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

- For $\boldsymbol{x} = x(t)$, $\boldsymbol{y} = y(t)$ (complex-valued functions), define

$$< \mathbf{x}, \mathbf{y} >= \int_{-\infty}^{\infty} x(t)y^*(t)dt \in \mathbb{C}.$$

- *Energy* of the signal $x(t)$, $||\mathbf{x}||^2 =< \mathbf{x}, \mathbf{x} >$.
- If $||\mathbf{x}|| < \infty$, then signal $x(t)$ has finite energy.

Theorem

Finite-energy signals form a vector space over $\mathbb{C}$.

Proof:

- If $x(t)$ is finite-energy, then so is $cx(t)$ for any $c \in \mathbb{C}$.
- To show : If $x(t), y(t)$ are finite-energy, then so is $x(t) + y(t)$.
- Given : $||\boldsymbol{x}|| < \infty$, $||\boldsymbol{y}|| < \infty$, show $||\boldsymbol{x} + \boldsymbol{y}|| < \infty$.

Need for Linear Algebra in Communications and Coding

$$
\begin{aligned}
||\boldsymbol{x}+\boldsymbol{y}||^2 &= ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + <\boldsymbol{x},\boldsymbol{y}> + <\boldsymbol{y},\boldsymbol{x}> \\
&\leq ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2|<\boldsymbol{x},\boldsymbol{y}>|. \\
&\leq ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2||\boldsymbol{x}||.||\boldsymbol{y}|| \quad (\text{if } \; |<\boldsymbol{x},\boldsymbol{y}>| \leq ||\boldsymbol{x}||.||\boldsymbol{y}||) \\
&< \infty \qquad (\text{as each of the above terms are finite})
\end{aligned}
$$

.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

$$
\begin{aligned}
||\boldsymbol{x}+\boldsymbol{y}||^2 &= ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + <\boldsymbol{x},\boldsymbol{y}> + <\boldsymbol{y},\boldsymbol{x}> \\
&\leq ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2|<\boldsymbol{x},\boldsymbol{y}>|. \\
&\leq ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 + 2||\boldsymbol{x}||.||\boldsymbol{y}|| \quad (\text{if } \ |<\boldsymbol{x},\boldsymbol{y}>| \leq ||\boldsymbol{x}||.||\boldsymbol{y}||) \\
&< \infty \qquad (\text{as each of the above terms are finite})
\end{aligned}
$$

.

Cauchy-Schwarz inequality

$$|<\boldsymbol{x},\boldsymbol{y}>| \leq ||\boldsymbol{x}||.||\boldsymbol{y}||$$

Proof: Fact: $||\boldsymbol{x}-\lambda\boldsymbol{y}||^2 \geq 0$, for any $\lambda \in \mathbb{C}$. Expand this and substitute $\lambda = \frac{<\boldsymbol{x},\boldsymbol{y}>}{||\boldsymbol{y}||^2}$.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

$$
\begin{aligned}
||\boldsymbol{x}+\boldsymbol{y}||^2 &= ||\boldsymbol{x}||^2+||\boldsymbol{y}||^2+ <\boldsymbol{x},\boldsymbol{y}> + <\boldsymbol{y},\boldsymbol{x}> \\
&\leq ||\boldsymbol{x}||^2+||\boldsymbol{y}||^2+2|<\boldsymbol{x},\boldsymbol{y}>|. \\
&\leq ||\boldsymbol{x}||^2+||\boldsymbol{y}||^2+2||\boldsymbol{x}||.||\boldsymbol{y}|| \quad (\text{if } \ |<\boldsymbol{x},\boldsymbol{y}>| \leq ||\boldsymbol{x}||.||\boldsymbol{y}||) \\
&< \infty \qquad (\text{as each of the above terms are finite})
\end{aligned}
$$

.

Cauchy-Schwarz inequality

$$|<\boldsymbol{x},\boldsymbol{y}>| \leq ||\boldsymbol{x}||.||\boldsymbol{y}||$$

Proof: Fact: $||\boldsymbol{x}-\lambda\boldsymbol{y}||^2 \geq 0$, for any $\lambda \in \mathbb{C}$. Expand this and substitute $\lambda = \frac{<\boldsymbol{x},\boldsymbol{y}>}{||\boldsymbol{y}||^2}$.

(Turns out that $<x,y>$ is also an example of a linear algebraic object called inner product)

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

1. Finite-energy signals form a vector space over $\mathbb{C}$.

Field : Formal Definition

Definition: Fields

A *field* $\mathbb{F}$ is a set S with two operations (addition $(+)$ and multiplication(.)) such that

- For any $a, b \in S$, $a + b \in S$ (*closure under addition*)

Field : Formal Definition

Definition: Fields

A *field* $\mathbb{F}$ is a set S with two operations (addition $(+)$ and multiplication(.)) such that

- For any $a, b \in S$, $a + b \in S$ (*closure under addition*)
- Given $a, b, c \in S$, then $a + (b + c) = (a + b) + c$. (Addition is *associative*).

IIIT, HYDERABAD

Field : Formal Definition

Definition: Fields

A *field* $\mathbb{F}$ is a set S with two operations (addition $(+)$ and multiplication(.)) such that

- For any $a, b \in S$, $a + b \in S$ (*closure under addition*)
- Given $a, b, c \in S$, then $a + (b + c) = (a + b) + c$. (Addition is *associative*).
- There exists a special element $0 \in S$ such that $a + 0 = 0 + a = a$ for all $a \in S$ (*Additive identity* exists).

Field : Formal Definition

Definition: Fields

A *field* $\mathbb{F}$ is a set S with two operations (addition $(+)$ and multiplication(.)) such that

- For any $a, b \in S$, $a + b \in S$ (*closure under addition*)
- Given $a, b, c \in S$, then $a + (b + c) = (a + b) + c$. (Addition is *associative*).
- There exists a special element $0 \in S$ such that $a + 0 = 0 + a = a$ for all $a \in S$ (*Additive identity* exists).
- For $a \in S$ there exists an element $b \in S$ such that $a + b = b + a = 0$. (We write this element b as $-a$ and call it the *Additive inverse* of a in S. **Note: Subtraction is just addition with additive inverse.**)

IIIT, HYDERABAD

Field : Formal Definition

Definition: Fields

A *field* $\mathbb{F}$ is a set S with two operations (addition $(+)$ and multiplication$(.)$) such that

- For any $a, b \in S$, $a + b \in S$ (*closure under addition*)
- Given $a, b, c \in S$, then $a + (b + c) = (a + b) + c$. (Addition is *associative*).
- There exists a special element $0 \in S$ such that $a + 0 = 0 + a = a$ for all $a \in S$ (*Additive identity* exists).
- For $a \in S$ there exists an element $b \in S$ such that $a + b = b + a = 0$. (We write this element b as $-a$ and call it the *Additive inverse* of a in S. **Note: Subtraction is just addition with additive inverse.**)
- For all $a, b \in S$, $a + b = b + a$ (*Addition is Commutative*)

IIIT, HYDERABAD

Definition: Fields (continued)

..such that..

- S is closed under multiplication.
- Multiplication is associative.
- Multiplicative identity exists (denoted by 1).
- Multiplicative inverses exist for all elements but 0.
- Multiplication is commutative.

Definition: Fields (continued)

..such that..

- S is closed under multiplication.
- Multiplication is associative.
- Multiplicative identity exists (denoted by 1).
- Multiplicative inverses exist for all elements but 0.
- Multiplication is commutative.

...such that..

- For all $a, b, c \in S$, $a.(b + c) = a.b + a.c$ (Distributivity of multiplication).

It is really over! (I think)

Fields: Informally

Fields

A set where we can add, multiply, subtract (add with additive inverses), and divide (multiply with multiplicative inverses) and things work out *nicely*.

- Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.
- Non-examples: $\mathbb{R}^{m \times k}$ matrices ($m = k \neq 1$).

Fields: Informally

Fields

A set where we can add, multiply, subtract (add with additive inverses), and divide (multiply with multiplicative inverses) and things work out *nicely*.

- Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.
- Non-examples: $\mathbb{R}^{m\times k}$ matrices $(m = k \neq 1)$.
- Think: What kind of structure exist if $k = m = 1$?, $k = m$?, $k \neq m$?.

Vector Spaces : Formal Definition

A set V is a vector space over $\mathbb{F}$ *(field of scalars)* if the following properties are satisfied :

- V is closed under vector addition, which is commutative and associative. $\forall \boldsymbol{v}, \boldsymbol{w} \in V$, $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{w} + \boldsymbol{v} \in V$.

IIIT, HYDERABAD

Vector Spaces : Formal Definition

A set V is a vector space over $\mathbb{F}$ *(field of scalars)* if the following properties are satisfied :

- V is closed under vector addition, which is commutative and associative. $\forall \boldsymbol{v}, \boldsymbol{w} \in V$, $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{w} + \boldsymbol{v} \in V$.
- There exists $\mathbf{0} \in V$, $\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}$ [Zero vector (Additive identity)]

IIIT, HYDERABAD

Vector Spaces : Formal Definition

A set V is a vector space over $\mathbb{F}$ *(field of scalars)* if the following properties are satisfied :

- V is closed under vector addition, which is commutative and associative. $\forall \boldsymbol{v}, \boldsymbol{w} \in V$, $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{w} + \boldsymbol{v} \in V$.
- There exists $\mathbf{0} \in V$, $\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}$ [Zero vector (Additive identity)]
- $\forall \boldsymbol{x} \in V$, there exists $\boldsymbol{y} \in V$ such that $\boldsymbol{x} + \boldsymbol{y} = 0$. (Additive inverse exists).

Vector Space: Formal Definition

...if the following properties are satisfied :

- V is closed under Scalar Multiplication.
  $\forall \boldsymbol{x} \in V, \forall \alpha \in \mathbb{F}, \alpha \boldsymbol{x} \in V$.

Vector Space: Formal Definition

...if the following properties are satisfied :

- V is closed under Scalar Multiplication.
  $\forall \boldsymbol{x} \in V, \forall \alpha \in \mathbb{F}, \alpha \boldsymbol{x} \in V$.
- $\forall \boldsymbol{x}, \boldsymbol{y} \in V$ and $\alpha, \beta \in \mathbb{F}$
  1. $1\boldsymbol{x} = \boldsymbol{x}$
  2. $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \alpha \boldsymbol{x} + \alpha \boldsymbol{y}$
  3. $(\alpha\beta)\boldsymbol{x} = \alpha(\beta \boldsymbol{x})$
  4. $(\alpha + \beta)\boldsymbol{x} = \alpha \boldsymbol{x} + \beta \boldsymbol{x}$

Vector Space: Informal Definition

Vector space V over $\mathbb{F}$

A set closed under addition, scalar multiplication (multiplication by scalars from $\mathbb{F}$).

Notation:

Vector Space: Informal Definition

Vector space V over $\mathbb{F}$

A set closed under addition, scalar multiplication (multiplication by scalars from $\mathbb{F}$).

Notation:

- Normal font, (α, β) for scalars.
- Bold fonts $(\boldsymbol{v}, \boldsymbol{w})$ for vectors.
- Caps for Vector spaces (V, W).
- $\mathbb{F}$ for field.

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha\boldsymbol{v} + \boldsymbol{w} \in V, \forall\alpha$.

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha \boldsymbol{v} + \boldsymbol{w} \in V, \forall \alpha$.
- Examples:
- $V = \mathbb{R}^3$

$$W = \{(x_1, x_2, x_3) \in : x_1 + 2x_2 + 5x_3 = 0\}$$

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha \boldsymbol{v} + \boldsymbol{w} \in V, \forall \alpha$.
- Examples:
- $V = \mathbb{R}^3$

$$W = \{(x_1, x_2, x_3) \in : x_1 + 2x_2 + 5x_3 = 0\}$$

(**Yes!**)

IIIT, HYDERABAD

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha \boldsymbol{v} + \boldsymbol{w} \in V, \forall \alpha$.
- Examples:
- $V = \mathbb{R}^3$

$$W = \{(x_1, x_2, x_3) \in : x_1 + 2x_2 + 5x_3 = 0\}$$

(**Yes!**)

- $V = \{(x_1, x_2) \in \mathbb{R}^2 : x_2 = x_1 + 1\}$

IIIT, HYDERABAD

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha \boldsymbol{v} + \boldsymbol{w} \in V, \forall \alpha$.
- Examples:
- $V = \mathbb{R}^3$

$$W = \{(x_1, x_2, x_3) \in : x_1 + 2x_2 + 5x_3 = 0\}$$

  (**Yes!**)
- $V = \{(x_1, x_2) \in \mathbb{R}^2 : x_2 = x_1 + 1\}$ (**No!**)
- Set of all polynomials of degree only 5.

IIIT, HYDERABAD

Subspaces

- $W \subseteq V$ is called a subspace if it is a vector space (over $\mathbb{F}$).
- Checking whether a subset is a subspace:
  - For all $\boldsymbol{v}, \boldsymbol{w} \in V$, $\alpha \boldsymbol{v} + \boldsymbol{w} \in V, \forall \alpha$.
- Examples:
- $V = \mathbb{R}^3$

$$W = \{(x_1, x_2, x_3) \in : x_1 + 2x_2 + 5x_3 = 0\}$$

  (**Yes!**)
- $V = \{(x_1, x_2) \in \mathbb{R}^2 : x_2 = x_1 + 1\}$ (**No!**)
- Set of all polynomials of degree only 5. (**No!**)

IIIT, HYDERABAD

Linear Combination of vectors

- A linear combination of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, ..., r\} \subset V$ is

$$\sum_{i=1}^{r} \alpha_i \boldsymbol{v_i},$$

for some $\alpha_i \in \mathbb{F}$.

- Note that if $\alpha_i = 0, \forall i$, then the linear combination gives the $\mathbf{0} \in V$.
- Examples: $S = \{(1\ 0\ 0), (0\ 1\ 0)\}$. Then $(1\ 1\ 0)$ is a linear combination.

Linear Dependence

Linear Dependence of vectors

- Vectors $\{\boldsymbol{v_i} : i = 1, ..., r\}$ are called *linearly dependent*

$$\sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} = \mathbf{0},$$

for some α_is, at least one of which is non-zero.

IIIT, HYDERABAD

Linear Dependence

Linear Dependence of vectors

- Vectors $\{\boldsymbol{v_i} : i = 1, ..., r\}$ are called *linearly dependent*

$$\sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} = \mathbf{0},$$

for some α_is, at least one of which is non-zero.

- If $\alpha_j \neq 0$ for some $1 \leq j \leq r$ then

$$\boldsymbol{v_j} = \sum_{i=1, i \neq j}^{r} \beta_i \boldsymbol{v_i},$$

where $\beta_i = \frac{-\alpha_i}{\alpha_j}$.

IIIT, HYDERABAD

Linear Independence

- If $\{\boldsymbol{v_i} : i = 1, ..., r\}$ is not linearly dependent, then they are *linearly independent*.
- Only zero-linear combination gives $\mathbf{0}$.

Examples

- Consider the vectors (from $\mathbb{R}^2$)

$$S = \left\{ \boldsymbol{v_1} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \boldsymbol{v_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \tag{1}$$

- The set $\{\boldsymbol{v_1}, \boldsymbol{v_2}\}$ is linearly

Examples

- Consider the vectors (from $\mathbb{R}^2$)

$$S = \left\{ \mathbf{v_1} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \mathbf{v_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \tag{1}$$

- The set $\{\mathbf{v_1}, \mathbf{v_2}\}$ is linearly independent.

Examples

- Consider the vectors (from $\mathbb{R}^2$)

$$S = \left\{ \mathbf{v_1} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \mathbf{v_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \tag{1}$$

- The set $\{\mathbf{v_1}, \mathbf{v_2}\}$ is linearly independent.
- Consider $S \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. This is linearly

Examples

- Consider the vectors (from $\mathbb{R}^2$)

$$S = \left\{ \boldsymbol{v_1} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \boldsymbol{v_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \tag{1}$$

- The set $\{\boldsymbol{v_1}, \boldsymbol{v_2}\}$ is linearly independent.
- Consider $S \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. This is linearly dependent.
- Consider $S \cup \{\mathbf{0}\}$. This is linearly

Examples

- Consider the vectors (from $\mathbb{R}^2$)

$$S = \left\{ \boldsymbol{v_1} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \boldsymbol{v_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \tag{1}$$

- The set $\{\boldsymbol{v_1}, \boldsymbol{v_2}\}$ is linearly independent.
- Consider $S \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. This is linearly dependent.
- Consider $S \cup \{\mathbf{0}\}$. This is linearly dependent.

IIIT, HYDERABAD

Span of a subset of vectors

Span

The span of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, ..., r\}$ is the set of all linear combinations of the vectors in that set.

$$span(S) = \left\{ \sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} : \alpha_i \in \mathbb{F} \right\}.$$

Span of a subset of vectors

Span

The span of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, ..., r\}$ is the set of all linear combinations of the vectors in that set.

$$span(S) = \left\{ \sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} : \alpha_i \in \mathbb{F} \right\}.$$

- Let $A \in \mathbb{F}^{m \times n}$.

$$\text{Row space} = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{a_i} : \boldsymbol{a_i} \text{ is the } i^{th} \text{ row of } A,\ \ \alpha_i \in \mathbb{F} \right\}.$$

IIIT, HYDERABAD

Span of a subset of vectors

Span

The span of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, ..., r\}$ is the set of all linear combinations of the vectors in that set.

$$span(S) = \left\{ \sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} : \alpha_i \in \mathbb{F} \right\}.$$

- Let $A \in \mathbb{F}^{m \times n}$.

$$\text{Row space} = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{a_i} : \boldsymbol{a_i} \text{ is the } i^{th} \text{ row of } A,\ \ \alpha_i \in \mathbb{F} \right\}.$$

- $S = \{(1,2),(1,1),(-4,9)\}$. $Span(S) =$

Span of a subset of vectors

Span

The span of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, ..., r\}$ is the set of all linear combinations of the vectors in that set.

$$span(S) = \left\{ \sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} : \alpha_i \in \mathbb{F} \right\}.$$

- Let $A \in \mathbb{F}^{m \times n}$.

$$\text{Row space} = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{a_i} : \boldsymbol{a_i} \text{ is the } i^{th} \text{ row of } A, \;\; \alpha_i \in \mathbb{F} \right\}.$$

- $S = \{(1,2),(1,1),(-4,9)\}$. $Span(S) = \mathbb{R}^2$.

IIIT, HYDERABAD

Span of a subset of vectors

Span

The span of a set of vectors $S = \{\boldsymbol{v_i} : i = 1, \ldots, r\}$ is the set of all linear combinations of the vectors in that set.

$$span(S) = \left\{ \sum_{i=1}^{r} \alpha_i \boldsymbol{v_i} : \alpha_i \in \mathbb{F} \right\}.$$

- Let $A \in \mathbb{F}^{m \times n}$.

$$\text{Row space} = \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{a_i} : \boldsymbol{a_i} \text{ is the } i^{th} \text{ row of } A,\ \ \alpha_i \in \mathbb{F} \right\}.$$

- $S = \{(1, 2), (1, 1), (-4, 9)\}$. $Span(S) = \mathbb{R}^2$.

Basis of a Subspace

Basis of a subspace W

A subset B of W is called a basis of W if

1. B is linearly independent set
2. B spans W

- A subspace $W \subseteq V$ can have multiple bases.

IIIT, HYDERABAD

Basis of a Subspace

Basis of a subspace W

A subset B of W is called a basis of W if

1. B is linearly independent set
2. B spans W

- A subspace $W \subseteq V$ can have multiple bases.
- Examples: Let $V = \{p_0 + p_1 t + p_2 t^2 : p_i \in \mathbb{F}\}$. Basis for V is $\{1, t, t^2\}$ (so is $\{1 + t, 1 + t^2, 1 + t + t^2\}$).

IIIT, HYDERABAD

Basis of a Subspace

Basis of a subspace W

A subset B of W is called a basis of W if

1. B is linearly independent set
2. B spans W

- A subspace $W \subseteq V$ can have multiple bases.
- Examples: Let $V = \{p_0 + p_1 t + p_2 t^2 : p_i \in \mathbb{F}\}$. Basis for V is $\{1, t, t^2\}$ (so is $\{1+t, 1+t^2, 1+t+t^2\}$).
- Any set of k-linearly independent vectors of $\mathbb{F}^k$.

IIIT, HYDERABAD

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.

IIIT, HYDERABAD

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.
3. Note that $\boldsymbol{c_1} \neq \mathbf{0}$. This means we should have some $\boldsymbol{b_i} \in span(\{\boldsymbol{c_1}, \boldsymbol{b_1}, .., , ., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i})$.

IIIT, HYDERABAD

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$,
   $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.
3. Note that $\boldsymbol{c_1} \neq \mathbf{0}$. This means we should have some $\boldsymbol{b_i} \in span(\{\boldsymbol{c_1}, \boldsymbol{b_1}, .., , ., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i})$.
4. Let $B_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i}$. Then B_1 spans V and $|B_1| = |B|$.

IIIT, HYDERABAD

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.
3. Note that $\boldsymbol{c_1} \neq \boldsymbol{0}$. This means we should have some $\boldsymbol{b_i} \in span(\{\boldsymbol{c_1}, \boldsymbol{b_1}, .., ., ., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i})$.
4. Let $B_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i}$. Then B_1 spans V and $|B_1| = |B|$.
5. Continue this. To get B_{k+1}, we add one vector from C to B_k and remove one vector from B_k (while maintaining spanning property).

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.
3. Note that $\boldsymbol{c_1} \neq \mathbf{0}$. This means we should have some $\boldsymbol{b_i} \in span(\{\boldsymbol{c_1}, \boldsymbol{b_1}, .., , ., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i})$.
4. Let $B_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i}$. Then B_1 spans V and $|B_1| = |B|$.
5. Continue this. To get B_{k+1}, we add one vector from C to B_k and remove one vector from B_k (while maintaining spanning property).
6. At stage n, we get $B_n = \{\boldsymbol{c_1}, ..., \boldsymbol{c_n}\}$ which is a spanning set.

IIIT, HYDERABAD

Basis

Theorem

Any two bases for a subspace contain the same number of vectors

Proof:

1. Consider two bases $B = \{\boldsymbol{b_i} : i = 1, .., n\}$, $C = \{\boldsymbol{c_i} : i = 1, .., m\}$. Suppose $n < m$.
2. Consider $A_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. This is a linearly dependent set.
3. Note that $\boldsymbol{c_1} \neq \boldsymbol{0}$. This means we should have some $\boldsymbol{b_i} \in span(\{\boldsymbol{c_1}, \boldsymbol{b_1}, .., , ., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i})$.
4. Let $B_1 = \{\boldsymbol{c_1}, \boldsymbol{b_1}, ..., \boldsymbol{b_n}\} \backslash \boldsymbol{b_i}$. Then B_1 spans V and $|B_1| = |B|$.
5. Continue this. To get B_{k+1}, we add one vector from C to B_k and remove one vector from B_k (while maintaining spanning property).
6. At stage n, we get $B_n = \{\boldsymbol{c_1}, ..., \boldsymbol{c_n}\}$ which is a spanning set.
7. But that means C is dependent (contradiction).

IIIT, HYDERABAD

Basis and Dimension

The following are equivalent:

- B is linearly independent and spans W.
- B is a maximal linearly independent set of W.
- B is a minimal set which spans W.

Basis and Dimension

The following are equivalent:

- B is linearly independent and spans W.
- B is a maximal linearly independent set of W.
- B is a minimal set which spans W.

Dimension of a Subspace W

$$dim(W) = \text{No. of vectors in any basis of } W.$$

Basis Extension

Theorem

Let V be a finite dimensional vector space and S be a linearly independent subset of vectors from V. Then S can be extended to a basis of V, i.e., there is a basis B for V such that $S \subseteq B$.

Basis Extension

Theorem

Let V be a finite dimensional vector space and S be a linearly independent subset of vectors from V. Then S can be extended to a basis of V, i.e., there is a basis B for V such that $S \subseteq B$.

Proof idea:

- If $span(S) = V$, then nothing to prove

Basis Extension

Theorem

Let V be a finite dimensional vector space and S be a linearly independent subset of vectors from V. Then S can be extended to a basis of V, i.e., there is a basis B for V such that $S \subseteq B$.

Proof idea:

- If $span(S) = V$, then nothing to prove
- If $span(S) \neq V$, choose a vector $\boldsymbol{v} \notin span(S)$, and form $S_1 = S \cup \{\boldsymbol{v}\}$.

Basis Extension

Theorem

Let V be a finite dimensional vector space and S be a linearly independent subset of vectors from V. Then S can be extended to a basis of V, i.e., there is a basis B for V such that $S \subseteq B$.

Proof idea:

- If $span(S) = V$, then nothing to prove
- If $span(S) \neq V$, choose a vector $\boldsymbol{v} \notin span(S)$, and form $S_1 = S \cup \{\boldsymbol{v}\}$.
- If $span(S_1) = V$, then we are done. Else find a vector outside $span(S_1)$ and add. ... (repeat).

Basis Extension

Theorem

Let V be a finite dimensional vector space and S be a linearly independent subset of vectors from V. Then S can be extended to a basis of V, i.e., there is a basis B for V such that $S \subseteq B$.

Proof idea:

- If $span(S) = V$, then nothing to prove
- If $span(S) \neq V$, choose a vector $\boldsymbol{v} \notin span(S)$, and form $S_1 = S \cup \{\boldsymbol{v}\}$.
- If $span(S_1) = V$, then we are done. Else find a vector outside $span(S_1)$ and add. ... (repeat).
- We will have a basis for V at the end.

Vectors from n-dimensional V.S as n-tuples

Unique representation of vectors using basis vectors

Let V be a n-dimensional vector space with basis $B = \{\boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. Then any vector $\boldsymbol{v} \in V$ can be written as a unique linear combination of the basis vectors

$$\boldsymbol{v} = \sum_{i=1}^{n} \alpha_i \boldsymbol{b_i}.$$

IIIT, HYDERABAD

Vectors from n-dimensional V.S as n-tuples

Unique representation of vectors using basis vectors

Let V be a n-dimensional vector space with basis $B = \{\boldsymbol{b_1}, ..., \boldsymbol{b_n}\}$. Then any vector $\boldsymbol{v} \in V$ can be written as a unique linear combination of the basis vectors

$$\boldsymbol{v} = \sum_{i=1}^{n} \alpha_i \boldsymbol{b_i}.$$

- In terms of the basis B, we can represent $\boldsymbol{v}$ as the n-tuple,

$$[\boldsymbol{v}]_B = (\alpha_1, \alpha_2, ..., \alpha_n).$$

- This is only a representation, and may change with the basis chosen.

IIIT, HYDERABAD

Vectors as coordinates

- Let $V = \mathbb{R}^2$. Let $B = \{\boldsymbol{b_1} = (1,0), \boldsymbol{b_2} = (0,1)\}$.
- Consider a vector $\boldsymbol{v} = (5,6)$.
- $\boldsymbol{v} = 5\boldsymbol{b}_1 + 6\boldsymbol{b}_2$.
- In terms of B, we have

$$[\boldsymbol{v}]_B = \begin{bmatrix} 5 \\ 6 \end{bmatrix}.$$

Change of Basis

How do vector-representations change with change in the basis (from $B = \{\boldsymbol{b_i} : i = 1..n\}$ to $C = \{\boldsymbol{c_i} : i = 1..n\}$) chosen?

$$\text{Given } [\boldsymbol{v}]_B, \text{what is } [\boldsymbol{v}]_C?$$

Change of Basis

How do vector-representations change with change in the basis (from $B = \{\boldsymbol{b_i} : i = 1..n\}$ to $C = \{\boldsymbol{c_i} : i = 1..n\}$) chosen?

Given $[\boldsymbol{v}]_B$, what is $[\boldsymbol{v}]_C$?

- Given $B = \{\boldsymbol{b_i}\}$, we have

$$\boldsymbol{v} = \sum_{i=1}^{n} \alpha_i \boldsymbol{b_i},$$

how to get β_is such that

$$\boldsymbol{v} = \sum_{i=1}^{n} \beta_i \boldsymbol{c_i},$$

i.e. what is $[\boldsymbol{v}]_C$?

Change of Basis

Note that

$$
\begin{aligned}
[\boldsymbol{v}]_C &= \sum_{i=1}^{n} \alpha_i [\boldsymbol{b_i}]_C. \\
&= \begin{bmatrix} [\boldsymbol{b_1}]_C & [\boldsymbol{b_2}]_C & \ldots. & [\boldsymbol{b_n}]_C \end{bmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \\
&= \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}
\end{aligned}
$$

Change of Basis

Note that

$$
\begin{aligned}
[\boldsymbol{v}]_C &= \sum_{i=1}^{n} \alpha_i [\boldsymbol{b_i}]_C. \\
&= \begin{bmatrix} [\boldsymbol{b_1}]_C & [\boldsymbol{b_2}]_C & \dots. & [\boldsymbol{b_n}]_C \end{bmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \\
&= \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}
\end{aligned}
$$

$\begin{bmatrix} [\boldsymbol{b_1}]_C & [\boldsymbol{b_2}]_C & \dots. & [\boldsymbol{b_n}]_C \end{bmatrix}$ is known as the basis change matrix.

Basis change : Example

- Consider the basis $C = \{\boldsymbol{c_1} = (1,0), \boldsymbol{c_2} = (1,1)\}$ for $\mathbb{R}^2$.
- Let $\boldsymbol{v} = (5,6)$. What is $[\boldsymbol{v}]_C$?

Basis change : Example

- Consider the basis $C = \{\boldsymbol{c_1} = (1,0), \boldsymbol{c_2} = (1,1)\}$ for $\mathbb{R}^2$.
- Let $\boldsymbol{v} = (5,6)$. What is $[\boldsymbol{v}]_C$?
- $$\begin{aligned} [\boldsymbol{v}]_C &= 5[\boldsymbol{b}_1]_C + 6[\boldsymbol{b}_2]_C \\ &= 5\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 6\begin{bmatrix} -1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} -1 \\ 6 \end{bmatrix}. \end{aligned}$$
- Check : $\boldsymbol{v} = -1\boldsymbol{c_1} + 6\boldsymbol{c_2}$.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

$\mathcal{L}$=Finite energy signals which are also time-limited from $[0, T]$.

Theorem

A basis for $\mathcal{L}$ is

$$f_i(t) = \frac{1}{\sqrt{T}} e^{j2\pi it/T}, \;\; i = 0, \pm 1, \pm 2, \ldots$$

.

Proof:

- Fourier Series expansion.

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.
2. Span of time-limited sinusoids = Time-limited Finite-Energy signals
   - The sinusoidal basis helps to easily characterize output signal when the signal is passed through 'linear time-invariant' systems.
   - Can think of signals as vectors. Makes Digital Communication possible!

Linear Transformations

- Maps between Vector Spaces (defined over a common field $\mathbb{F}$).
- We like linearity.

Linear Transformation

Let V and W be vector spaces over the field F. A function $T : V \to W$ is a linear transformation if

$$T(c\boldsymbol{v_1} + \boldsymbol{v_2}) = cT(\boldsymbol{v_1}) + T(\boldsymbol{v_2}), \forall \boldsymbol{v_1}, \boldsymbol{v_2} \in V, \text{and}, \forall c \in \mathbb{F}.$$

If $V = W$, then T is called a *linear operator*.

IIIT, HYDERABAD

Linear Tranformation : Examples and Non-Examples

1. T: $R^{2\times 2} \rightarrow R$ where T is defined as
   $T\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) = x_1 + x_4.$

IIIT, HYDERABAD

Linear Tranformation : Examples and Non-Examples

1. T: $R^{2\times 2} \to R$ where T is defined as $T\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) = x_1 + x_4$. **(Yes!)**

2. $T : R^2 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{bmatrix}$.

IIIT, HYDERABAD

Linear Tranformation : Examples and Non-Examples

1. T: $R^{2\times 2} \rightarrow R$ where T is defined as $T\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) = x_1 + x_4$. (**Yes!**)

2. $T : R^2 \rightarrow R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{bmatrix}$.

   (**Yes!**)

3. $T : R^2 \rightarrow R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 x_2 \end{bmatrix}$.

IIIT, HYDERABAD

Linear Tranformation : Examples and Non-Examples

1. T: $R^{2\times 2} \to R$ where T is defined as $T\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) = x_1 + x_4$. (**Yes!**)

2. $T : R^2 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{bmatrix}$.

   (**Yes!**)

3. $T : R^2 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 x_2 \end{bmatrix}$.

   (**No!**)

4. $T : R^3 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ a \end{bmatrix}$.

Linear Tranformation : Examples and Non-Examples

1. T: $R^{2\times 2} \to R$ where T is defined as $T\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\right) = x_1 + x_4$. (**Yes!**)

2. $T : R^2 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{bmatrix}$.

   (**Yes!**)

3. $T : R^2 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 x_2 \end{bmatrix}$.

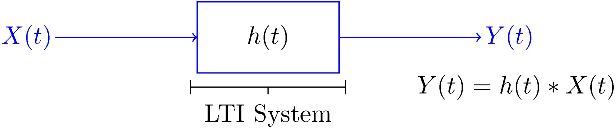
   (**No!**)

4. $T : R^3 \to R^3$ where T is defined as $T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ a \end{bmatrix}$.

   (**No** if $a \neq 0$, **Yes** if $a = 0$)

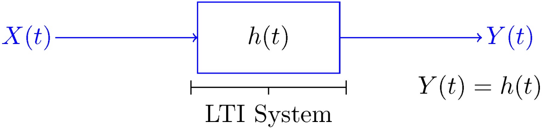
IIIT, HYDERABAD

Linear Transformation : Examples and Non-Examples



- $y(t) = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau$.
- Is this is a linear transformation? (What are its domain and codomain?)

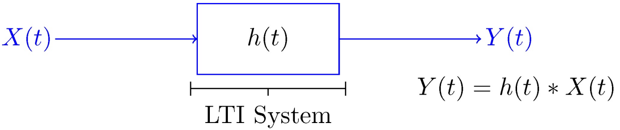
Linear Transformation : Examples and Non-Examples



$$Y(t) = h(t) * X(t)$$

- $y(t) = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau.$
- Is this is a linear transformation? (What are its domain and codomain?)
- Linear Transformation.

Linear Transformation : Examples and Non-Examples



- $y(t) = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau$.
- Is this is a linear transformation? (What are its domain and codomain?)
- Linear Transformation.
- Domain=Codomain=Vector Space of Finite energy signals.

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.
2. Span of time-limited sinusoids = Time-limited Finite-Energy signals.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.
2. Span of time-limited sinusoids $=$ Time-limited Finite-Energy signals.
3. LTI systems are Linear Operators on the Space of Finite Energy Signals.

Sum and Composition of Linear Transformations

- T_1 and T_2 are linear transformations from $V \to W$. Then so is their 'sum' T defined as

$$T(\boldsymbol{v}) = T_1(\boldsymbol{v}) + T_2(\boldsymbol{v}).$$

- So is T' ('composition') defined as

$$T'(\boldsymbol{v}) = T_2(T_1(\boldsymbol{v})).$$

Sum and Composition of Linear Transformations

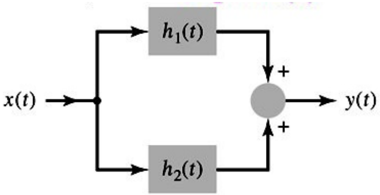
- T_1 and T_2 are linear transformations from $V \to W$. Then so is their 'sum' T defined as

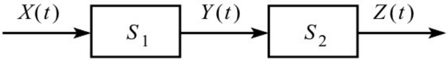
$$T(\boldsymbol{v}) = T_1(\boldsymbol{v}) + T_2(\boldsymbol{v}).$$

- So is T' ('composition') defined as

$$T'(\boldsymbol{v}) = T_2(T_1(\boldsymbol{v})).$$

- Series and Parallel LTI systems.





Range and Null Space of a Linear Transformation

Range (Image) and Null-Space (Kernel) of T

- Range (Image):

$$R(T) = \{\boldsymbol{w} \in W : T(\boldsymbol{v}) = \boldsymbol{w}, \text{for some } \boldsymbol{v} \in V\}.$$

- Nullspace (kernel):

$$N(T) = \{\boldsymbol{v} \in V : T(\boldsymbol{v}) = \boldsymbol{0} \in W\}.$$

Range and Null Space of a Linear Transformation

Range (Image) and Null-Space (Kernel) of T

- Range (Image):

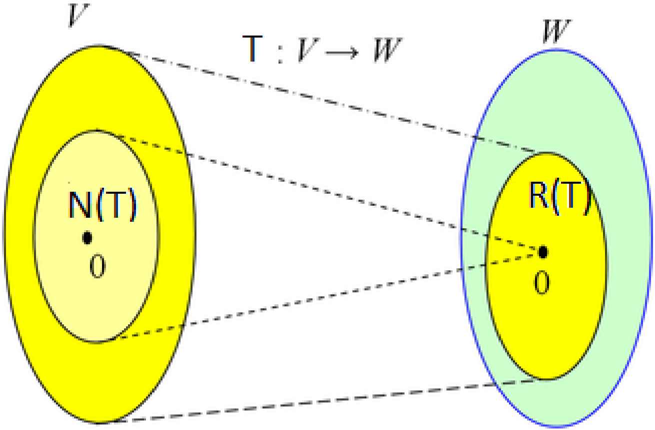
$$R(T) = \{\boldsymbol{w} \in W : T(\boldsymbol{v}) = \boldsymbol{w}, \text{for some } \boldsymbol{v} \in V\}.$$

- Nullspace (kernel):

$$N(T) = \{\boldsymbol{v} \in V : T(\boldsymbol{v}) = \mathbf{0} \in W\}.$$

- $R(T)$ is a subspace of W.
- $N(T)$ is a subspace of V.

Range and Null Space



Rank Nullity Theorem

Rank and Nullity

- $Rank(T) = dim(R(T))$.
- $Nullity(T) = dim(N(T))$.

Rank Nullity Theorem

Let V be a finite dimensional vector space and $T : V \to W$ be a L.T. Then

$$dim(V) = Rank(T) + Nullity(T).$$

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- Let $n = dim(V), k = dim(N(T))$. We want to show that $dim(R(T)) = n - k$.

Proof of Rank Nullity Theorem

- Let $n = dim(V), k = dim(N(T))$. We want to show that $dim(R(T)) = n - k$.
- Let $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}\}$ be basis for $N(T)$.

Proof of Rank Nullity Theorem

- Let $n = dim(V), k = dim(N(T))$. We want to show that $dim(R(T)) = n - k$.
- Let $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}\}$ be basis for $N(T)$.
- We can extend this to a basis $B = \{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}, \boldsymbol{v_{k+1}}, \ldots, \boldsymbol{v_n}\}$ for V.

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- Let $n = dim(V), k = dim(N(T))$. We want to show that $dim(R(T)) = n - k$.
- Let $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}\}$ be basis for $N(T)$.
- We can extend this to a basis $B = \{\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}, \boldsymbol{v_{k+1}}, \ldots, \boldsymbol{v_n}\}$ for V.
- It suffices to show that $\{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ is a basis for $R(T)$.

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- We first show $\{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ are independent. And then have to show that it spans $R(T)$.

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- We first show $\{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ are independent. And then have to show that it spans $R(T)$.
- Suppose not. Then, for some α_is not all zero,

$$\begin{aligned} \mathbf{0} &= \sum_{i=k+1}^{n} \alpha_i T(\boldsymbol{v_{k+i}}) \\ &= T(\sum_{i=k+1}^{n} \alpha_i \boldsymbol{v_i}). \end{aligned}$$

Proof of Rank Nullity Theorem

- We first show $\{T(\mathbf{v_{k+1}}), \ldots, T(\mathbf{v_n})\}$ are independent. And then have to show that it spans $R(T)$.
- Suppose not. Then, for some α_is not all zero,

$$\begin{aligned}\mathbf{0} &= \sum_{i=k+1}^{n} \alpha_i T(\mathbf{v_{k+i}}) \\ &= T(\sum_{i=k+1}^{n} \alpha_i \mathbf{v_i}).\end{aligned}$$

- This means $\sum_{i=1}^{n-k} \alpha_i \mathbf{v_{k+i}} \in N(T)$. Thus,

$$\sum_{i=k+1}^{n} \alpha_i \mathbf{v_i} = \sum_{i=1}^{k} \beta_i \mathbf{v_i}.$$

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- Rearranging,

$$\sum_{i=k+1}^{n} \alpha_i \boldsymbol{v_i} - \sum_{i=1}^{k} \beta_i \boldsymbol{v_i} = \mathbf{0},$$

for α_is not all zero.

Proof of Rank Nullity Theorem

- Rearranging,
$$\sum_{i=k+1}^{n} \alpha_i \boldsymbol{v_i} - \sum_{i=1}^{k} \beta_i \boldsymbol{v_i} = \mathbf{0},$$
for α_is not all zero.
- This is a contradiction as $\{\boldsymbol{v_i} : i = 1, ..., n\}$ is a basis.
- Thus $\{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ is linearly independent.

Proof of Rank Nullity Theorem

- Have to still show $B_R = \{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ spans $R(T)$.

Proof of Rank Nullity Theorem

- Have to still show $B_R = \{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ spans $R(T)$.
- For any vector $\boldsymbol{w} \in R(T)$, show that $\boldsymbol{w} \in span(B_R)$.

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- Have to still show $B_R = \{T(\boldsymbol{v_{k+1}}), \dots, T(\boldsymbol{v_n})\}$ spans $R(T)$.
- For any vector $\boldsymbol{w} \in R(T)$, show that $\boldsymbol{w} \in span(B_R)$.
- There exists a $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \boldsymbol{w}$.

Proof of Rank Nullity Theorem

- Have to still show $B_R = \{T(\boldsymbol{v_{k+1}}), \dots, T(\boldsymbol{v_n})\}$ spans $R(T)$.
- For any vector $\boldsymbol{w} \in R(T)$, show that $\boldsymbol{w} \in span(B_R)$.
- There exists a $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \boldsymbol{w}$.
- We have $\boldsymbol{v} = \sum_{i=1}^{n} \gamma_i \boldsymbol{v_i}$ (as B is a basis for V).

IIIT, HYDERABAD

Proof of Rank Nullity Theorem

- Have to still show $B_R = \{T(\boldsymbol{v_{k+1}}), \ldots, T(\boldsymbol{v_n})\}$ spans $R(T)$.
- For any vector $\boldsymbol{w} \in R(T)$, show that $\boldsymbol{w} \in span(B_R)$.
- There exists a $\boldsymbol{v} \in V$ such that $T(\boldsymbol{v}) = \boldsymbol{w}$.
- We have $\boldsymbol{v} = \sum_{i=1}^{n} \gamma_i \boldsymbol{v_i}$ (as B is a basis for V).
- Apply T on both sides to get the result.

IIIT, HYDERABAD

Example

- Let
$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix}$$
- Consider the linear transformation from $\mathbb{R}^3 \to \mathbb{R}^3$ given by $\boldsymbol{x} \to A\boldsymbol{x}$.
- What is the $N(T)$? What is $R(T)$?
- Check if R-N theorem is satisfied.

IIIT, HYDERABAD

Matrix of a Linear Transformation

Characterising linear transformations

Theorem

Let $T : V \to W$ be a L.T. Let $B = \{\mathbf{v_i} : i = 1.., n\}$. Then the action of T on any arbitrary $\mathbf{v} \in V$ is completely specified by its action on the basis vectors $\{\mathbf{v}_i : i = 1, .., n\}$.

IIIT, HYDERABAD

Matrix of a Linear Transformation

- Let $dim(V) = n, dim(W) = m$. Let $T(\boldsymbol{v}) = \boldsymbol{w}$.

Matrix of a Linear Transformation

- Let $dim(V) = n, dim(W) = m$. Let $T(\boldsymbol{v}) = \boldsymbol{w}$.
- Already know: Choosing a basis B_V for V enables us to write $\boldsymbol{v}$ as a n-tuple $[\boldsymbol{v}]_{B_V}$.

Matrix of a Linear Transformation

- Let $dim(V) = n, dim(W) = m$. Let $T(\boldsymbol{v}) = \boldsymbol{w}$.
- Already know: Choosing a basis B_V for V enables us to write $\boldsymbol{v}$ as a n-tuple $[\boldsymbol{v}]_{B_V}$.
- Choosing a basis B_W for W enables us to write $\boldsymbol{w}$ as a m-tuple $[\boldsymbol{w}]_{B_W}$.

Matrix of a Linear Transformation

- Let $dim(V) = n, dim(W) = m$. Let $T(\boldsymbol{v}) = \boldsymbol{w}$.
- Already know: Choosing a basis B_V for V enables us to write $\boldsymbol{v}$ as a n-tuple $[\boldsymbol{v}]_{B_V}$.
- Choosing a basis B_W for W enables us to write $\boldsymbol{w}$ as a m-tuple $[\boldsymbol{w}]_{B_W}$.
- Fixing B_V and B_W, we have a matrix representation $[T]$ for T.

$$[T][\boldsymbol{v}]_{B_V} = [\boldsymbol{w}]_{B_W}$$

Matrix of a Linear Transformation

- How to get $[T]$?

Matrix of a Linear Transformation

- How to get $[T]$?
- $$i^{th} \text{ column of } [T] = [T(\boldsymbol{v_i})]_{B_W}.$$

Example

- Consider the Lin. Operator on the space of real polynomials of degree upto 2, defined as follows.

$$T(a_0+a_1t+a_2t^2) = (a_0+a_2)+(a_1+a_2)t+(a_0+2a_1+3a_2)t^2.$$

- Find its representation under (a) Basis $B = \{1, t, t^2\}$ (b) Basis $C = (1+t, 1+t^2, 1+t+t^2)$.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

4. Linear Transformations are heavily used in Coding Theory and Cryptography.

Need for Linear Algebra in Communications and Coding

4. Linear Transformations are heavily used in Coding Theory and Cryptography.
    - Embed a low-D subspace in a High-D vector space to a Low-D vector space. (Compression or Source Coding)

Need for Linear Algebra in Communications and Coding

4. Linear Transformations are heavily used in Coding Theory and Cryptography.
    - Embed a low-D subspace in a High-D vector space to a Low-D vector space. (Compression or Source Coding)
    - Embed a low-D vector space as a Low-D subspace of a High-D vector space (Channel Coding).

Eigen values and vectors of a linear operator

Let $T : V \to V$ be a Linear Operator.

Eigen values and vectors

A non-zero $\boldsymbol{v} \in V$ and a constant $\lambda \in \mathbb{F}$ are called the eigen vector and its eigen value of T if

$$T(\boldsymbol{v}) = \lambda \boldsymbol{v}.$$

IIIT, HYDERABAD

Eigen values and vectors of a linear operator

- For certain types of Lin. Operators, there exists a basis $B = \{\boldsymbol{v}_i\}$ for V consisting of eigen vectors (with eigen values λ_is).

Eigen values and vectors of a linear operator

- For certain types of Lin. Operators, there exists a basis $B = \{\boldsymbol{v}_i\}$ for V consisting of eigen vectors (with eigen values λ_is).
- Understanding the I/O relationships of such Lin Operators are easy with such a basis.

IIIT, HYDERABAD

Eigen values and vectors of a linear operator

- For certain types of Lin. Operators, there exists a basis $B = \{\boldsymbol{v}_i\}$ for V consisting of eigen vectors (with eigen values λ_is).
- Understanding the I/O relationships of such Lin Operators are easy with such a basis.
- $$\begin{aligned} T(\boldsymbol{v}) &= T\left(\sum \alpha_i \boldsymbol{v}_i\right) \\ &= \sum \alpha_i T(\boldsymbol{v}_i) \\ &= \sum \alpha_i \lambda_i \boldsymbol{v}_i \end{aligned}$$

Example for Eigen vectors and Values

- $\mathcal{L}$=Finite energy signals which are also time-limited from $[0, T]$.
- A basis for $\mathcal{L}$ is

$$f_i(t) = \frac{1}{\sqrt{T}} e^{j2\pi it/T}, \;\; i = 0, \pm 1, \pm 2, \ldots$$

IIIT, HYDERABAD

Example for Eigen vectors and Values

- $\mathcal{L}$=Finite energy signals which are also time-limited from $[0, T]$.
- A basis for $\mathcal{L}$ is

$$f_i(t) = \frac{1}{\sqrt{T}} e^{j2\pi it/T}, \;\; i = 0, \pm 1, \pm 2, ...$$

- The function $f_i(t)$ are the eigen vectors for any LTI system given by L, with eigen value being the fourier series coefficient of $h(t)$ at $2\pi i/T$.

IIIT, HYDERABAD

Need for Linear Algebra in Communications and Coding

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.
2. Span of time-limited sinusoids = Time-limited Finite-Energy signals.
3. LTI systems are Linear Operators on the Space of Finite Energy Signals.
4. Linear Transformations are heavily used in Coding Theory and Cryptography.

Need for Linear Algebra in Communications and Coding

1. Finite-energy time-bounded signals form a vector space.
2. Span of time-limited sinusoids = Time-limited Finite-Energy signals.
3. LTI systems are Linear Operators on the Space of Finite Energy Signals.
4. Linear Transformations are heavily used in Coding Theory and Cryptography.
5. Fourier basis are also eigen vectors of LTI systems. So understanding I/O relationships of LTI systems is easy.

Thank You

IIIT, HYDERABAD