Reminders

Let $\mathbf{V}$ be a vector space over $\mathbf{F}$, let $v_1, \ldots, v_n \in \mathbf{V}$ be vectors.

Definition

For any $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$, the vector

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$

is a linear combination of $v_1, \ldots, v_n$.

Let $S \subseteq \mathbf{V}$ be a set of vectors.

Definition

The linear span of S (denoted by $\mathrm{span}(S)$) is the set of all linear combinations of elements of S.

We say that S generates a subspace $\mathbf{U}$ if $\mathbf{U} = \mathrm{span}(S)$.

Lemma

Let S be a subset of a vector space $\mathbf{V}$. If $v \in span(S)$, then

$$span(S \cup \{v\}) = span(S).$$

Proof.

If $v \in \text{span}(S)$, then

$$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$

for some $v_1, \ldots, v_n \in S$.
Clearly, $\text{span}(S) \subseteq \text{span}(S \cup \{v\})$. If $x \in \text{span}(S \cup \{v\})$, then w.l.o.g.

$$x = \beta v + \beta_1 v_1 + \ldots + \beta_n v_n.$$

Hence,

$$x = (\beta_1 + \beta\alpha_1)v_1 + \cdots + (\beta_n + \beta\alpha_n)v_n \in \text{span}(S).$$

Spans generating a subspace

$$\begin{aligned}\{(x,y,z) : 3x-3y+z=0\} &= \operatorname{span}(\{(x,y,z) : 3x-3y+z=0\})\\ &= \operatorname{span}((1,1,0),(1,2,3),(3,4,3))\\ &= \operatorname{span}((1,1,0),(1,2,3))\end{aligned}$$

Non-minimality

In

$$\mathrm{span}((1,1,0),(1,2,3),(3,4,3)),$$

the vector $(3,4,3)$ is redundant—a linear combination of other vectors.

$$(3,4,3) = 2(1,1,0) + (1,2,3).$$

Equivalently,

$$(3,4,3) - 2(1,1,0) - (1,2,3) = o.$$

A linear combination

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n \text{ is}$$

- trivial if $\alpha_1 = \ldots = \alpha_n = 0$,
- non-trivial otherwise.

Let $\mathbf{V}$ be a vector space.

Definition

A set $S \subseteq \mathbf{V}$ is linearly independent if no non-trivial linear combination of elements of S is equal to o.

Examples

- The set $\{(1,1,0),(1,2,3),(3,4,3)\}$ in $\mathbf{R}^3$ is not linearly independent, since
$$(3,4,3)-2(1,1,0)-(1,2,3)=o.$$
- The set $\{x^2+x+1, x^2+2x+3, x^2+2.5x+4, x+2\}$ in $\mathcal{P}$ is not linearly independent, since
$$-(x^2+x+1)+3(x^2+2x+3)-2(x^2+2.5x+4)=o.$$
- The set $\{(1,1,0),(1,2,3)\}$ in $\mathbf{R}^3$ is linearly independent.
- If $o \in S$, then S is not linearly independent, since
$$1o=o.$$
- The empty set is linearly independent.

Testing linear independence

Problem

Is $\{(0,1,0,1),(1,0,1,0),(1,2,3,4)\}$ *linearly independent?*

Decide whether there exist $\alpha_1, \alpha_2, \alpha_3 \neq 0,0,0$ such that

$$\alpha_1(0,1,0,1)+\alpha_2(1,0,1,0)+\alpha_3(1,2,3,4)=(0,0,0,0).$$

Equivalently

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 3 \\ 1 & 0 & 4 \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\text{RREF}\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 3 \\ 1 & 0 & 4 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

the only solution is $(\alpha_1, \alpha_2, \alpha_3)=(0,0,0)$. The vectors are linearly independent.

Linear independence and RREF

Lemma

Vectors $a_1, \ldots, a_k \in \mathbf{F}^{n\times 1}$ *are linearly independent if and only if all columns of*

$$RREF(a_1|a_2|\ldots|a_k)$$

are basis columns.

Linear independence and minimality of span

Lemma

A set $S \subseteq \mathbf{V}$ is linearly independent if and only if for every $T \subsetneq S$,

$$span(T) \neq span(S).$$

Proof.

$\Rightarrow$ If $\text{span}(T) = \text{span}(S)$ for some $T \subsetneq S$, then consider $v \in S \setminus T$. Since $v \in S \subseteq \text{span}(S) = \text{span}(T)$, we have

$$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$

for some $v_1, \ldots, v_n \in T$. But

$$\alpha_1 v_1 + \ldots + \alpha_n v_n - v = o$$

contradicts the independence of S.

Linear independence and minimality of span

Lemma

A set $S \subseteq \mathbf{V}$ is linearly independent if and only if for every $T \subsetneq S$,

$$span(T) \neq span(S).$$

Proof.

$\Leftarrow$ Suppose for a contradiction that

$$\alpha_1 v_1 + \ldots + \alpha_n v_n = o$$

for some $v_1, \ldots, v_n \in S$, with $\alpha_1 \neq 0$. Then

$$v_1 = -\alpha_1^{-1}(\alpha_2 v_2 + \ldots + \alpha_n v_n) \in \text{span}(S \setminus \{v_1\}),$$

and thus

$$\text{span}(S \setminus \{v_1\}) = \text{span}(S).$$

Basis

Let $\mathbf{V}$ be a vector space.

Definition

A set $S \subseteq \mathbf{V}$ is a basis if

- S generates $\mathbf{V}$, i.e., $\text{span}(S) = \mathbf{V}$, and
- S is linearly independent.

Example

Each of the following sets

- $\{(1,1,0),(1,2,3)\}$
- $\{(1,1,0),(3,4,3))\}$
- $\{(1,2,3),(3,4,3))\}$

is a basis of the plane $\{(x,y,z) : 3x - 3y + z = 0\}$.

Standard basis

The vectors

$$(1, 0, 0), (0, 1, 0), (0, 0, 1)$$

form a basis of $\mathbf{R}^3$.

More generally, the vectors

$$\begin{aligned} (1, 0, 0, \ldots) &= \left(e_1^{(n)}\right)^T \\ (0, 1, 0, \ldots) &= \left(e_2^{(n)}\right)^T \\ &\ldots \\ (0, 0, \ldots, 0, 1) &= \left(e_n^{(n)}\right)^T \end{aligned}$$

form the standard basis of $\mathbf{R}^n$.

Does every vector space have a basis?

- “It depends.”
- Equivalent to the Axiom of Choice.
- E.g., no constructive way to obtain basis for the space of functions $\mathbf{R} \to \mathbf{R}$.

Basis in a "nice" space

Definition

A vector space $\mathbf{V}$ is countably generated if there exists a (finite or infinite) sequence $v_1, v_2, \ldots \in \mathbf{V}$ such that

$$\mathbf{V} = \operatorname{span}(v_1, v_2, \ldots).$$

All spaces we considered are countably generated, except for

- the space of functions/continuous functions $\mathbf{R} \to \mathbf{R}$
- the space of infinite sequences
- $\mathbf{R}$ as a vector space over $\mathbf{Q}$

Basis in a “nice” space

Lemma

Every countably generated space has a basis.

Proof.

If $\mathbf{V} = \mathrm{span}(v_1, v_2, \ldots)$, let

$$B = \{v_i : v_i \notin \mathrm{span}(v_1, v_2, \ldots, v_{i-1})\}.$$

We have $\mathrm{span}(B) = \mathrm{span}(v_1, v_2, \ldots) = \mathbf{V}$.

If $\alpha_1 v_{i_1} + \ldots + \alpha_k v_{i_k} = o$ for some $v_{i_1}, \ldots, v_{i_k} \in B$, where $\alpha_k \neq 0$ and $i_1 < i_2 < \ldots < i_k$, then

$$v_{i_k} = -\alpha_k^{-1}(\alpha_1 v_{i_1} + \ldots + \alpha_{k-1} v_{i_{k-1}}) \in \mathrm{span}(v_1, \ldots, v_{i_k - 1}),$$

which contradicts the construction of B. $\square$

Transfer lemma

Lemma (Transfer lemma)

Suppose that $S \subset span(T)$ is a linearly independent set. If $span(S) \neq span(T)$, then there exists $v \in T \setminus S$ such that $S \cup \{v\}$ is linearly independent.

Proof.

Since $\text{span}(S) \neq \text{span}(T)$, there exists $v \in T \setminus \text{span}(S)$. Suppose that

$$\alpha v + \alpha_1 v_1 + \ldots + \alpha_n v_n = o$$

for some $v_1, \ldots, v_n \in S$. If $\alpha \neq 0$, then

$$v = -\alpha^{-1}(\alpha_1 v_1 + \ldots + \alpha_n v_n) \in \text{span}(S), \text{ a contradiction.}$$

Hence $\alpha = 0$, and since S is linearly independent, $\alpha_1 = \ldots = \alpha_n = 0$. Therefore, $S \cup \{v\}$ is linearly independent. □

Extension to basis

Corollary (Extension lemma)

If a vector space $\mathbf{V}$ *has a finite basis* B*, then every independent set is a subset of some basis.*

Proof.

Let S be an independent set. Keep adding elements of B to S by the Transfer lemma until S becomes generating. $\square$

Exchange lemma

Corollary (Exchange lemma)

Let $S \subset \mathrm{span}(T)$ be a linearly independent set. For every $s \in S \setminus T$ there exists $t \in T \setminus S$ such that

$$(S \setminus \{s\}) \cup \{t\}$$

is linearly independent.

Proof.

Since S is linearly independent,

$$\mathrm{span}(S \setminus \{s\}) \subsetneq \mathrm{span}(S) \subseteq \mathrm{span}(T).$$

By the Transfer Lemma, there exists $t \in T \setminus S$ such that $(S \setminus \{s\}) \cup \{t\}$ is linearly independent. $\square$

Generating and independent sets

Lemma (Generating-independent inequality)

Suppose that S and T are sets of vectors, where T is finite. If $S \subseteq span(T)$ is linearly independent, then S is finite and $|S| \leq |T|$.

Proof.

- Using the Exchange lemma, replace elements of $S \setminus T$ by elements of $T \setminus S$ in S as long as possible (at most $|T|\times$).
- In the end, $S \subseteq T$, and thus $|S| \leq |T|$.

$\square$

Sizes of bases

Lemma

If a vector space $\mathbf{V}$ *has a finite basis, then all its bases are finite and have the same size.*

Proof.

Let B_1 and B_2 be two bases of $\mathbf{V}$, where B_1 is finite.

- $\text{span}(B_1) = \mathbf{V}$ and $B_2 \subseteq \mathbf{V}$ is linearly independent.
- By the Generating-independent inequality, $|B_2| \leq |B_1|$.
- Symmetrically, $|B_1| \leq |B_2|$.

$\square$

Definition

The dimension $\dim(\mathbf{V})$ of a vector space is the size of its basis.

Examples

- $\mathbf{R}^n$ has dimension n.
- $\mathbf{R}^{n \times m}$ has dimension nm.
- Complex numbers as a vector space over $\mathbf{R}$ have dimension 2.
- The space of polynomials has infinite dimension.
- The space of polynomials of degree at most n has dimension $n + 1$.
- The trivial space $\{o\}$ has dimension 0.

Dimension, independent and generating sets

Lemma

Let $\mathbf{V}$ be a vector space of a finite dimension n.

- *Every independent set in $\mathbf{V}$ has size at most n, and all independent sets of size n are bases.*
- *Every set that generates $\mathbf{V}$ has size at least n, and all generating sets of size n are bases.*

Proof.

Let S be independent, G generating.

- $|S| \leq n \leq |G|$ by the Generating-independent inequality.
- If $|S| = n$, then no proper superset of S is independent.
- By the Transfer lemma, $\text{span}(S) = \mathbf{V}$.

$\square$

Dimension, independent and generating sets

Lemma

Let $\mathbf{V}$ be a vector space of a finite dimension n.

- *Every independent set in $\mathbf{V}$ has size at most n, and all independent sets of size n are bases.*
- *Every set that generates $\mathbf{V}$ has size at least n, and all generating sets of size n are bases.*

Proof.

Let S be independent, G generating.

- $|S| \leq n \leq |G|$ by the Generating-independent inequality.
- If $|G| = n$, then no proper subset of G is generating.
- Hence, $\text{span}(A) \neq \text{span}(G)$ for every $A \subsetneq G$.
- Implies that G is linearly independent.

□

Dimension and subspaces

Lemma

Suppose that $\mathbf{V}$ *has finite dimension, and* $\mathbf{U} \Subset \mathbf{V}$*.*

- $\dim(\mathbf{U}) \leq \dim(\mathbf{V})$
- *If* $\dim(\mathbf{U}) = \dim(\mathbf{V})$*, then* $\mathbf{U} = \mathbf{V}$*.*

Proof.

- Let B_U be a basis of $\mathbf{U}$.
- By the Extension lemma, we have a basis $B_V \supseteq B_U$ of $\mathbf{V}$.
- $\dim(\mathbf{U}) = |B_U| \leq |B_V| = \dim(\mathbf{V})$
- If $\dim(\mathbf{U}) = \dim(\mathbf{V})$, then $B_U = B_V$ and

$$\mathbf{U} = \operatorname{span}(B_U) = \operatorname{span}(B_V) = \mathbf{V}.$$

$\square$

Example: Dimension and subspaces

Subspaces of $\mathbf{R}^3$:

- Dimension 3: $\mathbf{R}^3$
- Dimension 2: spans of 2 independent vectors = planes containing $(0,0,0)$.
- Dimension 1: spans of vectors = lines containing $(0,0,0)$.
- Dimension 0: $\{(0,0,0)\}$

Example: bases of polynomials

$\mathcal{P}_n$ has dimension $n+1$

- Basis $1, x, x^2, \ldots, x^n$.

Lagrange polynomials

Let $a_0, \ldots, a_n \in \mathbf{R}$ be pairwise distinct.

- For $k = 0, \ldots, n$, let

$$p_k(x) = \frac{(x - a_0) \cdots (x - a_{k-1})(x - a_{k+1}) \cdots (x - a_n)}{(a_k - a_0) \cdots (a_k - a_{k-1})(a_k - a_{k+1}) \cdots (a_k - a_n)}.$$

- We have $p_k(a_i) = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$
- The set $B = \{p_0, \ldots, p_n\}$ is another basis of $\mathcal{P}_n$.
    - $|B| = \dim(\mathcal{P}_n)$
    - B is linearly independent:

$$(\alpha_0 p_0 + \ldots + \alpha_n p_n)(a_i) = \alpha_0 p_0(a_i) + \ldots + \alpha_n p_n(a_i) = \alpha_i,$$

      hence if $\alpha_0 p_0 + \ldots + \alpha_n p_n = o$, then $\alpha_i = o(a_i) = 0$ for $i = 0, \ldots, n$.

Polynomial interpolation

Corollary (Polynomial interpolation lemma)

A polynomial p of degree at most n is uniquely determined by its values in $n+1$ distinct points.

Proof.

- Since B generates $\mathcal{P}_n$, there exist $\alpha_0, \ldots, \alpha_n \in \mathbf{R}$ such that

$$p = \alpha_0 p_0 + \ldots + \alpha_n p_n.$$

- For $i = 0, \ldots, n$,

$$p(a_i) = \alpha_0 p_0(a_i) + \ldots + \alpha_n p_n(a_i) = \alpha_i.$$

- Therefore,

$$p = p(a_0)p_0 + \ldots + p(a_n)p_n$$

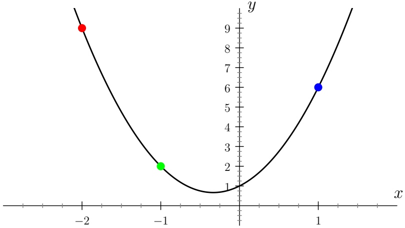
  is uniquely determined by the values of p in $a_0, \ldots, a_n$.

Example

Problem

Find the equation of a quadratic function through points

$$(-2, 9),\ (-1, 2),\ \textit{and}\ (1, 6)$$



$$9\frac{(x+1)(x-1)}{(-2+1)(-2-1)} + 2\frac{(x+2)(x-1)}{(-1+2)(-1-1)} + 6\frac{(x+2)(x+1)}{(1+2)(1+1)}$$

$$= 3x^2 + 2x + 1$$

Vandermonde matrix

Definition

For distinct real numbers $a_0, \ldots, a_n$,

$$V^{(a_0,\ldots,a_n)} = \begin{pmatrix} 1 & a_0 & a_0^2 & \ldots & a_0^n \\ 1 & a_1 & a_1^2 & \ldots & a_1^n \\ & & \ldots & & \\ 1 & a_n & a_n^2 & \ldots & a_n^n \end{pmatrix},$$

is a Vandermonde matrix.

For any polynomial $p(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n$,

$$V^{(a_0,\ldots,a_n)} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \ldots \\ \beta_n \end{pmatrix} = \begin{pmatrix} p(a_0) \\ p(a_1) \\ \ldots \\ p(a_n) \end{pmatrix}$$

Vandermonde matrix and polynomial interpolation

For $b_0, \ldots, b_n$, if a polynomial

$$p(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n$$

satisfies $p(a_0) = b_0$, $p(a_1) = b_1, \ldots, p(a_n) = b_n$, then

$$V^{(a_0,\ldots,a_n)} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \ldots \\ \beta_n \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ \ldots \\ b_n \end{pmatrix}$$

By the Polynomial interpolation lemma, this system always has a solution,

$$\beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n = b_0 p_0(x) + b_1 p_1(x) + \ldots + b_n p_n(x).$$

Corollary

Every Vandermonde matrix is regular.

Problem

Describe all infinite sequences $a_0, a_1, \ldots$ that satisfy

$$a_{n+2} = 5a_{n+1} - 6a_n \text{ for every } n \geq 0. \tag{1}$$

Let $\mathcal{S}$ be the vector space of infinite sequences, and let $U \subseteq \mathcal{S}$ consist of those satisfying (1). Then U is a subspace:

- $(0, 0, \ldots) \in U$
- If $A = (\alpha_0, \alpha_1, \ldots) \in U$ and $B = (\beta_0, \beta_1, \ldots) \in U$, and $\gamma \in \mathbf{R}$, then

$$\begin{aligned} \alpha_{n+2} + \beta_{n+2} &= 5(\alpha_{n+1} + \beta_{n+1}) - 6(\alpha_n + \beta_n) \\ \gamma\alpha_{n+2} &= 5\gamma\alpha_{n+1} - 6\gamma\alpha_n, \end{aligned}$$

  and thus $A + B, \gamma A \in U$.

Linear recurrences

Problem

Describe all infinite sequences $a_0, a_1, \dots$ that satisfy

$$a_{n+2} = 5a_{n+1} - 6a_n \text{ for every } n \geq 0. \tag{1}$$

The choice of a_0 and a_1 uniquely determines the rest of the sequence. Hence, $\dim(U) = 2$. "Standard" basis:

- $a_0 = 0, a_1 = 1 \to (0, 1, 5, 19, 65, \dots)$
- $a_0 = 1, a_1 = 0 \to (1, 0, -6, -30, -114, \dots)$

Linear recurrences

Problem

Describe all infinite sequences $a_0, a_1, \ldots$ that satisfy

$$a_{n+2} = 5a_{n+1} - 6a_n \text{ for every } n \geq 0. \tag{1}$$

Nicer basis:

- $a_n = 2^n \to (1, 2, 4, 8, 16, \ldots)$
- $a_n = 3^n \to (1, 3, 9, 27, 81, \ldots)$

$$2^{n+2} = 4 \cdot 2^n = 10 \cdot 2^n - 6 \cdot 2^n = 5 \cdot 2^{n+1} - 6 \cdot 2^n$$
$$3^{n+2} = 9 \cdot 3^n = 15 \cdot 3^n - 6 \cdot 3^n = 5 \cdot 3^{n+1} - 6 \cdot 3^n$$

Therefore, for $\alpha, \beta \in \mathbf{R}$, $a_n = \alpha 2^n + \beta 3^n$ is a solution, and no other solutions exist.