

Quick Reference of Linear Algebra

Hao Zhang

National Key Laboratory for Novel Software Technology, Nanjing University, China

zhangh0214@gmail.com

Abstract

In linear algebra, concepts are much more important than computations. Computers can do the calculations, but you have to choose the calculations and interpret the results. The heart of linear algebra is the linear combination of vectors.

In this note, we give a quick reference of some of the key concepts and applications of linear algebra. The section of inner product spaces is omitted, since it rarely appear in computer science. Please refer to [1] if you are interested in. For further reading, you may consult [3, 4, 5, 6, 7, 8, 9].

1 Introduction: Vectors and Matrices

1.1 Vector and Matrix Norms

Definition 1 (ℓ_p -norm $\|\mathbf{x}\|_p$). $\|\mathbf{x}\|_p := (\sum_i |x_i|^p)^{\frac{1}{p}}$. In particular,

- $\|\mathbf{x}\|_0 := \sum_i \mathbb{I}(x_i \neq 0)$.
- $\|\mathbf{x}\|_1 := \sum_i |x_i|$.
- $\|\mathbf{x}\|_2 := \sqrt{\sum_i x_i^2} = \sqrt{\mathbf{x}^\top \mathbf{x}}$
- $\|\mathbf{x}\|_\infty := \max_i |x_i|$.

Definition 2 (Mahalanobis Distance). Given a set of instances $\{\mathbf{x}_i\}_{i=1}^m$ with empirical mean $\boldsymbol{\mu} \in \mathbb{R}^d$ and empirical covariance $\boldsymbol{\Sigma} \in \mathbb{R}^{d \times d}$, then the Mahalanobis distance of \mathbf{x} is defined as

$$\sqrt{(\mathbf{x} - \boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1} (\mathbf{x} - \boldsymbol{\mu})} = \left\| \boldsymbol{\Lambda}^{-\frac{1}{2}} \mathbf{Q}^\top (\mathbf{x} - \boldsymbol{\mu}) \right\|, \quad (1)$$

where $\boldsymbol{\Sigma} = \mathbf{Q} \boldsymbol{\Lambda} \mathbf{Q}^\top$.

Definition 3 (Matrix Norm). $\|\mathbf{A}\|_p := \max_{\mathbf{x} \neq \mathbf{0}} \frac{\|\mathbf{A}\mathbf{x}\|_p}{\|\mathbf{x}\|_p}$. In particular,

- $\|\mathbf{A}\|_1 := \max_j \sum_{i=1}^m |a_{ij}|$.
- $\|\mathbf{A}\|_\infty := \max_i \sum_{j=1}^m |a_{ij}|$.
- $\|\mathbf{A}\|_* := \|\boldsymbol{\sigma}\|_1 = \sum_{i=1}^r \sigma_i$.

- $\|\mathbf{A}\|_2 := \|\boldsymbol{\sigma}\|_\infty = \max_i \sigma_i$.
 - $\|\mathbf{A}\|_F := \|\boldsymbol{\sigma}\|_2 = \sqrt{\text{tr } \mathbf{A}^\top \mathbf{A}} = \sqrt{\text{tr } \mathbf{A} \mathbf{A}^\top} = \|\text{vec } \mathbf{A}\|_2$.
- In which $\mathbf{A} = \mathbf{U} \boldsymbol{\Sigma} \mathbf{V}^\top$.

Lemma 1 (Cosine Formula). If $\mathbf{u} \neq \mathbf{0}, \mathbf{v} \neq \mathbf{0}$, $\cos \langle \mathbf{u}, \mathbf{v} \rangle = \frac{\mathbf{u}^\top \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|}$.

Lemma 2 (Schwarz Inequality). $|\mathbf{u}^\top \mathbf{v}| \leq \|\mathbf{u}\| \|\mathbf{v}\|$. The equality holds when $\exists c \in \mathbb{R}. \mathbf{u} = c\mathbf{v}$.

Lemma 3 (Triangle Inequality). $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$. The equality holds when $\exists c \geq 0. \mathbf{u} = c\mathbf{v}$.

1.2 Vector and Matrix Multiplications

Algorithm 1 (Computing $\mathbf{A}\mathbf{x}$). $T(m, n) \sim mn$. In practice, the fastest way to compute $\mathbf{A}\mathbf{x}$ depends on the way the data is stored in the memory. Fortran (column major order) computes $\mathbf{A}\mathbf{x}$ as a linear combination of the columns of \mathbf{A} , while C (row major order) computes $\mathbf{A}\mathbf{x}$ using rows of \mathbf{A} .

$$\mathbf{A}\mathbf{x} = \sum_{j=1}^n x_j \mathbf{a}_j = \begin{bmatrix} \mathbf{a}_1^\top \mathbf{x} \\ \mathbf{a}_2^\top \mathbf{x} \\ \vdots \\ \mathbf{a}_m^\top \mathbf{x} \end{bmatrix}. \quad (2)$$

Algorithm 2 (Computing $\mathbf{y}^\top \mathbf{A}$). $T(m, n) \sim mn$.

$$\mathbf{y}^\top \mathbf{A} = \sum_{i=1}^m y_i \mathbf{a}_i^\top = [\mathbf{y}^\top \mathbf{a}_1 \quad \mathbf{y}^\top \mathbf{a}_2 \quad \cdots \quad \mathbf{y}^\top \mathbf{a}_n]. \quad (3)$$

Algorithm 3 (Computing $\mathbf{A}\mathbf{B}$). Suppose $\mathbf{A} \in \mathbb{R}^{m \times p}, \mathbf{B} \in \mathbb{R}^{p \times n}$. $T(m, n, k) \sim mnk$. In practice, Fortran (column major order) computes $\mathbf{A}\mathbf{B}$ by columns in parallel, while C (row major order) computes $\mathbf{A}\mathbf{B}$ by rows in parallel.

$$\mathbf{A}\mathbf{B} = [\mathbf{A}\mathbf{b}_1 \quad \mathbf{A}\mathbf{b}_2 \quad \cdots \quad \mathbf{A}\mathbf{b}_n] = \begin{bmatrix} \mathbf{a}_1^\top \mathbf{B} \\ \mathbf{a}_2^\top \mathbf{B} \\ \vdots \\ \mathbf{a}_m^\top \mathbf{B} \end{bmatrix} = [\mathbf{a}_i^\top \mathbf{b}_j]_{m \times n} = \sum_{k=1}^p \mathbf{a}_k \mathbf{b}_k^\top. \quad (4)$$

Lemma 4 (Warnings of Matrix Multiplications). The followings are warnings of matrix multiplications.

- In general, $\mathbf{AB} \neq \mathbf{BA}$.
- In general, $\mathbf{AB} = \mathbf{AC} \not\Rightarrow \mathbf{B} = \mathbf{C}$.
- In general, $\mathbf{AB} = \mathbf{0} \not\Rightarrow \mathbf{A} = \mathbf{0} \vee \mathbf{B} = \mathbf{0}$.

1.3 Common Matrix Operations

Table 1 and 2 summarize the properties of common matrix operations.

Lemma 5. Any square matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$ can be formed as a sum of symmetric matrix and an anti-symmetric matrix $\mathbf{A} = \frac{1}{2}(\mathbf{A} + \mathbf{A}^\top) + \frac{1}{2}(\mathbf{A} - \mathbf{A}^\top)$.

Lemma 6. $\text{diag } \mathbf{A}\mathbf{A}^\top = (\mathbf{A} \odot \mathbf{A})\mathbf{1}$.

Lemma 7. The followings are properties of vec operation.

- $(\text{vec } \mathbf{A})^\top (\text{vec } \mathbf{B}) = \text{tr } \mathbf{A}^\top \mathbf{B}$.
- $(\text{vec } \mathbf{A}\mathbf{A}^\top)^\top (\text{vec } \mathbf{B}\mathbf{B}^\top) = \text{tr}(\mathbf{A}^\top \mathbf{B})^\top (\mathbf{A}^\top \mathbf{B}) = \|\mathbf{A}^\top \mathbf{B}\|_F^2 = \sum_{i=1}^n \sum_{j=1}^n (\mathbf{a}_i^\top \mathbf{b}_j)^2$, where $\mathbf{A} := [\mathbf{a}_1 \ \mathbf{a}_2 \ \dots \ \mathbf{a}_n]$ and $\mathbf{B} := [\mathbf{b}_1 \ \mathbf{b}_2 \ \dots \ \mathbf{b}_n]$.

Algorithm 4 (Computing the Rank). rank \mathbf{A} is determined by the SVD of \mathbf{A} . The rank is the number of nonzero singular values. In this case, extremely small nonzero singular values are assumed to be zero. In general, rank estimation is not a simple problem.

Algorithm 5 (Computing the Determinant). Get the REF \mathbf{U} of \mathbf{A} . If there are p row interchanges, $\det \mathbf{A} = (-1)^p$ (product of pivots in \mathbf{U}). Although \mathbf{U} is not unique and pivots are not unique, the product of pivots is unique. $T(n) \sim \frac{1}{3}n^3$.

2 Theory: Vector Spaces and Subspaces

2.1 The Four Fundamental Subspaces

Definition 4 (Orthogonal Subspaces $S_1 \perp S_2$). Two subspaces S_1 and S_2 are orthogonal if $\forall \mathbf{v}_1 \in S_1, \forall \mathbf{v}_2 \in S_2, \mathbf{v}_1^\top \mathbf{v}_2 = 0$.

Definition 5 (Orthogonal Complement S^\perp). The orthogonal complement of a subspace S_1 contains every vector that is perpendicular to S . $C(\mathbf{A})^\perp = \mathcal{N}(\mathbf{A}^\top)$ and $C(\mathbf{A}^\top)^\perp = \mathcal{N}(\mathbf{A})$.

Theorem 8. $\mathcal{N}(\mathbf{A}^\top \mathbf{A}) = \mathcal{N}(\mathbf{A})$. That is to say, if \mathbf{A} has independent columns, $\mathbf{A}^\top \mathbf{A}$ is invertible.

Proof.

$$\mathbf{Ax} = \mathbf{0} \Rightarrow \mathbf{A}^\top \mathbf{Ax} = \mathbf{0} \Rightarrow \mathcal{N}(\mathbf{A}) \subseteq \mathcal{N}(\mathbf{A}^\top \mathbf{A}), \quad (5)$$

$$\mathbf{A}^\top \mathbf{Ax} = \mathbf{0} \Rightarrow \mathbf{x}^\top \mathbf{A}^\top \mathbf{Ax} = 0 \Rightarrow \mathbf{Ax} = \mathbf{0} \Rightarrow \mathcal{N}(\mathbf{A}^\top \mathbf{A}) \subseteq \mathcal{N}(\mathbf{A}). \quad (6)$$

□

Definition 6 (Vector Space). A set of “vectors” together with rules for vector addition and for multiplication by real numbers. The addition and multiplication must produce vectors that are in the space. The space \mathbb{R}^n consists of all column vectors \mathbf{x} with n components. The zero-dimensional space $\mathbf{0}$ consists only of a zero vector $\mathbf{0}$.

Definition 7 (Subspace). A subspace of a vector space is a set of vectors (including $\mathbf{0}$) where all linear combinations stay in that subspace.

Definition 8 (Span). A set of vectors spans a space if their linear combinations fill the space. The span of a set of vectors is the smallest subspace containing those vectors.

Definition 9 (Linear Independent). The columns of \mathbf{A} are linear independent iff $\mathcal{N}(\mathbf{A}) = \mathbf{0}$, or rank $\mathbf{A} = n$.

Definition 10 (Basis). A basis for a vector space is a set of linear independent vectors which span the space. Every vector in the space is a unique combination of the basis vectors. The columns of $\mathbf{A} \in \mathbb{R}^{n \times n}$ are a basis for \mathbb{R}^n iff \mathbf{A} is invertible.

Definition 11 (Dimension). The dimension of a space is the number of vectors in every basis. $\dim \mathbf{0} = 0$ since $\mathbf{0}$ itself forms a linearly dependent set.

Definition 12 (Rank). rank $\mathbf{A} := \dim C(\mathbf{A})$, which also equals to the number pivots of \mathbf{A} .

There are four fundamental subspaces for a matrix \mathbf{A} , as illustrated in Table 3.

2.2 Matrix Inverses

Definition 13 (Invertible Matrix). A square matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$ is invertible if there exists a matrix \mathbf{A}^{-1} such that $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$ or $\mathbf{AA}^{-1} = \mathbf{I}$ (if one holds, the other holds with the same \mathbf{A}^{-1}). A singular matrix is a square matrix that is not invertible. The comparison between invertible and singular matrices are illustrated in Table 4.

Lemma 9. A square matrix \mathbf{A} cannot have two different inverses. This shows that a left-inverse and right-inverse of a square matrix must be the same matrix.

$$\text{Proof. } \mathbf{A}_l^{-1} = \mathbf{A}_l^{-1} \mathbf{I} = \mathbf{A}_l^{-1} \mathbf{AA}_r^{-1} = \mathbf{IA}_r^{-1} = \mathbf{A}_r^{-1}. \quad \square$$

Lemma 10. The followings are inverse of common matrices.

- A diagonal matrix has an inverse iff no diagonal entries are 0. If $\mathbf{A} = \text{diag}(d_1, d_2, \dots, d_n)$, then $\mathbf{A}^{-1} = \text{diag}(d_1^{-1}, d_2^{-1}, \dots, d_n^{-1})$.
- A triangular matrix has an inverse iff no diagonal entries are 0.
- An elimination matrix \mathbf{E}_{ij} has an inverse \mathbf{E}_{ij}^{-1} the same as \mathbf{E}_{ij} , except the (i, j) entry flipped sign.
- The inverse of a symmetric matrix is also symmetric.

Table 1: Properties of common matrix operations (I).

	Inverse	Transpose	Rank
$f(\mathbf{A}^\top)$	$(\mathbf{A}^\top)^{-1} = (\mathbf{A}^{-1})^\top$ exists iff \mathbf{A}^\top is invertible	$(\mathbf{A}^\top)^\top = \mathbf{A}$	$\text{rank } \mathbf{A}^\top = \text{rank } \mathbf{A}$
$f(\mathbf{A}^{-1})$	$(\mathbf{A}^{-1})^{-1} = \mathbf{A}$	$(\mathbf{A}^{-1})^\top = (\mathbf{A}^\top)^{-1}$	-
$f(c\mathbf{A})$	$(c\mathbf{A})^{-1} = \frac{1}{c}\mathbf{A}^{-1}$	$(c\mathbf{A})^\top = c\mathbf{A}^\top$	$\text{rank } c\mathbf{A} = \text{rank } \mathbf{A} \ (c \neq 0)$
$f(\mathbf{A} + \mathbf{B})$	$(\mathbf{A} + \mathbf{B})^{-1} = \mathbf{A}^{-1} + \mathbf{B}^{-1}$	$(\mathbf{A} + \mathbf{B})^\top = \mathbf{A}^\top + \mathbf{B}^\top$	$\text{rank}(\mathbf{A} + \mathbf{B}) \leq \text{rank } \mathbf{A} + \text{rank } \mathbf{B}$
$f(\mathbf{AB})$	$(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$ exists if \mathbf{A} and \mathbf{B} are invertible	$(\mathbf{AB})^\top = \mathbf{B}^\top\mathbf{A}^\top$	$\text{rank } \mathbf{AB} \leq \min(\text{rank } \mathbf{A}, \text{rank } \mathbf{B})$
$f(\mathbf{A}^\top\mathbf{A})$	$(\mathbf{A}^\top\mathbf{A})^{-1}$ exists iff \mathbf{A} has independent columns	$(\mathbf{A}^\top\mathbf{A})^\top = \mathbf{A}^\top\mathbf{A}$	$\text{rank } \mathbf{A}^\top\mathbf{A} = \text{rank } \mathbf{AA}^\top = \text{rank } \mathbf{A}$
Others	\mathbf{A} and \mathbf{B} are invertible $\nRightarrow \mathbf{A} + \mathbf{B}$ is invertible	$(\mathbf{Ax})^\top \mathbf{y} = \mathbf{x}^\top (\mathbf{A}^\top \mathbf{y})$	-

Table 2: Properties of common matrix operations (II).

	Determinant	Trace	Eigenvalue
$f(\mathbf{A})$	$\det \mathbf{A} = \prod_{i=1}^n \lambda_i$	$\text{tr } \mathbf{A} = \sum_{i=1}^n \lambda_i$	-
$f(\mathbf{A}^\top)$	$\det \mathbf{A}^\top = \det \mathbf{A}$	$\text{tr } \mathbf{A}^\top = \text{tr } \mathbf{A}$	$\lambda(\mathbf{A}^\top) = \lambda(\mathbf{A})$
$f(\mathbf{A}^{-1})$	$\det \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}$	-	$\lambda(\mathbf{A}^{-1}) = \frac{1}{\lambda(\mathbf{A})}$
$f(c\mathbf{A})$	$\det c\mathbf{A} = c^n \det \mathbf{A}$	$\text{tr } c\mathbf{A} = c \text{tr } \mathbf{A}$	-
$f(\mathbf{A} + \mathbf{B})$	-	$\text{tr}(\mathbf{A} + \mathbf{B}) = \text{tr } \mathbf{A} + \text{tr } \mathbf{B}$	-
$f(\mathbf{AB})$	$\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$	$\text{tr } \mathbf{AB} = \text{tr } \mathbf{BA}$	-
$f(\mathbf{A}^\top\mathbf{A})$	-	-	$\lambda(\mathbf{A}^\top\mathbf{A}) = \lambda(\mathbf{AA}^\top) = \sigma(\mathbf{A})^2$
$f(\mathbf{A}^k)$	$\det \mathbf{A}^k = (\det \mathbf{A})^k$	-	$\lambda(\mathbf{A}^k) = \lambda(\mathbf{A})^k$ (if $k \geq 1$)
Others	$\det(\mathbf{I} + \mathbf{uv}^\top) = 1 + \mathbf{u}^\top \mathbf{v}$	$\mathbf{x}^\top \mathbf{y} = \text{tr } \mathbf{xy}^\top$	$\lambda(c\mathbf{I} + \mathbf{A}) = c + \lambda(\mathbf{A})$

Table 3: Vector spaces for $\mathbf{A} \in \mathbb{R}^{m \times n}$, where $\mathbf{R} = \mathbf{EA}$ is the RREF of \mathbf{A} .

Subspace	Definition	Basis	Dimension
Column space	$\mathcal{C}(\mathbf{A}) := \{\mathbf{v} \in \mathbb{R}^m \mid \exists \mathbf{x}. \mathbf{Ax} = \mathbf{v}\}$	Pivot columns of \mathbf{A}	$\text{rank } \mathbf{A}$
Left nullspace	$\mathcal{N}(\mathbf{A}^\top) := \{\mathbf{x} \in \mathbb{R}^m \mid \mathbf{A}^\top \mathbf{x} = \mathbf{0}\}$	Last rows of \mathbf{E}	$m - \text{rank } \mathbf{A}$
Row space	$\mathcal{C}(\mathbf{A}^\top) := \{\mathbf{v} \in \mathbb{R}^n \mid \exists \mathbf{x}. \mathbf{A}^\top \mathbf{x} = \mathbf{v}\}$	Pivot rows of \mathbf{A} or \mathbf{R}	$\text{rank } \mathbf{A}$
Nullspace	$\mathcal{N}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{Ax} = \mathbf{0}\}$	Special solutions of \mathbf{A} or \mathbf{R}	$n - \text{rank } \mathbf{A}$

Table 4: Comparasions of invertible and singular matrices (the matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$).

	Invertible matrices	Singular matrices
Number pivots	n	$< n$
$\text{rank } \mathbf{A}$	n	$< n$
RREF	\mathbf{I}	$\begin{bmatrix} \mathbf{R} & \mathbf{F} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$
Columns	Independent	Dependent
Rows	Independent	Dependent
Solution to $\mathbf{Ax} = \mathbf{0}$	Only $\mathbf{0}$	Infinitely many solutions
Solution to $\mathbf{Ax} = \mathbf{b}$	Only $\mathbf{A}^{-1}\mathbf{b}$	No or infinitely many solutions
Eigenvalue	All $\lambda > 0$	Some eigenvalue is 0
$\det \mathbf{A}$	$\neq 0$	0
$\mathbf{A}^\top \mathbf{A}$	PD	PSD
Linear transformation $\mathbf{x} \mapsto \mathbf{Ax}$	One-to-one and onto	-

Algorithm 6 (The \mathbf{A}^{-1} Algorithm). When \mathbf{A} is square and invertible, Gaussian Elimination on $[\mathbf{A} \ \mathbf{I}]$ to produce $[\mathbf{R} \ \mathbf{E}]$. Since $\mathbf{R} = \mathbf{I}$, then $\mathbf{EA} = \mathbf{R}$ becomes $\mathbf{EA} = \mathbf{I}$. The elimination result is $[\mathbf{I} \ \mathbf{A}^{-1}]$. $T(n) \sim n^3$. In practice, \mathbf{A}^{-1} is seldom

computed, unless the entries of \mathbf{A}^{-1} is explicitly needed.

2.3 Ill-conditioned Matrices

Definition 14 (Ill-conditioned Matrix). An invertible matrix that can become singular if some of its entries are changed ever so slightly. In this case, row reduction may produce fewer than n pivots as a result of roundoff error. Also, round-off error can sometimes make a singular matrix appear to be invertible.

Definition 15 (Condition Number $\text{cond } \mathbf{A}$). $\text{cond } \mathbf{A} := \frac{\sigma_1}{\sigma_r}$ for a matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$. The larger the condition number, the closer the matrix is to being singular. $\text{cond } \mathbf{I} = 1$, and $\text{cond}(\text{singular matrix}) = \infty$.

2.4 Least-squares and Projections

It is often the case that $\mathbf{Ax} = \mathbf{b}$ is overdetermined: $m > n$. The n columns span a small part of \mathbb{R}^m . Typically \mathbf{b} is outside $C(\mathbf{A})$ and there is no solution. One approach is least-squares.

Theorem 11 (Least-squares Approximation). The projection of $\mathbf{b} \in \mathbb{R}^m$ onto $C(\mathbf{A})$ is

$$\hat{\mathbf{b}} = \mathbf{A}(\mathbf{A}^\top \mathbf{A})^{-1} \mathbf{A}^\top \mathbf{b}, \quad (7)$$

where the projection matrix $\mathbf{P} = \mathbf{A}(\mathbf{A}^\top \mathbf{A})^{-1} \mathbf{A}^\top$ and

$$\arg \min_{\mathbf{x}} \frac{1}{m} \|\mathbf{Ax} - \mathbf{b}\|^2 = (\mathbf{A}^\top \mathbf{A})^{-1} \mathbf{A}^\top \mathbf{b}. \quad (8)$$

In particular, the projection of \mathbf{b} onto the line $\mathbf{a} \in \mathbb{R}^m$ is

$$\hat{\mathbf{b}} = \frac{\mathbf{a}\mathbf{a}^\top}{\mathbf{a}^\top \mathbf{a}} \mathbf{b}. \quad (9)$$

Proof. Let $\mathbf{x}^* := \arg \min_{\mathbf{x}} \frac{1}{m} \|\mathbf{Ax} - \mathbf{b}\|^2$ and the approximation error term $\mathbf{e} := \mathbf{b} - \mathbf{Ax}^*$. $\mathbf{e} \perp C(\mathbf{A}) \Rightarrow \mathbf{e} \in \mathcal{N}(\mathbf{A}^\top) \Rightarrow \mathbf{A}^\top \mathbf{e} = \mathbf{A}^\top (\mathbf{b} - \mathbf{Ax}^*) = \mathbf{0} \Rightarrow \mathbf{A}^\top \mathbf{Ax}^* = \mathbf{A}^\top \mathbf{b}$. Another proof is by setting $\frac{\partial \mathcal{L}(\mathbf{x})}{\partial \mathbf{x}} = \frac{2}{m} \mathbf{A}^\top \mathbf{Ax} - \frac{2}{m} \mathbf{A}^\top \mathbf{b} = \mathbf{0}$. \square

Lemma 12. $\mathbf{Ax} = \mathbf{b}$ has a unique least-squares solution for each \mathbf{b} when the columns of \mathbf{A} are linearly independent.

Algorithm 7 (Least-squares Approximation). Since $\text{cond } \mathbf{A}^\top \mathbf{A} = (\text{cond } \mathbf{A})^2$, least-squares is solved by QR factorization.

$$\mathbf{A}^\top \mathbf{Ax} = \mathbf{A}^\top \mathbf{b} \Rightarrow \mathbf{R}^\top \mathbf{Rx} = \mathbf{R}^\top \mathbf{Q}^\top \mathbf{b} \Rightarrow \mathbf{Rx} = \mathbf{Q}^\top \mathbf{b}. \quad (10)$$

$$T(m, n) \sim mn^2.$$

Another common case is that $\mathbf{Ax} = \mathbf{b}$ is underdetermined: $m < n$ or \mathbf{A} has dependent columns. Typically there are infinitely many solutions. One approach is using regularization.

Theorem 13 (Least-squares Approximation With Regularization).

$$\arg \min_{\mathbf{x}} \left(\frac{1}{m} \|\mathbf{Ax} - \mathbf{b}\|^2 + \lambda \|\mathbf{x}\|^2 \right) = \left(\frac{1}{m} \mathbf{A}^\top \mathbf{A} + \lambda \mathbf{I} \right)^{-1} \frac{1}{m} \mathbf{A}^\top \mathbf{b}. \quad (11)$$

Proof. By setting $\frac{\partial \mathcal{L}(\mathbf{x})}{\partial \mathbf{x}} = \frac{2}{m} \mathbf{A}^\top \mathbf{Ax} - \frac{2}{m} \mathbf{A}^\top \mathbf{b} + 2\lambda \mathbf{x} = \mathbf{0}$. \square

Lemma 14 (Weighted Least-squares Approximation). Suppose $\mathbf{C} \in \mathbb{R}^{m \times m}$ is a diagonal matrix specifying the weight for the equations,

$$\arg \min_{\mathbf{x}} \frac{1}{m} (\mathbf{Ax} - \mathbf{b})^\top \mathbf{C} (\mathbf{Ax} - \mathbf{b}) = (\mathbf{A}^\top \mathbf{C} \mathbf{A})^{-1} \mathbf{A}^\top \mathbf{C} \mathbf{b}. \quad (12)$$

Proof. By setting $\frac{\partial \mathcal{L}(\mathbf{x})}{\partial \mathbf{x}} = \frac{2}{m} \mathbf{A}^\top \mathbf{C} \mathbf{Ax} - \frac{2}{m} \mathbf{A}^\top \mathbf{C} \mathbf{b} = \mathbf{0}$. \square

2.5 Orthogonality

Lemma 15 (Plane in Point-normal Form). The equation of a hyperplane with a point \mathbf{x}_0 in the plane and a normal vector \mathbf{w} orthogonal to the plane is $\mathbf{w}^\top (\mathbf{x} - \mathbf{x}_0) = 0$.

Lemma 16. The distance from a point \mathbf{x} to a plane with a point \mathbf{x}_0 on the plane and a normal vector \mathbf{w} orthogonal to the plane is $\frac{|\mathbf{w}^\top (\mathbf{x} - \mathbf{x}_0)|}{\|\mathbf{w}\|}$.

Definition 16 (Orthogonal Vectors). Two vectors \mathbf{u} and \mathbf{v} are orthogonal if $\mathbf{u}^\top \mathbf{v} = 0$.

Definition 17 (Orthonormal Vectors \mathbf{q}). The columns of \mathbf{Q} are orthonormal if $\mathbf{Q}^\top \mathbf{Q} = [\mathbf{q}_i^\top \mathbf{q}_j]_{n \times n} = \mathbf{I}$. If \mathbf{Q} is square, it is called the *orthogonal matrix*.

Lemma 17. The followings are orthogonal matrices.

- Every permutation matrix \mathbf{P} .
- Reflection matrix $\mathbf{I} - 2\mathbf{e}\mathbf{e}^\top$ where \mathbf{e} is any unit vector.

Lemma 18. Orthogonal matrices \mathbf{Q} preserve certain norms.

- $\|\mathbf{Qx}\|_2 = \|\mathbf{x}\|_2$.
- $\|\mathbf{Q}_1 \mathbf{A} \mathbf{Q}_2^\top\|_2 = \|\mathbf{A}\|_2$.
- $\|\mathbf{Q}_1 \mathbf{A} \mathbf{Q}_2^\top\|_F = \|\mathbf{A}\|_F$.

Theorem 19. The projection of $\mathbf{b} \in \mathbb{R}^m$ onto $C(\mathbf{Q})$ is

$$\hat{\mathbf{b}} = \mathbf{Q} \mathbf{Q}^\top \mathbf{b} = \sum_{j=1}^n \mathbf{q}_j \mathbf{q}_j^\top \mathbf{b}. \quad (13)$$

If \mathbf{Q} is square, $\mathbf{b} = \sum_{j=1}^n \mathbf{q}_j \mathbf{q}_j^\top \mathbf{b}$.

Definition 18 (QR Factorization). $\mathbf{A} \in \mathbb{R}^{n \times n}$ can be written as $\mathbf{A} = \mathbf{Q} \mathbf{R}$, where columns of $\mathbf{Q} \in \mathbb{R}^{n \times n}$ are orthonormal, and $\mathbf{R} \in \mathbb{R}^{n \times n}$ is an upper triangular matrix.

Algorithm 8 (Gram-Schmidt Process). The idea is to subtract from every new vector its projections in the directions already set, and divide the resulting vectors by their lengths, such that

$$\begin{aligned} \mathbf{A} &= [\mathbf{a}_1 \ \mathbf{a}_2 \ \cdots \ \mathbf{a}_n] \\ &= [\mathbf{q}_1 \ \mathbf{q}_2 \ \cdots \ \mathbf{q}_n] \begin{bmatrix} \mathbf{q}_1^\top \mathbf{a}_1 & \mathbf{q}_1^\top \mathbf{a}_2 & \cdots & \mathbf{q}_1^\top \mathbf{a}_n \\ \mathbf{q}_2^\top \mathbf{a}_2 & \cdots & \mathbf{q}_2^\top \mathbf{a}_n \\ \vdots & \ddots & \vdots \\ \mathbf{q}_n^\top \mathbf{a}_n \end{bmatrix} \\ &= \mathbf{Q} \mathbf{Q}^\top \mathbf{A} = \mathbf{Q} \mathbf{R}. \end{aligned} \quad (14)$$

The algorithm is illustrated in Alg. 1. $T(n) = \sum_{j=1}^n \sum_{i=1}^j 2n \sim n^3$. In practice, the roundoff error can build up.

Algorithm 1 QR Factorization.

Input: $A \in \mathbb{R}^{n \times n}$
Output: $Q \in \mathbb{R}^{n \times n}, R \in \mathbb{R}^{n \times n}$

```

1:  $Q \leftarrow R \leftarrow \mathbf{0}$ 
2: for  $j \leftarrow 0$  to  $n - 1$  do
3:    $q_j \leftarrow a_j$ 
4:   for  $i \leftarrow 0$  to  $j - 1$  do
5:      $r_{ij} \leftarrow q_i^T a_j$ 
6:      $q_j \leftarrow q_j - r_{ij} q_i$ 
7:    $r_{jj} \leftarrow \|q_j\|$ 
8:    $q_j \leftarrow \frac{q_j}{\|q_j\|}$ 
9: return  $Q, R$ 

```

Algorithm 9 (Householder reflections). In practice, Householder reflections are often used instead of the Gram-Schmidt process, even though the factorization requires about twice as much arithmetic.

3 Application: Solving Linear Systems

Understanding the linear system $Ax = b$.

- Row picture: m hyperplanes meet at a single point (if possible).
- Column picture: n vectors are combined to produce b .

Definition 19 (Consistent Linear System). A linear system is said to be *consistent* if it has either one solution or infinitely many solutions, and it is said to be *inconsistent* if it has no solution.

The idea of *Gaussian elimination* is to replace one linear system with an equivalent linear system (i.e., one with the same solution set) that is easier to solve.

3.1 Elementary Row Operations

Definition 20 (Elementary Row Operations). The followings are three types of elementary row operations.

- (Replacement) Replace one row by the subtraction of itself and a multiple of another row of the matrix.
- (Interchange) Interchange any two rows.
- (Scaling) Multiply all entries of a row by a nonzero constant.

Definition 21 (Elementary Matrix E_{ij}). Identity matrix with an extra nonzero entry $-l_{ij}$ in the (i, j) position, where multiplier $l_{ij} := \frac{\text{entry to eliminate in row } i}{\text{pivot in row } j}$. $E_{ij}A$ means that we perform (row i) $-l_{ij}$ (row j) to make the (i, j) entry zero.

Definition 22 (Block Elimination). We perform (row 2) $-CA^{-1}$ (row 1) to get a zero block in the first column.

$$\begin{bmatrix} I & 0 \\ -CA^{-1} & I \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & B \\ 0 & D - CA^{-1}B \end{bmatrix}. \quad (15)$$

The final block $D - CA^{-1}B$ is called the *Schur complement*.

Definition 23 (Row Exchange Matrix P_{ij}). Identity matrix with row i and row j exchanged. $P_{ij}A$ means that we exchange row i and row j .

Definition 24 (Permutation Matrix P). A permutation matrix has the rows of the identity I in any order. This matrix has a single 1 in every row and every column. The simplest permutation matrix is I . The next simplest are the row exchange matrix P_{ij} . There are $n!$ permutation matrices of order n , half of which have determinant 1, and the other half are -1. If P is a permutation matrix, then $P^{-1} = P^T$, which is also a permutation matrix.

Definition 25 (Augmented Matrix $[A \ b]$). Elimination does the same row operations to A and to b . We can include b as an extra column and let elimination act on whole rows of this matrix.

Definition 26 (Row Equivalent). Two matrices are called row equivalent if there is a sequence of elementary row operations that transforms one matrix into the other.

Lemma 20. If the augmented matrices of two linear systems are row equivalent, then the two linear systems have the same solution set.

3.2 Row Reduction and Echelon Forms

Definition 27 (Row Echelon Form (REF) U). A rectangular matrix is in row echelon form if it has the following properties.

- All nonzero rows are above any rows of all zeros.
- Each leading entry of a row is in a column to the right of the leading entry of the row above it.
- All entries in a column below a leading are zeros.

Definition 28 (Reduced Row Echelon Form (RREF) R). If a matrix in row echelon form satisfies the following additional conditions, then it is in reduced row echelon form.

- The leading entry in each nonzero row is 1.
- Each leading 1 is the only nonzero entry in its column.

The general form is $R = \begin{bmatrix} I & F \\ 0 & 0 \end{bmatrix}$, which has r pivot rows and pivot columns, $m - r$ zero rows, and $n - r$ free columns. Every free column is a combination of earlier pivot columns. Free variables can be given any values whatsoever.

Definition 29 (Pivot). A *pivot position* in a matrix A is a location in A that corresponds to a leading 1 in the RREF of

Table 5: The four possibilities for steady state problem $\mathbf{Ax} = \mathbf{b}$, where $\mathbf{A} \in \mathbb{R}^{m \times n}$ and $r := \text{rank } \mathbf{A}$. Gaussian elimination on $[\mathbf{A} \ \mathbf{b}]$ gives $\mathbf{Rx} = \mathbf{d}$, where $\mathbf{R} := \mathbf{EA}$ and $\mathbf{d} := \mathbf{Eb}$.

Case	Shape of \mathbf{A}	RREF \mathbf{R}	Particular solution \mathbf{x}_p	Nullspace matrix	# solutions	Left inverse	Right inverse
$r = m = n$	Square and invertible	$[\mathbf{I}]$	$[\mathbf{A}^{-1}\mathbf{b}]$	$[\mathbf{0}]$	1	\mathbf{A}^{-1}	\mathbf{A}^{-1}
$r = m < n$	Short and wide	$[\mathbf{I} \ \mathbf{F}]$	$\begin{bmatrix} \mathbf{d} \\ \mathbf{0} \end{bmatrix}$	$\begin{bmatrix} -\mathbf{F} \\ \mathbf{I} \end{bmatrix}$	∞	-	$\mathbf{A}^\top(\mathbf{AA}^\top)^{-1}$
$r = n < m$	Tall and thin	$\begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix}$	$[\mathbf{d}]$ or none	$[\mathbf{0}]$	0 or 1	$(\mathbf{A}^\top \mathbf{A})^{-1} \mathbf{A}$	-
$r < m, r < n$	Not full rank	$\begin{bmatrix} \mathbf{I} \ \mathbf{F} \\ \mathbf{0} \ \mathbf{0} \end{bmatrix}$	$\begin{bmatrix} \mathbf{d} \\ \mathbf{0} \end{bmatrix}$ or none	$\begin{bmatrix} -\mathbf{F} \\ \mathbf{I} \end{bmatrix}$	0 or ∞	-	-

A. A *pivot row/column* is a row/column of \mathbf{A} that contains a pivot position. A *pivot* is a nonzero number in a pivot position. A zero in the pivot position can be repaired if there is a nonzero below it.

Algorithm 10 (RREF). *The algorithm to get the RREF of \mathbf{A} is illustrated in Alg. 2. We use partial pivoting to reduce the roundoff errors in the calculations. The FLOP (number of multiplication/division on two floating point numbers) is $T(m, n) = \sum_{i=1}^{m-1} (n-i+1)(m-i) \sim \frac{1}{3}m^3 + \frac{1}{3}m^2n$.*

Algorithm 2 The RREF algorithm.

Input: $\mathbf{A} \in \mathbb{R}^{m \times n}$

Output: $\mathbf{R} \in \mathbb{R}^{m \times n}$

- 1: \triangleright Elimination downwards to produce zeros below the pivots.
- 2: **while** there is nonzero row to modify **do**
- 3: Pick the leftmost nonzero column. This is a pivot column. The pivot position is at the top.
- 4: Use elementary row interchange to select the entry with the largest absolute value in the pivot column as a pivot.
- 5: Use elementary row replacements to create zeros in all positions below the pivot.
- 6: Cover/Ignore that pivot row.
- 7: Use elementary row scaling to produce 1 in all pivot positions.
- 8: \triangleright Elimination upwards to produce zeros above the pivots.
- 9: **while** there is nonzero row to modify **do**
- 10: Pick the rightmost nonzero column.
- 11: Use elementary row replacements to create zeros in all positions above the pivot.
- 12: Cover/Ignore that pivot row.
- 13: **return** the result

Lemma 21. *Any nonzero matrix is row equivalent to more than one matrix in REF, by using different sequences of elementary row operations. However, each matrix is row equivalent to one and only one matrix in RREF.*

Lemma 22. *An elimination matrix $\mathbf{E} \in \mathbb{R}^{m \times m}$ which is a product of elementary matrices \mathbf{E}_{ij} , row exchange matrices \mathbf{P}_{ij} , and diagonal matrix \mathbf{D}^{-1} (divides rows by their pivots to produce 1's) puts the original \mathbf{A} into its RREF, i.e., $\mathbf{EA} = \mathbf{R}$. If we want \mathbf{E} , we can apply row reduction to the matrix $[\mathbf{A} \ \mathbf{I}]$, namely, $\mathbf{E}[\mathbf{A} \ \mathbf{I}] = [\mathbf{R} \ \mathbf{E}]$.*

3.3 Solution of a Linear System $\mathbf{Ax} = \mathbf{b}$

Algorithm 11 (Solving $\mathbf{Ax} = \mathbf{b}$). *The algorithm is illustrated in Alg. 3. There are four possibilities for $\mathbf{Ax} = \mathbf{b}$ depending on rank \mathbf{A} , as illustrated in Table 5. $T(m, n) \sim \frac{1}{3}m^3 + \frac{1}{3}m^2n$.*

Algorithm 3 Solving a linear system $\mathbf{Ax} = \mathbf{b}$.

Input: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$

Output: $\mathbf{x} \in \mathbb{R}^n$

- 1: Use elementary row operations to transform the augmented matrix $[\mathbf{A} \ \mathbf{b}]$ to its RREF $[\mathbf{R} \ \mathbf{d}]$, where $\mathbf{R} = \begin{bmatrix} \mathbf{I} \ \mathbf{F} \\ \mathbf{0} \ \mathbf{0} \end{bmatrix}$.
- 2: **if** there is a row in $[\mathbf{R} \ \mathbf{d}]$ whose entries are all zeros except the last one on the right **then**
- 3: **return** "The system is inconsistent and has no solution"
- 4: Find one particular solution $\mathbf{x}_p := \begin{bmatrix} \mathbf{d} \\ \mathbf{0} \end{bmatrix}$, which solves $\mathbf{Ax}_p = \mathbf{b}$, by setting the free variables to 0.
- 5: Find special solutions which are columns of the nullspace matrix $\mathbf{N} := \begin{bmatrix} -\mathbf{F} \\ \mathbf{I} \end{bmatrix}$ which solves $\mathbf{Ax}_n = \mathbf{0}$. Every free column leads to a special solution. The complete null solution \mathbf{x}_n is a linear combination of the special solutions.
- 6: **return** $\mathbf{x}_p + \mathbf{x}_n$

3.4 The LU Factorization

The LU factorization is motivated by the problem of solving a set of linear systems all with the same coefficient matrix: $\{\mathbf{Ax}_k = \mathbf{b}_k\}_{k=1}^K$.

Definition 30 (LU Factorization). Assuming no row exchanges, $\mathbf{A} \in \mathbb{R}^{m \times n}$ can be written as $\mathbf{A} = \mathbf{LU}$, where $\mathbf{L} \in \mathbb{R}^{m \times m}$ is an invertible lower triangular matrix with 1's on the diagonal and multipliers l_{ij} are below the diagonal. $\mathbf{U} \in \mathbb{R}^{m \times n}$ is an REF of \mathbf{A} .

Besides, we can extract from \mathbf{U} a diagonal matrix $\mathbf{D} \in \mathbb{R}^{m \times m}$ containing the pivots: $\mathbf{A} = \mathbf{LDU}$. The new \mathbf{U} matrix has 1's on the pivot positions. When \mathbf{A} is symmetric, the usual LU factorization becomes $\mathbf{A} = \mathbf{LDL}^\top$. Sometimes row exchanges are needed to produce pivots $\mathbf{PA} = \mathbf{LU}$.

Algorithm 12 (The LU Factorization). *The algorithm is illustrated in Alg. 4. $T(m, n) \sim \frac{1}{3}m^3 + \frac{1}{3}m^2n$. For a band matrix \mathbf{B} with w nonzero diagonals below and above its main diagonal, $T(m, n, w) \sim mw^2$.*

Algorithm 4 LU factorization on \mathbf{A} .

Input: $\mathbf{A} \in \mathbb{R}^{m \times n}$

Output: \mathbf{L}, \mathbf{U}

```

1:  $\mathbf{L} \leftarrow \mathbf{0} \in \mathbb{R}^{m \times m}$ 
2:  $k \leftarrow 0$ 
3: for  $j \leftarrow 0$  to  $n - 1$  do
4:   if  $j$ -th column is not a pivot column then
5:     continue
6:   Row exchange to make  $a_{kj}$  as the largest available pivot.
7:    $l_{kk} \leftarrow 1$ 
8:   for  $i \leftarrow k + 1$  to  $m - 1$  do
9:      $l_{ik} \leftarrow \frac{a_{ij}}{a_{kj}}$  ▷ Multiplier
10:    ▷ Eliminates row  $i$  beyond row  $k$ 
11:    (row  $i$  of  $\mathbf{A}$ )  $\leftarrow$  (row  $i$  of  $\mathbf{A}$ ) -  $l_{ik}$  (row  $k$  of  $\mathbf{A}$ )
12:     $k \leftarrow k + 1$ 
13: return  $\mathbf{L}, \mathbf{A}$ 

```

Lemma 23. *Assuming no row exchanges, when a row of \mathbf{A} starts with zeros, so does that row of \mathbf{L} . When a column of \mathbf{A} starts with zeros, so does that column of \mathbf{U} .*

Algorithm 13 (Solving $\{\mathbf{A}\mathbf{x}_k = \mathbf{b}_k\}_{k=1}^K$). *The algorithm is illustrated in Alg. 5. $T(m, n, K) \sim \frac{1}{3}m^3 + \frac{1}{3}m^2n + n^2K$. For a band matrix \mathbf{B} with w nonzero diagonals below and above its main diagonal, $T(m, n, w) \sim mw^2 + 2nwK$.*

Algorithm 5 Solving $\{\mathbf{A}\mathbf{x}_k = \mathbf{b}_k\}_{k=1}^K$.

Input: $\mathbf{A}, \{\mathbf{b}_k\}_{k=1}^K$.

Output: $\{\mathbf{x}_k\}_{k=1}^K$

```

1: LU factorization  $\mathbf{A} = \mathbf{LU}$ .
2: for  $k \leftarrow 1$  to  $K$  do
3:   Solve  $\mathbf{L}\mathbf{y}_k = \mathbf{b}_k$  by forward substitution.
4:   Solve  $\mathbf{U}\mathbf{x}_k = \mathbf{y}_k$  by backward substitution.
5: return  $\{\mathbf{x}_k\}_{k=1}^K$ 

```

3.5 Matrices in Engineering

Suppose there are n masses vertically connected by a line of m springs. We define

- $\mathbf{u} \in \mathbb{R}^n$: The movement of the masses, where we define $u_j > 0$ when a mass move downward,
- $\mathbf{y} \in \mathbb{R}^m$: The internal force of each spring, where we define $y_i > 0$ when a spring is in stretched.
- $\mathbf{f} := [m_j g]_n \in \mathbb{R}^n$: The external force comes from gravity.
- $\mathbf{C} := \text{diag } \mathbf{c} \in \mathbb{R}^{m \times m}$: The spring constant of each spring.

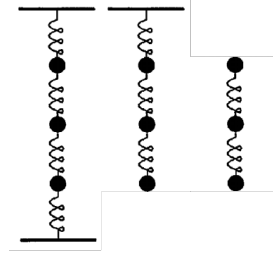


Figure 1: Three different cases (fixed-fixed, fixed-free, and free-free) for a spring system.

- $\mathbf{e} \in \mathbb{R}^m$: The stretching distance of each spring.

By Hooke's Law $y_i = c_i e_i$. In matrix form, $\mathbf{y} = \mathbf{C}\mathbf{e}$.

These are three different cases for these springs, as illustrated in Fig. 1.

Fixed-fixed Case. In this case, $m = n + 1$ and the top and bottom spring are fixed. Originally there is no stretching. Then gravity acts to move down the masses by \mathbf{u} . Each spring is stretched by the difference in displacements of its end $e_i = u_i - u_{i-1}$. Besides, $e_1 = u_1$ since the top is fixed, and $e_m = -u_n$ since the bottom is fixed. In matrix form,

$$\mathbf{e} = \mathbf{A}\mathbf{u} := \begin{bmatrix} 1 & & & \\ -1 & 1 & & \\ & -1 & \ddots & \\ & & \ddots & 1 \\ & & & -1 \end{bmatrix} \mathbf{u}. \quad (16)$$

Finally comes the balance equation, the internal forces from the springs balance the external forces on the masses $f_i = y_i - y_{i+1}$. In matrix form,

$$\mathbf{f} = \mathbf{A}^\top \mathbf{y} := \begin{bmatrix} 1 & -1 & & \\ & 1 & -1 & \\ & & \ddots & \ddots \\ & & & 1 & -1 \end{bmatrix} \mathbf{y}. \quad (17)$$

Combining the three matrices gives

$$\mathbf{A}^\top \mathbf{C} \mathbf{A} \mathbf{u} = \mathbf{f}. \quad (18)$$

When $\mathbf{C} = \mathbf{I}$,

$$\mathbf{K} = \mathbf{A}^\top \mathbf{A} = \begin{bmatrix} 2 & -1 & & \\ -1 & 2 & \ddots & \\ & \ddots & \ddots & -1 \\ & & -1 & 2 \end{bmatrix} \in \mathbb{R}^{n \times n}. \quad (19)$$

Lemma 24. *The followings are properties of the matrix \mathbf{K} .*

- \mathbf{K} is symmetric.
- \mathbf{K} is tridiagonal.
- The i -th pivot of \mathbf{K} is $\frac{i+1}{i}$, and it converges to 1 when $n \rightarrow \infty$.
- \mathbf{K} is PD.
- $\det \mathbf{K} = n + 1$.

- \mathbf{K}^{-1} is a full matrix with all positive entries. \mathbf{K}^{-1} is also PD.

Fixed-free Case. In this case, $m = n$ and the top spring are fixed. When $\mathbf{C} = \mathbf{I}$,

$$\mathbf{A} = \begin{bmatrix} 1 & & & & \\ -1 & 1 & & & \\ & \ddots & \ddots & & \\ & & -1 & 1 & \\ & & & & 1 \end{bmatrix}, \mathbf{K} = \begin{bmatrix} 2 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & & -1 & 1 \\ & & & & 1 \end{bmatrix}. \quad (20)$$

Free-free Case. In this case, $m = n - 1$ and the both ends are free. When $\mathbf{C} = \mathbf{I}$,

$$\mathbf{A} = \begin{bmatrix} -1 & 1 & & & \\ & \ddots & \ddots & & \\ & & -1 & 1 & \\ & & & & 1 \end{bmatrix}, \mathbf{K} = \begin{bmatrix} 1 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & & -1 & 1 \\ & & & & 1 \end{bmatrix}. \quad (21)$$

There is a nonzero solution to $\mathbf{A}\mathbf{u} = \mathbf{0}$. The masses can move $\mathbf{u}_n = \mathbf{1}$ with no stretching of the springs $\mathbf{e} = \mathbf{0}$. \mathbf{K} is only PSD, and $\mathbf{K}\mathbf{u} = \mathbf{f}$ is solvable for special \mathbf{f} , i.e., $\mathbf{1}^\top \mathbf{f} = 0$, or the whole line of spring (with both ends free) will take off like a rocket.

3.6 Graph and Networks

Definition 31 (Adjacency Matrix). Given a directed graph $G = (V, E)$ where $|V| = n$, the adjacency matrix is $\mathbf{A} = [\mathbb{1}((i, j) \in E)]_{n \times n}$, i.e., $a_{ij} = 1$ if there exists path from vertex i to vertex j . The (i, j) entry of \mathbf{A}^k counts the number of k -step path from vertex i to vertex j . If G is undirected, \mathbf{A} is symmetric.

Definition 32 (Incidence Matrix). Given a directed graph $G = (V, E)$ where $|V| = n$ and $|E| = m$, the incidence matrix is $\mathbf{A} \in \mathbb{R}^{m \times n}$ where $a_{ij} = -1$ if edge i starts from vertex j , $a_{ij} = 1$ if edge i ends at vertex j , and $a_{ij} = 0$ otherwise.

For a curcuit in Fig. 2, the incidence matrix is

$$\mathbf{A} := \begin{bmatrix} -1 & 1 & & & \\ -1 & & 1 & & \\ & -1 & 1 & & \\ -1 & & & 1 & \\ & -1 & & & 1 \\ & & -1 & 1 & \end{bmatrix}. \quad (22)$$

We define

- $\mathbf{u} \in \mathbb{R}^n$. Potentials (the voltages) at n nodes.
- $\mathbf{y} \in \mathbb{R}^m$. Currents flowing along m edges.
- $\mathbf{f} \in \mathbb{R}^n$ be the current sources into n nodes.
- $\mathbf{C} := \text{diag}(c_1, c_2, \dots, c_m) \in \mathbb{R}^{m \times m}$. Conductance of each edge.

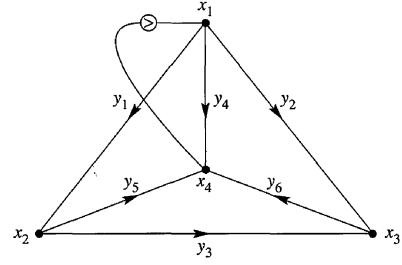


Figure 2: A curcuit with a current source into vertex 1.

$\mathbf{A}\mathbf{u}$ gives the potential differences across the m edges. *Ohm's law* says that the current y_i through the resistor is proportional to the potential difference $\mathbf{y} = \mathbf{C}\mathbf{A}\mathbf{u}$. *Kirchhoff's current law* says that the net current into every node is zero, which is expressed as

$$\mathbf{A}^\top \mathbf{y} = \mathbf{A}^\top \mathbf{C}\mathbf{A}\mathbf{u} = \mathbf{f}. \quad (23)$$

Kirchhoff's voltage law says that the sum of potential differences around a loop must be zero.

Lemma 25. The followings are properties of an incidence matrix \mathbf{A} .

- $\dim C(\mathbf{A}) = \dim C(\mathbf{A}^\top) = n - 1$.
- $\dim \mathcal{N}(\mathbf{A}) = 1$
- $\dim \mathcal{N}(\mathbf{A}^\top) = m - n + 1$.

Proof. Since we can raise or lower all the potentials by the same constant, $\mathbf{1} \in \mathcal{N}(\mathbf{A})$. Rows of \mathbf{A} are dependent if the corresponding edges containing a loop. At the end of elimination we have a full set of r independent rows. Those r edges form a spanning tree of the graph, which has $n - 1$ edges of the graph is connected. \square

3.7 Two-point Boundary-value Problems

Solving

$$-\frac{d^2 u(x)}{dx^2} = f(x), x \in [0, 1], \quad (24)$$

with boundary condition $u(0) = 0$ and $u(1) = 0$. This equation describe a steady state system, e.g., the temperature distribution of a rod with a heat source $f(x)$ and both ends fixed at 0°C .

Since a computer cannot solve a differential equation exactly, we have to approximate the differential equation with a difference equation. For that reason we can only accept a finite amount of information at n equally spaced points

$$u_1 := u(h), u_2 := u(2h), \dots, u_n := u(nh) \quad (25)$$

$$f_1 := f(h), f_2 := f(2h), \dots, f_n := f(nh) \quad (26)$$

where $h := \frac{1}{n}$. The boundary condition becomes $u_0 := 0$ and $u_{n+1} := 0$.

We approximate the second-order derivative by

$$\begin{aligned} -\frac{d^2u(x)}{dx^2} &\approx -\frac{u(x+h) - 2u(x) + u(x-h)}{h^2} \\ &= \frac{-u_{j+1} + u_j - u_{j-1}}{h^2}. \end{aligned} \quad (27)$$

Therefore, the differential equation $-\frac{d^2u(x)}{dx^2} = f(x)$ becomes

$$\mathbf{K}\mathbf{u} = \begin{bmatrix} 2 & -1 & & \\ -1 & 2 & \ddots & \\ & \ddots & \ddots & -1 \\ & & -1 & 2 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = h^2 \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = h^2 \mathbf{f}. \quad (28)$$

Lemma 26. The FLOPs for solving $\mathbf{K}\mathbf{f} = h^2\mathbf{f}$ is $T(n) \sim 3n$.

4 Theory: Eigenvalues and Eigenvectors

4.1 Eigenvalues and Eigenvectors

Definition 33 (Eigenvalue λ and Eigenvector \mathbf{x}). λ and $\mathbf{x} \neq \mathbf{0}$ are the eigenvalue and eigenvector of \mathbf{A} if $\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$.

Algorithm 14 (Solving Eigenvalues and Eigenvectors). $\mathbf{A}\mathbf{x} = \lambda\mathbf{x} \Rightarrow (\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}$. Since $\mathbf{x} \neq \mathbf{0}$, $\mathcal{N}(\mathbf{A} - \lambda\mathbf{I}) \neq \emptyset$, which has $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$. The algorithm is illustrated in Alg. 6. In practice, the best way to compute eigenvalues is to compute similar matrices $\mathbf{A}_1, \mathbf{A}_2, \dots$ that approach a triangular matrix.

Algorithm 6 Solve the eigenvalues and eigenvector for \mathbf{A} .

Input: $\mathbf{A} \in \mathbb{R}^{n \times n}$

Output: λ_i, \mathbf{x}_i

- 1: Solve $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$, which is a polynomial in λ of degree n , for eigenvalue λ .
 - 2: For each eigenvalue λ , solve $(\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}$ for eigenvector \mathbf{x} .
 - 3: **return** λ_i, \mathbf{x}_i
-

Definition 34 (Geometric Multiplicity (GM)). The number of independent eigenvectors for λ , which is $\dim \mathcal{N}(\mathbf{A} - \lambda\mathbf{I})$.

Definition 35 (Algebraic Multiplicity (AM)). The number of repetitions of λ among the eigenvalues. Look at the n roots of $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$.

Lemma 27. The followings are properties of eigenvalues and eigenvectors.

- For each eigenvalue, $GM \leq AM$. A matrix is diagonalizable iff every eigenvalue has $GM = AM$.
- Each eigenvalue has ≥ 1 eigenvector.
- All eigenvalues are different \Rightarrow all eigenvectors are independent, which means the matrix can be diagonalized.

- There is no connection between invertibility and diagonalizability. Invertibility is concerned with the eigenvalues ($\lambda = 0$ or $\lambda \neq 0$). Diagonalizability is concerned with the eigenvectors (too few or enough for \mathbf{S}).
- Suppose both \mathbf{A} and \mathbf{B} can be diagonalized, they share the same eigenvector matrix \mathbf{S} iff $\mathbf{AB} = \mathbf{BA}$.

4.2 Diagonalizable

Theorem 28 (Diagonalizable). If $\mathbf{A} \in \mathbb{R}^{n \times n}$ has n independent eigenvectors, \mathbf{A} is diagonalizable

$$\mathbf{A} = \mathbf{S}\mathbf{\Lambda}\mathbf{S}^{-1}, \quad (29)$$

where $\mathbf{S} := [\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_n]$ and $\mathbf{\Lambda} := \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$. In other words, \mathbf{A} is similar to $\mathbf{\Lambda}$.

Proof. $\mathbf{AS} = [\lambda_1\mathbf{x}_1 \ \lambda_2\mathbf{x}_2 \ \dots \ \lambda_n\mathbf{x}_n] = \mathbf{S}\mathbf{\Lambda}$. □

Definition 36 (Normal Matrix). A square matrix \mathbf{A} is normal when $\mathbf{A}^\top \mathbf{A} = \mathbf{A}\mathbf{A}^\top$. That includes symmetric, antisymmetric, and orthogonal matrices. In this case, $\sigma_i = |\lambda_i|$.

Lemma 29. The eigenvectors of \mathbf{A} is orthonormal when \mathbf{A} is normal.

Theorem 30 (Spectral Theorem). Every symmetric matrix \mathbf{A} has the factorization

$$\mathbf{A} = \mathbf{Q}\mathbf{\Lambda}\mathbf{Q}^\top = \sum_{i=1}^n \lambda_i \mathbf{x}_i \mathbf{x}_i^\top \quad (30)$$

Properties of eigenvalues and eigenvectors of special matrices are illustrated in Table 10.

5 Application: Solving Dynamic Problems

5.1 Solving Difference and Differential Equations

The algorithm for solving first-order difference and differential equations are illustrated in Alg. 7 and Alg. 8, respectively.

Algorithm 7 Solving $\mathbf{u}_{k+1} = \mathbf{A}\mathbf{u}_k$.

Input: $\mathbf{A} \in \mathbb{R}^{n \times n}, \mathbf{u}_0$

Output: \mathbf{u}_k

- 1: Diagonalize on $\mathbf{A} = \mathbf{S}\mathbf{\Lambda}\mathbf{S}^{-1}$.
 - 2: Solving $\mathbf{S}\mathbf{c} = \mathbf{u}_0$ to write \mathbf{u}_0 as a linear combination of eigenvectors.
 - 3: The solution $\mathbf{u}_k = \mathbf{A}^k \mathbf{u}_0 = \mathbf{S}\mathbf{\Lambda}^k \mathbf{S}^{-1} \mathbf{u}_0 = \mathbf{S}\mathbf{\Lambda}^k \mathbf{c} = \sum_{i=1}^n c_i \lambda_i^k \mathbf{x}_i$
 - 4: **return** \mathbf{u}_k
-

Algorithm 8 Solving $\frac{du(t)}{dt} = \mathbf{A}u(t)$, where \mathbf{A} is a constant coefficient matrix.

Input: $\mathbf{A} \in \mathbb{R}^{n \times n}, u(0)$

Output: $u(t)$

- 1: Diagonalize on $\mathbf{A} = \mathbf{S}\mathbf{\Lambda}\mathbf{S}^{-1}$.
 - 2: Solving $\mathbf{S}\mathbf{c} = u(0)$ to write $u(0)$ as a linear combination of eigenvectors.
 - 3: The solution $u(t) = \exp(\mathbf{A}t)u(0) = \mathbf{S}\exp(\mathbf{\Lambda}t)\mathbf{S}^{-1}u(0) = \mathbf{S}\exp(\mathbf{\Lambda}t)\mathbf{c} = \sum_{i=1}^n c_i \exp(\lambda_i t) \mathbf{x}_i$
 - 4: If two λ 's are equal, with only one eigenvector, another solution $t \exp(\lambda t) \mathbf{x}$ is needed.
 - 5: **return** $u(t)$
-

Example 1 (Fibonacci Numbers). Find the k -th Fibonacci number where the sequence is defined as $F_0 = 0, F_1 = 1$, and $F_{k+2} = F_{k+1} + F_k$.

Solution. Let $u_k := \begin{bmatrix} F_{k+1} \\ F_k \end{bmatrix}$, then $u_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $u_{k+1} = \mathbf{A}u_k := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} u_k$. $\lambda_1 = \frac{1+\sqrt{5}}{2}, \lambda_2 = \frac{1-\sqrt{5}}{2}$. $x_1 = \begin{bmatrix} \lambda_1 \\ 1 \end{bmatrix}, x_2 = \begin{bmatrix} \lambda_2 \\ 1 \end{bmatrix}$. $c = \frac{1}{\lambda_1 - \lambda_2} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$. $u_k = \frac{1}{\lambda_1 - \lambda_2} (\lambda_1^k x_1 - \lambda_2^k x_2)$. $F_k = \frac{1}{\sqrt{5}} (\lambda_1^k - \lambda_2^k) = \text{nearest integer to } \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k$.

Example 2 (Simple Harmonic Vibration). Solve $\frac{d^2 x(t)}{dt^2} + x(t) = 0$, where $x(0) = 1, \frac{dx(0)}{dt} = 0$. This is a $ma = -kx$ where $m = 1, k = 1$.

Solution. Let $u(t) := \begin{bmatrix} x \\ \frac{dx}{dt} \end{bmatrix}$, then $u(0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\frac{du}{dt} = \mathbf{A}u(t) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} u(t)$. $\lambda_1 = i, \lambda_2 = -i$. $x_1 = \begin{bmatrix} 1 \\ i \end{bmatrix}, x_2 = \begin{bmatrix} 1 \\ -i \end{bmatrix}$. $c = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. $u(t) = \frac{1}{2} (\exp(it)x_1 + \exp(-it)x_2)$. $x(t) = \frac{1}{2} (\exp(it) + \exp(-it)) = \cos t$.

Definition 37 (Markov Matrices). A $n \times n$ matrix is a Markov matrix if all entries are nonnegative and the each column of the matrix adds up to 1.

Lemma 31. A Markov matrix \mathbf{A} has the following properties

- $\lambda_1 = 1$ is an eigenvalue of \mathbf{A} .
- Its eigenvector x_1 is nonnegative, and it is steady state since $\mathbf{A}x_1 = x_1$.
- The other eigenvalues satisfy $|\lambda_i| \leq 1$.
- If \mathbf{A} or any power of \mathbf{A} has all positive entries, these other $|\lambda_i| < 1$. The solution $\mathbf{A}^k u_0$ approaches a multiple of x_1 , which is the steady state u_∞ .

Lemma 32. The difference equation $u_{k+1} = \mathbf{A}u_k$ is

- stable if $\forall i, |\lambda_i| < 1$.
- neutrally stable if $\exists i, |\lambda_i| = 1$, and all the other $|\lambda_i| < 1$.
- unstable if $\exists i, |\lambda_i| > 1$.

In the stable case, the powers \mathbf{A}^k approach zero and so does $u_k = \mathbf{A}^k u_0$.

Lemma 33. The differential equation $\frac{d}{dt}u(t) = \mathbf{A}u(t)$ is

- stable and $\exp \mathbf{A}t \rightarrow \mathbf{0}$ if $\forall i, \text{Re} \lambda_i < 0$.
- neutrally stable if $\exists i, \text{Re} \lambda_i = 0$, and all the other $\text{Re} \lambda_i < 0$.
- unstable and $\exp \mathbf{A}t$ is unbounded if $\exists i, \text{Re} \lambda_i > 0$.

5.2 Singular Value Decomposition

Theorem 34 (SVD Factorization). For matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$ with $r := \text{rank } \mathbf{A}$, choose $\mathbf{U} \in \mathbb{R}^{m \times m}$ to contain orthonormal eigenvectors of $\mathbf{A}\mathbf{A}^\top$, and $\mathbf{V} \in \mathbb{R}^{n \times n}$ to contain orthonormal eigenvectors of $\mathbf{A}^\top \mathbf{A}$. The shared eigenvalues are $\sigma_1^2, \sigma_2^2, \dots, \sigma_r^2$. Then

$$\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^\top = \sum_{i=1}^r \sigma_i u_i v_i^\top. \quad (31)$$

\mathbf{U} and \mathbf{V} satisfy the followings.

- The first r columns of \mathbf{U} contains orthonormal bases for $C(\mathbf{A})$.
- The last $m-r$ columns of \mathbf{U} contains orthonormal bases for $\mathcal{N}(\mathbf{A}^\top)$.
- The first r columns of \mathbf{V} contains orthonormal bases for $C(\mathbf{A}^\top)$.
- The last $n-r$ columns of \mathbf{V} contains orthonormal bases for $\mathcal{N}(\mathbf{A})$.

Proof. Start from $\mathbf{A}^\top \mathbf{A} v_i = \sigma_i^2 v_i$. Multiply both sides by \mathbf{A} gives $\mathbf{A}\mathbf{A}^\top (\mathbf{A} v_i) = \sigma_i^2 (\mathbf{A} v_i)$, which shows that $\mathbf{A} v_i$ is an eigenvector of $\mathbf{A}\mathbf{A}^\top$ with shared eigenvalue σ_i^2 . Since $\|\mathbf{A} v_i\| = \sqrt{v_i^\top \mathbf{A}^\top \mathbf{A} v_i} = \sqrt{\sigma_i^2 v_i^\top v_i} = \sigma_i$, we denote $u_i := \frac{\mathbf{A} v_i}{\|\mathbf{A} v_i\|} = \frac{\mathbf{A} v_i}{\sigma_i}$, namely, $\mathbf{A} v_i = \sigma_i u_i$. It shows column by column that $\mathbf{A}\mathbf{V} = \mathbf{U}\mathbf{\Sigma}$. Since \mathbf{V} is orthogonal, $\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^\top$. \square

Lemma 35. The largest singular value dominates all eigenvalues and all entries of \mathbf{A} . That is, $\sigma_1 \geq \max_i |\lambda_i|$ and $\sigma_1 \geq \max_{i,j} |a_{ij}|$.

Lemma 36. For a square matrix \mathbf{A} , spectral factorization and SVD factorization give the same result when \mathbf{A} is PSD.

Proof. We need orthonormal eigenvectors (\mathbf{A} should be symmetric), and nonnegative eigenvalues (\mathbf{A} is PSD). \square

5.3 Leontief's Input-output Model

Leontief divided the US economy into n sectors that produce goods or services (e.g., coal, automotive, and communication), and another sectors that only consume goods or services (e.g., consumer and government).

Table 6: Comparison of PD and PSD matrices.

	PD matrices	PSD matrices
$\mathbf{x}^\top \mathbf{A} \mathbf{x}$, if $\mathbf{x} \neq \mathbf{0}$	> 0	≥ 0
$\mathbf{A}^\top \mathbf{A}$	If \mathbf{A} has independent columns	If \mathbf{A} has dependent columns
$\mathbf{A}^\top \mathbf{C} \mathbf{A}$ (\mathbf{C} is diagonal with positive elements)	If \mathbf{A} has independent columns	If \mathbf{A} has dependent columns
Upper left determinants	All positive	All nonnegative
Pivots	All positive	All nonnegative
Eigenvalues	All Postive	All nonnegative

- *Production vector* $\mathbf{x} \in \mathbb{R}^n$. Ouput of each producer for one year.
- *Final demand vector* $\mathbf{b} \in \mathbb{R}^n$. Demand for each producer by the consumer for a year.
- *Intermediate demand vector* $\mathbf{u} := \mathbf{A} \mathbf{x} \in \mathbb{R}^n$. Demand for each producer by the producer for a year. $\mathbf{A} \in \mathbb{R}^{n \times n}$ is the *consumption matrix*.

Theorem 37 (Leontief Input-output Model). *When there is a production level \mathbf{x} such that the amounts produced will exactly balance the total demand for that production*

$$\mathbf{x} = \mathbf{A} \mathbf{x} + \mathbf{b}. \quad (32)$$

If \mathbf{A} and \mathbf{b} have nonnegative entries and the largest eigenvalue of \mathbf{A} is less than 1, then the solution exists and has nonnegative entires

$$\mathbf{x} = (\mathbf{I} - \mathbf{A})^{-1} \mathbf{b} = \left(\mathbf{I} + \sum_{k=1}^{\infty} \mathbf{A}^k \right) \mathbf{b}. \quad (33)$$

6 Theory: Positive Definite Matrices and Optimizations

In many cases, the sign of eigenvalues are crucial.

6.1 Positive Definite Matrices

The comparison of PD and PSD matrices are illustrated in Table 6.

Algorithm 15 (Determine Whether \mathbf{A} is PD). *Try to factor $\mathbf{A} = \mathbf{R}^\top \mathbf{R}$ where \mathbf{R} is upper triangular with positive diagonal entries (i.e., Cholesky factorization).*

Lemma 38. *For symmetric matrices, the pivots and the eigenvalues have the same signs.*

Lemma 39. $\mathbf{x}^\top \mathbf{A} \mathbf{x} = 1$ *is an ellipsoid in n dimensions. The axes of the ellipsoid point toward the eigenvector of \mathbf{A} .*

6.2 Unconstrained Optimization

The goal is to solve

$$\arg \min_{\mathbf{u}} f(\mathbf{u}). \quad (34)$$

Definition 38 (Stationary Point). Point where $\frac{\partial f}{\partial \mathbf{u}} = \mathbf{0}$. Such point can be a local minimum, a local maximum, or a saddle point.

Lemma 40. $f(\mathbf{u})$ *has a local minimum when $\frac{\partial^2 f}{\partial \mathbf{u}^2}$ is PD. Similarly, $f(\mathbf{u})$ has a local maximum when $\frac{\partial^2 f}{\partial \mathbf{u}^2}$ is ND. If some eigenvalues are postive and some are negative, $f(\mathbf{u})$ has a saddle point. If $\frac{\partial^2 f}{\partial \mathbf{u}^2}$ has eigenvalue 0, the test is inconclusive.*

In some cases, we can directly get the stationary point by solving $\frac{\partial f}{\partial \mathbf{u}} = \mathbf{0}$. In other cases, we iteratively approach to the stationary point.

Algorithm 16 (Gradient Descent). $\mathbf{u} \leftarrow \mathbf{u} - \eta \frac{\partial f}{\partial \mathbf{u}}$.

Algorithm 17 (Newton's Method). $\mathbf{u} \leftarrow \mathbf{u} - \left(\frac{\partial^2 f}{\partial \mathbf{u}^2} \right)^{-1} \frac{\partial f}{\partial \mathbf{u}}$.

Lemma 41 (Taylor Series).

$$f(\mathbf{u}) \approx f(\mathbf{u}_0) + (\mathbf{u} - \mathbf{u}_0)^\top \frac{\partial f}{\partial \mathbf{u}} \Big|_{\mathbf{u}_0} + \frac{1}{2} (\mathbf{u} - \mathbf{u}_0)^\top \frac{\partial^2 f}{\partial \mathbf{u}^2} \Big|_{\mathbf{u}_0} (\mathbf{u} - \mathbf{u}_0). \quad (35)$$

6.3 Constrained Optimization

Construct the Lagrange function is an important method for solving constrained optimization problems.

Definition 39 (Lagrange Function). For a constrained optimization problem

$$\begin{aligned} \min_{\mathbf{u}} \quad & f(\mathbf{u}) \\ \text{s. t.} \quad & g_i(\mathbf{u}) \leq 0, \quad i = 1, 2, \dots, m, \\ & h_j(\mathbf{u}) = 0, \quad j = 1, 2, \dots, n, \end{aligned} \quad (36)$$

The Lagrange function is defined as

$$\mathcal{L}(\mathbf{u}, \boldsymbol{\alpha}, \boldsymbol{\beta}) := f(\mathbf{u}) + \sum_{i=1}^m \alpha_i g_i(\mathbf{u}) + \sum_{j=1}^n \beta_j h_j(\mathbf{u}), \quad (37)$$

where $\alpha_i \geq 0$.

Lemma 42. *The optimization problem of 36 is equivalent to*

$$\begin{aligned} \min_{\mathbf{u}} \max_{\boldsymbol{\alpha}, \boldsymbol{\beta}} \quad & \mathcal{L}(\mathbf{u}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \\ \text{s. t.} \quad & \alpha_i \geq 0, \quad i = 1, 2, \dots, m. \end{aligned} \quad (38)$$

Proof.

$$\begin{aligned}
& \min_u \max_{\alpha, \beta} \mathcal{L}(\mathbf{u}, \alpha, \beta) \\
&= \min_u \left(f(\mathbf{u}) + \max_{\alpha, \beta} \left(\sum_{i=1}^m \alpha_i g_i(\mathbf{u}) + \sum_{j=1}^n \beta_j h_j(\mathbf{u}) \right) \right) \\
&= \min_u \left(f(\mathbf{u}) + \begin{cases} 0 & \text{if } \mathbf{u} \text{ feasible;} \\ \infty & \text{otherwise} \end{cases} \right) \\
&= \min_u f(\mathbf{u}), \text{ and } \mathbf{u} \text{ feasible,} \quad (39)
\end{aligned}$$

When g_i is infeasible $g_i(\mathbf{u}) > 0$, we can let $\alpha_i = \infty$, such that $\alpha_i g_i(\mathbf{u}) = \infty$; When h_j is infeasible $h_j(\mathbf{u}) \neq 0$, we can let $\beta_j = \text{sign}(h_j(\mathbf{u}))\infty$, such that $\beta_j h_j(\mathbf{u}) = \infty$. When \mathbf{u} feasible, since $\alpha_i \geq 0$, $g_i(\mathbf{u}) \leq 0$, $\alpha_i g_i(\mathbf{u}) \leq 0$. Therefore, the maximum of $\alpha_i g_i(\mathbf{u})$ is 0. \square

Corollary 43 (KKT condition). *The optimization problem of 38 should satisfy the followings at the optimum.*

- *Primal feasible:* $g_i(\mathbf{u}) \leq 0$, $h_i(\mathbf{u}) = 0$;
- *Dual feasible:* $\alpha_i \geq 0$;
- *Complementary slackness:* $\alpha_i g_i(\mathbf{u}) = 0$.

Definition 40 (Dual problem). The dual problem of 36 is

$$\begin{aligned}
& \max_{\alpha, \beta} \min_u \mathcal{L}(\mathbf{u}, \alpha, \beta) \quad (40) \\
& \text{s. t.} \quad \alpha_i \geq 0, \quad i = 1, 2, \dots, m.
\end{aligned}$$

Lemma 44. *Dual problem is a lower bound of the primal problem.*

$$\max_{\alpha, \beta} \min_u \mathcal{L}(\mathbf{u}, \alpha, \beta) \leq \min_u \max_{\alpha, \beta} \mathcal{L}(\mathbf{u}, \alpha, \beta). \quad (41)$$

Proof. For any (α', β') , $\min_u \mathcal{L}(\mathbf{u}, \alpha', \beta') \leq \min_u \max_{\alpha, \beta} \mathcal{L}(\mathbf{u}, \alpha, \beta)$. When $(\alpha', \beta') = \max_{\alpha', \beta'} \min_u \mathcal{L}(\mathbf{u}, \alpha', \beta')$, it still holds true, i.e., $\max_{\alpha', \beta'} \min_u \mathcal{L}(\mathbf{u}, \alpha', \beta') \leq \min_u \max_{\alpha, \beta} \mathcal{L}(\mathbf{u}, \alpha, \beta)$. \square

Definition 41 (Convex Function). A function f is convex if

$$\forall \alpha \in [0, 1]. f(\alpha \mathbf{x} + (1 - \alpha) \mathbf{y}) \leq \alpha f(\mathbf{x}) + (1 - \alpha) f(\mathbf{y}), \quad (42)$$

which means that if we pick two points on the graph of a convex function and draw a straight line segment between them, the portion of the function between these two points will lie below this straight line.

Lemma 45. *A function f is convex if every point on the tangent line will lie below the corresponding point on f*
 $f(\mathbf{y}) \geq f(\mathbf{x}) + (\mathbf{y} - \mathbf{x})^\top \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}$ or $\frac{\partial^2 f}{\partial \mathbf{x}^2}$ is PSD.

Definition 42 (Affine Function). Function f in the form $f(\mathbf{x}) = \mathbf{c}^\top \mathbf{x} + d$.

Lemma 46 (Slater Condition). *When primal problem is convex, i.e., f and g_i are convex, h_j is affine, and there exists at least one point in the feasible region to let the inequality strictly holds true, the dual problem is equivalent to the primal problem.*

Proof. The proof is out of the range of this note. Please refer to [2] if you are interested. \square

7 Application: Solving Optimization Problems

7.1 Remove Non-differentiability

Lemma 47. *The optimization problem*

$$\arg \min_{\mathbf{u}} |f(\mathbf{u})| \quad (43)$$

is equivalent to

$$\begin{aligned}
& \arg \min_{\mathbf{u}, x} x \quad (44) \\
& \text{s. t.} \quad f(\mathbf{u}) - x \leq 0 \\
& \quad \quad -f(\mathbf{u}) - x \leq 0.
\end{aligned}$$

Proof. $\arg \min_{\mathbf{u}} |f(\mathbf{u})|$ is equivalent to $\arg \min_{\mathbf{u}} \max(f(\mathbf{u}), -f(\mathbf{u}))$. Let x be an upper bound of $\max(f(\mathbf{u}), -f(\mathbf{u}))$. \square

7.2 Linear Programming

7.3 Support Vector Machine

Definition 43 (Support Vector Machine (SVM)). Given a set of training examples $\{(\mathbf{x}_i, y_i)\}_{i=1}^m$, the goal of SVM is to find a hyperplane to separate examples with different classes, and that hyperplane is farthest from training examples.

$$\begin{aligned}
& \arg \max_{\mathbf{w}, b} \min_i \frac{2}{\|\mathbf{w}\|} |\mathbf{w}^\top \mathbf{x}_i + b| \quad (45) \\
& \text{s. t.} \quad y_i(\mathbf{w}^\top \mathbf{x}_i + b) > 0, \quad i = 1, 2, \dots, m.
\end{aligned}$$

Since scaling of (\mathbf{w}, b) does not change the solution, for simplicity, we add a constraint that

$$\min_i |\mathbf{w}^\top \mathbf{x}_i + b| = 1. \quad (46)$$

Theorem 48 (Standard Form of SVM). *The optimization problem of SVM is equivalent to*

$$\begin{aligned}
& \arg \min_{\mathbf{w}, b} \frac{1}{2} \|\mathbf{w}\|^2 \quad (47) \\
& \text{s. t.} \quad y_i(\mathbf{w}^\top \mathbf{x}_i + b) \geq 1, \quad i = 1, 2, \dots, m.
\end{aligned}$$

Proof. By contradiction. Suppose the equality of the constraint does not hold at the optimal (\mathbf{w}^*, b^*) , i.e., $\min_i y_i(\mathbf{w}^{*\top} \mathbf{x}_i + b^*) > 1$. There exists $(r\mathbf{w}, rb)$ where $0 < r < 1$ such that $\min_i y_i((r\mathbf{w})^\top \mathbf{x}_i + rb) = 1$, and $\frac{1}{2}\|r\mathbf{w}\|^2 < \frac{1}{2}\|\mathbf{w}\|^2$. That implies (\mathbf{w}^*, b^*) is not an optimal, which contradicts to the assumption. Therefore, Eqn. 47 is equivalent to

$$\begin{aligned} \arg \min_{\mathbf{w}, b} \quad & \frac{1}{2} \mathbf{w}^\top \mathbf{w} \\ \text{s. t.} \quad & \min_i y_i(\mathbf{w}^\top \mathbf{x}_i + b) = 1. \end{aligned} \quad (48)$$

The objective function is equivalent to

$$\begin{aligned} \arg \min_{\mathbf{w}, b} \frac{1}{2} \mathbf{w}^\top \mathbf{w} &= \arg \max_{\mathbf{w}, b} \frac{2}{\|\mathbf{w}\|} \cdot 1 \\ &= \arg \max_{\mathbf{w}, b} \min_i \frac{2}{\|\mathbf{w}\|} y_i(\mathbf{w}^\top \mathbf{x}_i + b) \\ &= \arg \max_{\mathbf{w}, b} \min_i \frac{2}{\|\mathbf{w}\|} |\mathbf{w}^\top \mathbf{x}_i + b|. \end{aligned} \quad (49)$$

□

Theorem 49 (Dual problem of SVM). *The dual problem of SVM is*

$$\begin{aligned} \arg \min_{\alpha} \quad & \frac{1}{2} \sum_{i=1}^m \sum_{j=1}^m \alpha_i \alpha_j y_i y_j \mathbf{x}_i^\top \mathbf{x}_j - \sum_{i=1}^m \alpha_i \\ \text{s. t.} \quad & \sum_{i=1}^m \alpha_i y_i = 0, \\ & \alpha_i \geq 0, \quad i = 1, 2, \dots, m. \end{aligned} \quad (50)$$

Proof. The Lagrange function is

$$\mathcal{L}(\mathbf{w}, b, \alpha) := \frac{1}{2} \mathbf{w}^\top \mathbf{w} + \sum_{i=1}^m \alpha_i (1 - y_i(\mathbf{w}^\top \mathbf{x}_i + b)). \quad (51)$$

Its dual problem is

$$\begin{aligned} \arg \max_{\alpha} \min_{\mathbf{w}, b} \quad & \frac{1}{2} \mathbf{w}^\top \mathbf{w} + \sum_{i=1}^m \alpha_i (1 - y_i(\mathbf{w}^\top \mathbf{x}_i + b)) \\ \text{s. t.} \quad & \alpha_i \geq 0, \quad i = 1, 2, \dots, m. \end{aligned} \quad (52)$$

Since the inner optimization problem is unconstrained, we can get the optimal by

$$\frac{\partial \mathcal{L}}{\partial \mathbf{w}} = \mathbf{0} \Rightarrow \mathbf{w} = \sum_{i=1}^m \alpha_i y_i \mathbf{x}_i, \quad (53)$$

$$\frac{\partial \mathcal{L}}{\partial b} = 0 \Rightarrow \sum_{i=1}^m \alpha_i y_i = 0. \quad (54)$$

Substitute them into Eqn. 52 gives Eqn. .

□

Table 7: Analogy of real-valued functions with linear transformations.

	Function	Linear transformation
Definition	$f : \mathbb{R} \rightarrow \mathbb{R}$	$T : \mathbb{R}^n \rightarrow \mathbb{R}^m$
Domain, Codomain	\mathbb{R}, \mathbb{R}	$\mathbb{R}^n, \mathbb{R}^m$
Image of x	$f(x)$	$T(\mathbf{x}) := \mathbf{A}\mathbf{x}$
Range	$\{y \mid \exists x. y = f(x)\}$	$C(\mathbf{A})$
Zero	$\{x \mid f(x) = 0\}$	$\mathcal{N}(\mathbf{A})$
Inverse	$f^{-1}(y)$	$T^{-1}(\mathbf{y}) = \mathbf{A}^{-1}\mathbf{y}$
Decomposition	$g \circ f = g(f(x))$	$T_B \circ T_A = \mathbf{B}\mathbf{A}\mathbf{x}$

Table 8: Terminologies of linear transformation $T(\mathbf{x}) = \mathbf{A}\mathbf{x}$.

Terminology	Meaning	Property
Onto (surjective)	≥ 1 arrow in	$C(\mathbf{A}) = \mathbb{R}^m$.
One-to-one (injective)	≤ 1 arrow in	$\mathcal{N}(\mathbf{A}) = \mathbf{0}$

Definition 44 (Support Vector). Example with dual variable $\alpha_i > 0$, which has $y_i(\mathbf{w}^\top \mathbf{x}_i + b) = 1$.

Lemma 50. *The hypothesis function of linear SVM is*

$$h(\mathbf{x}) = \text{sign} \left(\sum_{i \in SV} \alpha_i y_i \mathbf{x}_i^\top \mathbf{x} + b \right). \quad (55)$$

8 Theory: Linear Transformations

8.1 Linear Transformations

Definition 45 (Transformation T). A transformation $T : \mathbb{R}^n \rightarrow \mathbb{R}^m$ is a rule that assigns to each vector $\mathbf{x} \in \mathbb{R}^n$ a vector $T(\mathbf{x}) \in \mathbb{R}^m$.

Definition 46 (Linear Transformation). A transformation T is linear if $T(c_1 \mathbf{v}_1 + c_2 \mathbf{v}_2) = c_1 T(\mathbf{v}_1) + c_2 T(\mathbf{v}_2)$. It is always the case that $T(\mathbf{0}) = \mathbf{0}$. The comparison between real-valued functions and linear transformations is illustrated in Table 7 and terminologies of transformations are illustrated in Table 8.

Theorem 51 (Standard Matrix for a Linear Transformation). *Let $T : \mathbb{R}^n \rightarrow \mathbb{R}^m$ be a linear transformation. There exists a unique matrix $\mathbf{A} := [T(\mathbf{e}_1) \ T(\mathbf{e}_2) \ \dots \ T(\mathbf{e}_n)] \in \mathbb{R}^{m \times n}$ such that $T(\mathbf{x}) = \mathbf{A}\mathbf{x}$, where \mathbf{e}_j is the j -th column of $\mathbf{I} \in \mathbb{R}^{n \times n}$.*

Proof. $T(\mathbf{x}) = T\left(\sum_{j=1}^n x_j \mathbf{e}_j\right) = \sum_{j=1}^n x_j T(\mathbf{e}_j) = \mathbf{A}\mathbf{x}$. □

Lemma 52 (Genral Matrix for a Linear Transformation). *Let $T : \mathcal{V} \rightarrow \mathcal{U}$ be a linear transformation, where $\mathcal{V} \in \mathbb{R}^{n \times n}$ is the input basis and $\mathcal{U} \in \mathbb{R}^{m \times m}$ is the output basis. There exists a unique matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$ that gives the coordinate*

$T(\mathbf{c}) = \mathbf{A}\mathbf{c}$ in the output space when the coordinate of input space is \mathbf{c} . The j -th column of \mathbf{A} is found by solving $T(\mathbf{v}_j) = \mathbf{U}\mathbf{a}_j$.

8.2 Identity Transformations = Change of Basis

Definition 47 (Coordinate). The coordinate of a vector $\mathbf{x} \in \mathbb{R}^n$ relative to the bases matrix $\mathbf{W} \in \mathbb{R}^{n \times n}$ is the coefficient \mathbf{c} such that $\mathbf{x} = \mathbf{W}\mathbf{c}$, or equivalently $\mathbf{c} = \mathbf{W}^{-1}\mathbf{x}$.

Example 3 (Wavelet Transform). Wavelets are little waves. They have different length and they localized at different places. The basis matrix is

$$\mathbf{W} := \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & -1 & 0 & -1 \end{bmatrix}. \quad (56)$$

Those bases are orthogonal. The wavelet transform finds the coefficients \mathbf{c} when the input signal \mathbf{x} is expressed in the wavelet basis $\mathbf{x} = \mathbf{W}\mathbf{c}$.

Example 4 (Discrete Fourier Transform). The Fourier transform decomposes the signal into waves at equally spaced frequencies. The basis matrix is

$$\mathbf{F} := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & (i^2)^2 & (i^3)^2 \\ 1 & i^3 & (i^2)^3 & (i^3)^3 \end{bmatrix}. \quad (57)$$

Those bases are orthogonal. The discrete Fourier transform finds the coefficients \mathbf{c} when the input signal \mathbf{x} is expressed in the Fourier basis $\mathbf{x} = \mathbf{F}\mathbf{c}$.

Lemma 53 (Change of Basis). Suppose we want to change the basis from $\mathbf{V} := [\mathbf{v}_1 \ \mathbf{v}_2 \ \dots \ \mathbf{v}_n]$ to $\mathbf{U} := [\mathbf{u}_1 \ \mathbf{u}_2 \ \dots \ \mathbf{u}_n]$. The coordinate of a vector \mathbf{x} is \mathbf{c} in \mathbf{V} , and is \mathbf{b} in \mathbf{U} . Then $\mathbf{b} = \mathbf{U}^{-1}\mathbf{V}\mathbf{c}$, where $\mathbf{A} := \mathbf{U}^{-1}\mathbf{V}$ is called the change of basis matrix.

Proof. $\mathbf{x} = \mathbf{V}\mathbf{c} = \mathbf{U}\mathbf{b} \Rightarrow \mathbf{b} = \mathbf{U}^{-1}\mathbf{V}\mathbf{c}$. \square

Algorithm 18 (Solving the Change of Basis Matrix). Perform elementary row operations on $[\mathbf{U} \ \mathbf{V}]$ to $[\mathbf{I} \ \mathbf{A}]$. $T(n) \sim n^3$.

Example 5 (Diagonalization). $T(\mathbf{x}) := \mathbf{A}\mathbf{x} = \mathbf{S}\mathbf{\Lambda}\mathbf{S}^{-1}\mathbf{x}$ defines a linear transformation which changes the basis from \mathbf{I} to \mathbf{S} , then transform \mathbf{x} in space of \mathbf{S} , and last changes the basis from \mathbf{S} back to \mathbf{I} .

Example 6 (SVD Factorization). $T(\mathbf{x}) := \mathbf{A}\mathbf{x} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T\mathbf{x}$ defines a linear transformation which changes the basis from \mathbf{I} to \mathbf{V} , then transform \mathbf{x} from space \mathbf{V} to space \mathbf{U} , and last changes the basis from \mathbf{U} back to \mathbf{I} .

Table 9: Transformation using homogeneous coordinates.

Transformation	Result
Scaling	$\begin{bmatrix} c_x & 0 & 0 \\ 0 & c_y & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} c_x x \\ c_y y \\ 1 \end{bmatrix}$
Translation	$\begin{bmatrix} 1 & 0 & x_0 \\ 0 & 1 & y_0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x + x_0 \\ y + y_0 \\ 1 \end{bmatrix}$
Reflection	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} y \\ x \\ 1 \end{bmatrix}$
Clockwise rotation	$\begin{bmatrix} \cos \alpha & -\sin \alpha & 0 \\ \sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$

9 Applications: Linear Transformations

9.1 Computer Graphics

Definition 48 (Homogeneous Coordinates). Each point

$\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ can be identified with the point $\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \in \mathbb{R}^3$. Homogeneous coordinates can be transformed via multiplication by

3×3 matrices, as illustrated in Table 9. By analogy, each

point $\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3$ can be identified with the point $\begin{bmatrix} x \\ y \\ z \\ 1 \end{bmatrix} \in \mathbb{R}^4$.

Theorem 54 (Perspective projections). A 3D object is represented on the 2D computer screen by projecting the object onto a viewing plane at $z = 0$. Suppose the eye of a viewer is

at the point $\begin{bmatrix} 0 \\ 0 \\ d \end{bmatrix}$. A perspective projection maps each point

$\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ onto an image point $\begin{bmatrix} x_p \\ y_p \\ 0 \end{bmatrix}$ such that those two point and the eye position (center of projection) are on a line.

$$x_p = \frac{x}{1 - \frac{z}{d}}, \quad y_p = \frac{y}{1 - \frac{z}{d}}. \quad (58)$$

9.2 Principle Component Analysis

Definition 49 (Principle Component Analysis, PCA). Given a set of instances $\{\mathbf{x}_i\}_{i=1}^m$ with empirical mean $\boldsymbol{\mu} \in \mathbb{R}^d$ and empirical covariance $\boldsymbol{\Sigma} \in \mathbb{R}^{d \times d}$, PCA wants to find a set of orthonormal bases $\mathbf{W} := [\mathbf{w}_1 \ \mathbf{w}_2 \ \dots \ \mathbf{w}_d]$ such that the sum of variance of the projected data along each component

Table 10: Properties of eigenvalues and eigenvectors of special matrices.

Matrix	Eigenvalues	Eigenvectors
Symmetric $\mathbf{A}^\top = \mathbf{A}$	All real	Orthnormal
Anti-symmetric $\mathbf{A}^\top = -\mathbf{A}$	All imaginary	Orthnormal
Orthogonal $\mathbf{Q}^{-1} = \mathbf{Q}^\top$	All $ \lambda = 1$	Orthnormal
PD	All $\lambda > 0$	Orthnormal
PSD	All $\lambda \geq 0$	Orthnormal
Diagonalizable $\mathbf{A} = \mathbf{S}\mathbf{\Lambda}\mathbf{S}^{-1}$	diag $\mathbf{\Lambda}$	Columns of \mathbf{S} are independent
Rectangular $\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^\top$	rank $\mathbf{A} = \text{rank } \mathbf{\Sigma}$	Eigenvectors of $\mathbf{A}^\top \mathbf{A}$, $\mathbf{A}\mathbf{A}^\top$ in \mathbf{V} , \mathbf{U}
Stable powers $\mathbf{A}^n \rightarrow \mathbf{0}$	All $ \lambda < 1$	Any
Markov $A_{ij} > 0$, $\sum_{i=1}^n A_{ij} = 1$	$\max_i \lambda_i = 1$	Steady state $\mathbf{x} > 0$
Stable exponential $\exp \mathbf{A} t \rightarrow 0$	All $\text{Re } \lambda < 0$	Any
Projection $\mathbf{P} = \mathbf{P}^2 = \mathbf{P}^\top$	1, 0	$\mathcal{C}(\mathbf{P})$, $\mathcal{N}(\mathbf{P})$
Rank-1 $\mathbf{u}\mathbf{u}^\top$	$\mathbf{v}^\top \mathbf{u}, 0, \dots, 0$	\mathbf{u} , whole plane \mathbf{v}^\perp
Reflection $\mathbf{I} - 2\mathbf{e}\mathbf{e}^\top$	$-1, 1, \dots, 1$	\mathbf{e} , whole plane \mathbf{e}^\perp
Plane rotation	$\exp(i\theta), \exp(-i\theta)$	$[1 \ i]^\top, [1 \ -i]^\top$
Cyclic permutation: row 1 of \mathbf{I} last	$\lambda_k = \exp \frac{2\pi i k}{n}$	$\mathbf{x}_k = [1 \ \lambda_k \ \dots \ \lambda_k^{n-1}]^\top$
Tridiagonal: -1, 2, -1 on diagonals	$\lambda_k = 2 - 2 \cos \frac{k\pi}{n+1}$	$\mathbf{x}_k = \left[\sin \frac{k\pi}{n+1} \ \sin \frac{2k\pi}{n+1} \ \dots \right]^\top$

is maximized.

$$\begin{aligned} \arg \max_{\mathbf{W}} \quad & \text{tr cov } \mathbf{W}^\top (\mathbf{x} - \boldsymbol{\mu}) \\ \text{s. t.} \quad & \mathbf{W}^\top \mathbf{W} = \mathbf{I}. \end{aligned} \quad (59)$$

Theorem 55. *The optimum \mathbf{W} to Eqn. 61 is the top d' eigenvectors of $\boldsymbol{\Sigma}$.*

Proof. Since $\mathbb{E}[\mathbf{W}^\top (\mathbf{x} - \boldsymbol{\mu})] = \mathbf{W}^\top \mathbb{E}[\mathbf{x} - \boldsymbol{\mu}] = \mathbf{0}$,

$$\begin{aligned} \text{tr cov } \mathbf{W}^\top (\mathbf{x} - \boldsymbol{\mu}) &= \text{tr } \mathbb{E}[(\mathbf{W}^\top (\mathbf{x} - \boldsymbol{\mu}) - \mathbf{0})(\mathbf{W}^\top (\mathbf{x} - \boldsymbol{\mu}) - \mathbf{0})^\top] \\ &= \text{tr } \mathbf{W}^\top \mathbb{E}[(\mathbf{x} - \boldsymbol{\mu})(\mathbf{x} - \boldsymbol{\mu})^\top] \mathbf{W} \\ &= \text{tr } \mathbf{W}^\top \boldsymbol{\Sigma} \mathbf{W}. \end{aligned} \quad (60)$$

The optimization problem is equivalent to

$$\begin{aligned} \arg \min_{\mathbf{W}} \quad & -\text{tr } \mathbf{W}^\top \boldsymbol{\Sigma} \mathbf{W} \\ \text{s. t.} \quad & \mathbf{W}^\top \mathbf{W} = \mathbf{I}. \end{aligned} \quad (61)$$

The Lagrange function is

$$\begin{aligned} \mathcal{L}(\mathbf{W}, \mathbf{B}) &:= -\text{tr } \mathbf{W}^\top \boldsymbol{\Sigma} \mathbf{W} + (\text{vec } \mathbf{B})^\top (\text{vec}(\mathbf{W}^\top \mathbf{W} - \mathbf{I})) \\ &= -\text{tr } \mathbf{W}^\top \boldsymbol{\Sigma} \mathbf{W} + \text{tr } \mathbf{B}^\top (\mathbf{W}^\top \mathbf{W} - \mathbf{I}). \end{aligned} \quad (62)$$

We can get the optimal by

$$\frac{\partial \mathcal{L}}{\partial \mathbf{W}} = \mathbf{0} \Rightarrow \boldsymbol{\Sigma} \mathbf{W} = \mathbf{W} \mathbf{B}. \quad (63)$$

□

Corollary 56. $\hat{\mathbf{x}} := \mathbf{Q}^\top (\mathbf{x} - \boldsymbol{\mu})$ has $\mathbb{E}[\hat{\mathbf{x}}] = \mathbf{0}$ and $\text{cov } \hat{\mathbf{x}} = \mathbf{\Lambda}$, where $\boldsymbol{\Sigma} = \mathbf{Q}\mathbf{\Lambda}\mathbf{Q}^\top$.

Definition 50 (PCA Whitening). $\hat{\mathbf{x}} := \mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{Q}^\top (\mathbf{x} - \boldsymbol{\mu})$ has $\mathbb{E}[\hat{\mathbf{x}}] = \mathbf{0}$ and $\text{cov } \hat{\mathbf{x}} = \mathbf{I}$.

Definition 51 (ZCA Whitening). $\hat{\mathbf{x}} := \mathbf{Q}\mathbf{\Lambda}^{-\frac{1}{2}} \mathbf{Q}^\top (\mathbf{x} - \boldsymbol{\mu})$ has $\mathbb{E}[\hat{\mathbf{x}}] = \mathbf{0}$ and $\text{cov } \hat{\mathbf{x}} = \mathbf{I}$.

10 Appendix

Lemma 57 (Sum of Series).

$$\sum_{i=1}^n i = \frac{n(n+1)}{2} \sim \frac{1}{2}n^2, \quad (64)$$

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6} \sim \frac{1}{3}n^3. \quad (65)$$

References

- [1] S. Axler. *Linear algebra done right*. Springer, 1997. 1
- [2] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge University Press, 2004. 12
- [3] S. Boyd and L. Vandenberghe. *Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares*. Cambridge University Press, 2018. 1
- [4] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, 1990. 1
- [5] D. C. Lay, S. R. Lay, and J. J. McDonald. *Linear Algebra and Its Applications (Fifth Edition)*. Pearson, 2014. 1
- [6] K. B. Petersen, M. S. Pedersen, et al. *The matrix cookbook*. Technical University of Denmark, 2008. 1
- [7] G. Strang. *Linear algebra and its applications (Fourth Edition)*. Academic Press, 2006. 1

- [8] G. Strang. *Computational science and engineering*. Wellesley-Cambridge Press, 2007. [1](#)
- [9] G. Strang. *Introduction to linear algebra (Fourth Edition)*. Wellesley-Cambridge Press, 2009. [1](#)