Linear Algebra

Lecture Notes

Rostyslav Hryniv

Ukrainian Catholic University
Business Analytics and Computer Science Programmes

4th term
Spring 2020

Lecture 5. Bases

Outline

Outline

Definition (Basis of a vector space)

A set S of vectors in a vector space V is called a basis of V if
(a) S is linearly independent; (b) S spans V

Example

- The standard vectors $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n$ form a basis in $\mathbb{R}^n$
- The functions $1, x, x^2, \dots, x^n$ form a basis of $\mathcal{P}_n$
- Matrices M_{ij} (1 on ij^{th} place and zeros otherwise) form a basis of $M_{m\times n}(\mathbb{R})$

Example (Another basis for $\mathbb{R}^3$)

$\mathbf{v}_1 = (1,2,0)^\top$, $\mathbf{v}_2 = (2,1,0)^\top$, $\mathbf{v}_3 = (1,1,1)^\top$ form a basis of $\mathbb{R}^3$.

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 = \mathbf{b} \iff \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

3×3 matrix is nonsingular $\implies$ solutions for all $\mathbf{b}$;
only trivial solution for $\mathbf{b} = \mathbf{0}$

Further examples of bases in linear spaces

Any linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ in $\mathbb{R}^n$ form its basis

Need to show: $\mathbf{v}_1, \dots, \mathbf{v}_n$ span $\mathbb{R}^n$

$$c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{b} \iff [\mathbf{v}_1 \ \dots \mathbf{v}_n]\mathbf{c} = \mathbf{b}$$

The matrix $A = [\mathbf{v}_1 \cdots \mathbf{v}_n]$ is nonsingular $\implies C(A) = \mathbb{R}^n$

Lemma

If $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a basis of a vector space V, then any $\mathbf{x} \in V$ has a unique representation $\mathbf{x} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$.

Proof.

$$\mathbf{x} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = c_1'\mathbf{v}_1 + \cdots + c_n'\mathbf{v}_n$$

yields $$\mathbf{0} = (c_1 - c_1')\mathbf{v}_1 + \dots (c_n - c_n')\mathbf{v}_n \implies c_j = c_j'$$ □

Definition (Coordinates of $\mathbf{x}$ in the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$)

The above c_j are the coordinates of $\mathbf{x}$ in the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$, and $(c_1, \dots, c_n)$ is the corresponding coordinate vector

Outline

Dimension of a space

Definition

A vector space V is called finite-dimensional if it possesses a finite basis; otherwise, V is infinite-dimensional

Example

$\mathcal{P}_\infty$ is infinite-dimensional.

Theorem

Any two bases of a finite-dimensional ***l.v.s.*** *have the same number of elements*

Proof by contradiction:

Assume $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is a basis of V and $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subset V$, with $m > n$
We show $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly dependent,

i.e., that $\sum_j c_j \mathbf{v}_j = \mathbf{0}$ for a nontrivial $\mathbf{c} = (c_1, \ldots, c_m)$:

- write $\mathbf{v}_j = \sum_k a_{jk} \mathbf{u}_k$ and form $A = (a_{jk})_{m \times n}$; then
- $\sum_j c_j \mathbf{v}_j = \sum_j c_j \sum_k a_{jk} \mathbf{u}_k = \sum_k (\sum_j c_j a_{jk}) \mathbf{u}_k = \sum_k (\mathbf{c}A)_k \mathbf{u}_k$
- can fulfil $\mathbf{c}A = \mathbf{0}$ for a nonzero $\mathbf{c}$! why?

Dimension of a vector space

Definition

The number of elements in any basis of a finite-dimensional vector space V is called the dimension of the space V and is denoted $\dim V$

Example (Dimension of some spaces)

- $\mathbb{R}^n$ is of dimension n
- $M_{m\times n}(\mathbb{R})$ is of dimension $m \cdot n$
- $\mathcal{P}_n$ is of dimension $n+1$ (why not n?!)
- the space of diagonal $n \times n$ matrices is of dimension n
- U_n upper-triangular $n \times n$ matrices; $\dim U_n = n(n+1)/2$

Theorem (Sufficient conditions for a basis)

Assume V is an n-dim. ***l.v.s.*** *and $S \subset V$ has n elements. Then TFAE:*
(a) S is a basis of V; (b) S is linearly independent; (c) $\mathrm{ls}(S) = V$

(b) $\implies$ (c): if $\mathrm{ls}(S) \neq V$, can enlarge S keeping linear independence
(c) $\implies$ (b): if S were lin. dependent, $\exists$ a proper $S' \subset S$ s.t. $\mathrm{ls}(S') = V$

Warning on dimensions

Remark

Dimension of a ***l.v.s.*** *depends on the field of scalars ($\mathbb{R}$ or $\mathbb{C}$)*

Example

Let V be a **l.v.s.** $M_{2\times 2}(\mathbb{C})$ of 2×2 matrices with complex entries. Then

- $\dim V = 4$ if the field of constants is $\mathbb{C}$
- $\dim V = 8$ if the field of constants is $\mathbb{R}$

What are the corresponding bases in each case?

Example (Quantum computers and Pauli matrices)

In quantum computation, 2×2 Hermitian matrices are of importance. These are $A \in M_{2\times 2}(\mathbb{C})$ satisfying $A = A^* := \overline{A^\top}$, ie, $a_{jk} = \overline{a_{kj}}$. Hermitian matrices form a 4-dim subspace of $M_{2\times 2}(\mathbb{C})$ over $\mathbb{R}$; the Pauli matrices $\sigma_1, \sigma_2, \sigma_3$ along the identity I_2 form a basis:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Outline

Four subspaces of a matrix

Any $m \times n$ matrix $A = (a_{ij})_{m\times n}$ is composed of

- m row vectors $\begin{cases} \mathbf{r}_1 = (a_{11}, a_{12}, \dots, a_{1n}) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \mathbf{r}_m = (a_{m1}, a_{m2}, \dots, a_{mn}) \end{cases}$
- n column vectors $\mathbf{c}_1 = \begin{pmatrix} a_{11} \\ \dots \\ a_{m1} \end{pmatrix}, \dots, \mathbf{c}_n = \begin{pmatrix} a_{1n} \\ \dots \\ a_{mn} \end{pmatrix}$

Definition

- Column space $C(A)$ of A is the linear span of $\mathbf{c}_1, \dots, \mathbf{c}_n$; $C(A) \subset \mathbb{R}^m$
- Row space $R(A)$ of A is the linear span of $\mathbf{r}_1, \dots, \mathbf{r}_m$; coincides with $C(A^\top) \subset \mathbb{R}^n$
- Nullspace $N(A)$ of A is the solution set of $A\mathbf{x} = \mathbf{0}$; $N(A) \subset \mathbb{R}^n$
- Left nullspace $N(A^T)$ of A is the solution set of $\mathbf{y}^\top A = \mathbf{0}$; $N(A^T) \subset \mathbb{R}^m$

Dimensions of the four subspaces

Theorem (Dimensions of the four subspaces)

(i) *Dimension of the row space of A is equal to* $\operatorname{rank}(A)$

(ii) *Dimension of the nullspace (the nullity) of A is equal to* $n - \operatorname{rank}(A)$

(iii) *Dimension of the column space of A is equal to* $\operatorname{rank}(A)$

(iv) *Dimension of the left nullspace of A is equal to* $m - \operatorname{rank}(A)$

Proof.

- Reduce A to the row echelon form U using the elementary row transformations
- Each row of U is a linear combination of $\mathbf{r}_1(A), \ldots, \mathbf{r}_m(A)$
- Each row of A is a linear combination of $\mathbf{r}_1(U), \ldots, \mathbf{r}_m(U)$
- $\implies \operatorname{ls}\{\mathbf{r}_1(A), \ldots, \mathbf{r}_m(A)\} = \operatorname{ls}\{\mathbf{r}_1(U), \ldots, \mathbf{r}_m(U)\}$
- $\implies$ are both of dimension $\operatorname{rank}(A)$
- $N(A) = N(U)$; the latter has dimension $n - \operatorname{rank}(A)$ $\square$

Dimensions of the four subspaces

Example

$$U = \begin{pmatrix} 1 & -2 & 5 & 0 & 3 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- The row space of U is spanned by $\mathbf{r}_1(U), \mathbf{r}_2(U), \mathbf{r}_3(U)$
- x_1, x_2, x_4 are pivot variables, x_3 and x_5 are free variables
- The solution set of $U\mathbf{x} = \mathbf{0}$ has parameters x_3 and x_5:
- $x_3 = 1$ and $x_5 = 0 \implies$ solution $\mathbf{v}_1 = (-11, -3, 1, 0, 0)$
- $x_3 = 0$ and $x_5 = 1 \implies$ solution $\mathbf{v}_2 = (-3, 0, 0, -2, 1)$
- a general solution is given by $\mathbf{x} = s\mathbf{v}_1 + t\mathbf{v}_2$; corresponds to $x_3 = s$ and $x_5 = t$

Dimensions of the four subspaces

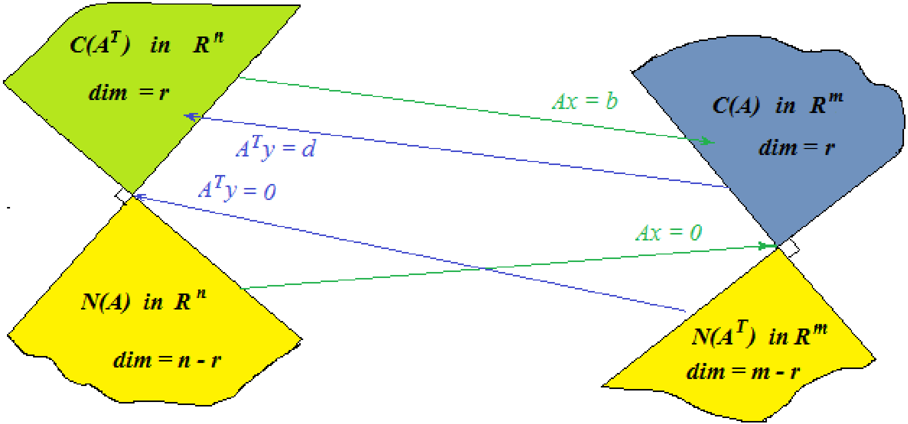
Proof (continued).

- transformation $A \sim U$ is made using the elementary row transformations $\implies \exists$ nonsingular B s.t. $BA = U$
- (usually $B = L^{-1}$ or $B = L^{-1}P$ from the LU-factorization)
- the column space $C(U)$ of U is spanned by the columns with pivots only; thus $C(U)$ is of dimension $\mathrm{rank}(A)$
- observe: $\mathbf{c}_j(U) = B\mathbf{c}_j(A)$, so that

$$k_1\mathbf{c}_1(A) + \cdots + k_n\mathbf{c}_n(A) = \mathbf{0} \iff k_1\mathbf{c}_1(U) + \cdots + k_n\mathbf{c}_n(U) = \mathbf{0}$$

- thus $C(A)$ and $C(U) = BC(A)$ are of the same dimension $\mathrm{rank}(A)$
- now $\dim(N(A^\top)) = m - \dim(C(A^\top)) = m - \mathrm{rank}(A)$ by (ii) $\square$

Dimensions of the four subspaces



Hamming error-correcting codes

Task: create auto-correcting encoding system, i.e.,

System able to detect and auto-correct errors in the received signals

1. **Input**: 4-bit message $\mathbf{p}$ over the field $GF(2)$
2. $\mathbf{p}$ encoded into the codeword $\mathbf{c} = G\mathbf{p}$; G is the 7×4 generator
3. $\mathbf{c}$ sent through noisy channel and received as $\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}$
4. error-detection and correction using the check vector $H\tilde{\mathbf{c}}$

The generator matrix G and check matrix H are given by

$$G^\top = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Question: Why and how this works?

- $\mathbf{c} \in C(G)$ but $C(G) \subset N(H)$, so that $H\tilde{\mathbf{c}} = H\mathbf{c} + H\mathbf{e} = H\mathbf{e}$
- $H\mathbf{e}$ shows in which of 7 positions (if any) $\mathbf{e}$ has 1 and recovers $\mathbf{c}$
- $\mathbf{p}$ uniquely recovered from $\mathbf{c}$: the columns of G form a basis of $C(G)$

Outline

1. Bases in vector spaces
   - Examples and Definition
   - Dimension
2. Four subspaces and rank of a matrix
   - Four subspaces
   - Rank of a matrix
3. Coordinates and change of basis
   - Coordinate maps
   - Change of basis

Rank of a matrix

Definition

Rank of a matrix A is the dimension of its column (or row) space

Properties of rank

- For an $m \times n$ matrix A, $\operatorname{rank}(A)$ equals $\dim \operatorname{range}(A)$
  Indeed, $\operatorname{range}(A) := \{A\mathbf{x} \mid \mathbf{x} \in \mathbb{R}^n\}$ is just the column space of A
- for an $n \times k$ matrix B, $\operatorname{rank}(AB) \leq \operatorname{rank}(A)$
  Follows from the fact that the range of AB is contained in that of A
- for an $k \times m$ matrix C, $\operatorname{rank}(CA) \leq \operatorname{rank}(A)$
  Reason: the row space of CA is contained in that of A
- for a non-singular B of size n, the ranks of A and AB coincide
  Reason: the ranges (column spaces) of A and AB are the same
- for a non-singular C of size m, the ranks of A and CA coincide
  Reason: the row spaces of A and AB are the same: $A = (AB)B^{-1}$

Outline

Coordinate map

- Fix a basis $S = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ of a vector space V
- every $\mathbf{x} \in V$ gets its unique coordinates $(c_1, c_2, \dots, c_n)$ in basis S:

$$\mathbf{x} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \dots + c_n\mathbf{v}_n$$

Definition (Coordinate map $T_S : V \to \mathbb{R}^n$)

$$T_S \,:\, \mathbf{x} \mapsto (c_1, c_2, \dots, c_n)^\top \in \mathbb{R}^n$$

is called the coordinate map of V in the basis S

Definition (Linear maps and isomorphisms)

Let V and W be linear vector spaces. A mapping $T : V \to W$ is

- linear if for all $\mathbf{x}, \mathbf{y} \in V$ and all $a, b \in \mathbb{R}$

$$\boxed{T(a\mathbf{x} + b\mathbf{y}) = aT(\mathbf{x}) + bT(\mathbf{y})}$$

- an isomorphism of V and W if it is linear, one-to-one, and onto

Definition (Isomorphic linear vector spaces)

Two linear vector spaces V and W are said to be isomorphic if there is an isomorphism $T : V \to W$

Isomorphism to $\mathbb{R}^n$

Lemma (Properties of T_S)

T_S is an isomorphism between V and $\mathbb{R}^n$

Proof.

T_S is one-to-one:

$$T_S(\mathbf{x}) = \mathbf{c} \qquad \Longleftrightarrow \qquad \mathbf{x} = \sum_j c_j \mathbf{v}_j$$

T_S is onto:

$$T_S^{-1}\mathbf{c} = \sum_j c_j \mathbf{v}_j \quad \text{is well defined}$$

T_S is linear:

$$\mathbf{x} = \sum_j c_j \mathbf{v}_j,\ \mathbf{y} = \sum_j d_j \mathbf{v}_j \implies a\mathbf{x} + b\mathbf{y} = \sum_j (ac_j + bd_j)\mathbf{v}_j \qquad \square$$

Corollary

Any two vector spaces of the same dimension are isomorphic

Corollary

Up to isomorphism, $\mathbb{R}^n$ is the only n-dimensional vector space

Example

- $S = \left(\mathbf{v}_1 = (1,2,0)^\top, \mathbf{v}_2 = (1,2,0)^\top, \mathbf{v}_3 = (1,1,1)^\top\right)$
- $T_S\mathbf{x} = \mathbf{c} \iff \mathbf{x} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 \iff$

$$\underbrace{\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{P_{S\to S'}} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

- x_1, x_2, x_3 are coordinates of $\mathbf{x}$ in the basis $S' = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$
  c_1, c_2, c_3 are coordinates of $\mathbf{x}$ in the basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$
- $(1,2,0)^\top, (2,1,0)^\top, (1,1,1)^\top$ are coordinate vectors of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ in the basis $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$
- $\mathbf{c} \mapsto \mathbf{x}$ amounts to matrix multiplication by $P_{S\to S'}$
- $\mathbf{x} \mapsto \mathbf{c}$ amounts to matrix multiplication by

$$P_{S'\to S} = (P_{S\to S'})^{-1}$$

Outline

Change of basis

- Assume $\mathbf{x}$ has coordinate vector $\mathbf{c} = T_S(\mathbf{x})$ in basis $S = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$
- Take another basis $S' = (\mathbf{v}'_1, \mathbf{v}'_2, \ldots, \mathbf{v}'_n)$; how can one calculate $\mathbf{c}' = T_{S'}(\mathbf{x})$?

Theorem (Change of basis)

$$\boxed{\mathbf{c}' = P_{S \to S'} \mathbf{c}}$$

where the transition matrix $P_{S \to S'}$ has columns equal to $T_{S'}(\mathbf{v}_1)$, $T_{S'}(\mathbf{v}_2), \ldots, T_{S'}(\mathbf{v}_n)$ respectively

Proof.

$$\mathbf{c}' := T_{S'}(\mathbf{x}) = T_{S'}\left(\sum_k c_k \mathbf{v}_k\right) = \sum_k c_k T_{S'}(\mathbf{v}_k) = P_{S \to S'} \mathbf{c}$$

□

Computing the transition matrices in $\mathbb{R}^n$

- We have an "old" basis $S = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$
  and a "new" basis $S' = (\mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_n)$
- Form matrix B whose columns are vector coordinates of $\mathbf{v}_k$ (in the standard basis $S_0 = (\mathbf{e}_1, \dots, \mathbf{e}_n)$)
- Form matrix B' whose columns are vector coordinates of $\mathbf{v}'_k$ (in the standard basis $S_0 = (\mathbf{e}_1, \dots, \mathbf{e}_n)$)
- Use elementary row transformations to get

$$(B' \mid B) \sim (I_n \mid P_{S \to S'})$$

- mnemonic rule:

$$\boxed{(\text{“new basis”} \mid \text{“old basis”}) \sim (I_n \mid P_{S \to S'})}$$

- the reason: $B' = P_{S' \to S_0}$, so that

$$(B')^{-1} B = (P_{S' \to S_0})^{-1} P_{S \to S_0} = P_{S_0 \to S'} P_{S \to S_0} = P_{S \to S'}$$

Example in $\mathbb{R}^2$

- Old basis S: $\mathbf{v}_1 = (1,1)^\top$, $\mathbf{v}_2 = (1,-1)^\top$
- new basis S': $\mathbf{v}'_1 = (1,2)^\top$, $\mathbf{v}'_2 = (2,-1)^\top$
- find the transition matrix $P_{S \to S'}$:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 1 \\ 2 & -1 & 1 & -1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & \frac{3}{5} & -\frac{1}{5} \\ 0 & 1 & \frac{1}{5} & \frac{3}{5} \end{array}\right)$$

- enough to check for $\mathbf{v}_1 \sim (1,0)^\top_S$ and $\mathbf{v}_2 \sim (0,1)^\top_S$:

$$T_S(\mathbf{v}_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \qquad T_{S'}(\mathbf{v}_1) = P_{S \to S'} T_S(\mathbf{v}_1) = \begin{pmatrix} \frac{3}{5} \\ \frac{1}{5} \end{pmatrix}$$

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{3}{5}\mathbf{v}'_1 + \frac{1}{5}\mathbf{v}'_2 = \frac{3}{5}\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \frac{1}{5}\begin{pmatrix} 2 \\ -1 \end{pmatrix}$$