Engineering Fundamentals

Major Contributors
Jean-Francois Chamberland and Henry D. Pfister

September 12, 2023
Contents

1 Logic and Set Theory ........................................... 1
   1.1 Statements .................................................. 2
   1.2 Relations between Statements ............................. 6
      1.2.1 Fallacious Arguments ................................ 9
      1.2.2 Quantifiers ............................................ 10
   1.3 Strategies for Proofs ....................................... 12
   1.4 Set Theory .................................................. 14
   1.5 Functions ................................................... 19

2 Metric Spaces and Topology ....................................... 23
   2.1 Metric Spaces ................................................ 24
      2.1.1 Convergence .......................................... 26
      2.1.2 Metric Topology ....................................... 27
      2.1.3 Continuity ............................................. 29
      2.1.4 Properties of the Real Numbers ..................... 30
      2.1.5 Sequences of Functions ............................... 32
      2.1.6 Completeness ......................................... 33
      2.1.7 Compactness ......................................... 37
      2.2 General Topology* ....................................... 38
         2.2.1 Closed Sets and Limit Points ..................... 40
         2.2.2 Continuity ......................................... 41

3 Linear Algebra .................................................. 47
   3.1 Fields ....................................................... 47
   3.2 Matrices .................................................... 48
   3.3 Vector Spaces ............................................... 51
## CONTENTS

3.3.1 Subspaces ................................................................. 52  
3.3.2 Bases and Dimensions ............................................... 53  
3.3.3 Coordinate System .................................................... 56  

3.4 Linear Transformations .................................................. 58  
3.4.1 Definitions ............................................................... 58  
3.4.2 Properties ................................................................. 59  

3.5 Norms .............................................................................. 62  
3.6 Inner Products ................................................................... 68  
3.6.1 Induced Norms .............................................................. 71  

3.7 Sets of Orthogonal Vectors ............................................... 74  
3.7.1 Hilbert Spaces ............................................................... 78  

3.8 Linear Functionals ............................................................ 79  

4 Representation and Approximation ......................................... 83  
4.1 Best Approximation .......................................................... 83  
4.1.1 Projection Operators ...................................................... 86  

4.2 Computing Approximations in Hilbert Spaces ....................... 89  
4.2.1 Normal Equations ........................................................ 89  
4.2.2 Orthogonality Principle ................................................ 91  

4.3 Approximation for Systems of Linear Equations .................... 92  
4.3.1 Matrix Representation .................................................. 92  
4.3.2 Standard Inner Products .............................................. 93  
4.3.3 Generalized Inner Products .......................................... 94  
4.3.4 Minimum Error ............................................................ 94  

4.4 Applications and Examples in Signal Processing ................... 95  
4.4.1 Linear Regression ......................................................... 95  
4.4.2 Linear Minimum Mean-Squared Error Estimation ............... 95  
4.4.3 The Wiener Filter ........................................................ 96  
4.4.4 LMMSE Filtering in Practice ........................................ 98  

4.5 Dual Approximation .......................................................... 100  
4.5.1 Minimum-Norm Solutions .......................................... 100  
4.5.2 Underdetermined Linear Systems ................................... 101  

4.6 Projection onto Convex Sets ............................................... 101  
4.6.1 Projection Properties and Examples ............................... 104
CONTENTS

8  Canonical Forms  157
  8.1  Eigenvalues and Eigenvectors  . . . . . . . . . . . . . . . . 157
  8.2  Applications of Eigenvalues  . . . . . . . . . . . . . . . . . 161
    8.2.1  Differential Equations  . . . . . . . . . . . . . . . . . 161
    8.2.2  Functions of a Matrix  . . . . . . . . . . . . . . . . . . 162
  8.3  The Jordan Form  . . . . . . . . . . . . . . . . . . . . . . . 163
  8.4  Applications of Jordan Normal Form  . . . . . . . . . . . . . 166
    8.4.1  Convergent Matrices  . . . . . . . . . . . . . . . . . . 166

9  Singular Value Decomposition  169
  9.1  Diagonalization of Hermitian Matrices  . . . . . . . . . . . . . 169
  9.2  Singular Value Decomposition  . . . . . . . . . . . . . . . . . 171
  9.3  Properties of the SVD  . . . . . . . . . . . . . . . . . . . . . 173

A  Optional Topics  175
  A.1  Dealing with Infinity*  . . . . . . . . . . . . . . . . . . . . . 175
    A.1.1  The Axiom of Choice  . . . . . . . . . . . . . . . . . . . 175
    A.1.2  Well-Ordered Sets  . . . . . . . . . . . . . . . . . . . . . 176
    A.1.3  The Maximum Principle  . . . . . . . . . . . . . . . . . . 177
Chapter 1

Logic and Set Theory

To criticize mathematics for its abstraction is to miss the point entirely. Abstraction is what makes mathematics work. If you concentrate too closely on too limited an application of a mathematical idea, you rob the mathematician of his most important tools: analogy, generality, and simplicity.

– Ian Stewart

Does God play dice? The mathematics of chaos

In mathematics, a proof is a demonstration that, assuming certain axioms, some statement is necessarily true. That is, a proof is a logical argument, not an empirical one. One must demonstrate that a proposition is true in all cases before it is considered a theorem of mathematics. An unproven proposition for which there is some sort of empirical evidence is known as a conjecture. Mathematical logic is the framework upon which rigorous proofs are built. It is the study of the principles and criteria of valid inference and demonstrations.

Logicians have analyzed set theory in great details, formulating a collection of axioms that affords a broad enough and strong enough foundation to mathematical reasoning. The standard form of axiomatic set theory is denoted ZFC and it consists of the Zermelo-Fraenkel (ZF) axioms combined with the axiom of choice (C). Each of the axioms included in this theory expresses a property of sets that is widely accepted by mathematicians. It is unfortunately true that careless use of set theory can lead to contradictions. Avoiding such contradictions was one of the original motivations for the axiomatization of set theory.
A rigorous analysis of set theory belongs to the foundations of mathematics and
mathematical logic. The study of these topics is, in itself, a formidable task. For
our purposes, it will suffice to approach basic logical concepts informally. That is,
we adopt a naive point of view regarding set theory and assume that the meaning of
a set as a collection of objects is intuitively clear. While informal logic is not itself
rigorous, it provides the underpinning for rigorous proofs. The rules we follow
in dealing with sets are derived from established axioms. At some point of your
academic career, you may wish to study set theory and logic in greater detail. Our
main purpose here is to learn how to state mathematical results clearly and how to
prove them.

\section{1.1 Statements}

A proof in mathematics demonstrates the truth of certain \textit{statement}. It is therefore
natural to begin with a brief discussion of statements. A statement, or \textit{proposition},
is the content of an assertion. It is either true or false, but cannot be both true and
false at the same time. For example, the expression “There are no classes at Texas
A&M University today” is a statement since it is either true or false. The expression
“Do not cheat and do not tolerate those who do” is not a statement. Note that an
expression being a statement does not depend on whether we personally can verify
its validity. The expression “The base of the natural logarithm, denoted \( e \), is an
irrational number” is a statement that most of us cannot prove.

Statements on their own are fairly uninteresting. What brings value to logic is
the fact that there are a number of ways to form new statements from old ones.
In this section, we present five ways to form new statements from old ones. They
correspond to the English expressions: and; or; not; if, then; if and only if. In the
discussion below, \( P \) and \( Q \) represent two abstract statements.

A logical \textit{conjunction} is an operation on two logical propositions that produces
a value of true if both statements are true, and is false otherwise. The conjunction
(or logical AND) of \( P \) and \( Q \), denoted by \( P \land Q \), is precisely defined by
Similarly, a logical **disjunction** is an operator on two logical propositions that is true if either statement is true or both are true, and is false otherwise. The disjunction (or logical OR) of \( P \) and \( Q \), denoted \( P \lor Q \), is defined by

\[
\begin{array}{c|c|c}
P & Q & P \lor Q \\
T & T & T \\
T & F & T \\
F & T & T \\
F & F & F \\
\end{array}
\]

In mathematics, a **negation** is an operator on the logical value of a proposition that sends true to false and false to true. The negation (or logical NOT) of \( P \), denoted \( \neg P \), is given by

\[
\begin{array}{c|c}
P & \neg P \\
T & F \\
F & T \\
\end{array}
\]

The next method of combining mathematical statements is slightly more subtle than the preceding ones. The **conditional connective** \( P \rightarrow Q \) is a logical statement that is read “if \( P \) then \( Q \)” and defined by the truth table

\[
\begin{array}{c|c|c}
P & Q & P \rightarrow Q \\
T & T & T \\
T & F & F \\
F & T & T \\
F & F & T \\
\end{array}
\]

In this statement, \( P \) is called the **antecedent** and \( Q \) is called the **consequent**. The truth table should match your intuition when \( P \) is true. When \( P \) is false, students often think the resulting truth value should be undefined. Although the given definition may seem strange at first glance, this truth table is universally accepted by mathematicians.
To motivate this definition, one can think of \( P \rightarrow Q \) as a promise that \( Q \) is true whenever \( P \) is true. When \( P \) is false, the promise is kept by default. For example, suppose your friend promises “if it is sunny tomorrow, I will ride my bike”. We will call this a true statement if they keep their promise. If it rains and they don’t ride their bike, most people would agree that they have still kept their promise. Therefore, this definition allows one to combine many statements together and detect broken promises without being distracted by uninformative statements.

Logicians draw a firm distinction between the **conditional connective** and the **implication relation**. They use the phrase “if \( P \) then \( Q \)” for the conditional connective and the phrase “\( P \) implies \( Q \)” for the implication relation. They explain the difference between these two forms by saying that the conditional is the contemplated relation, while the implication is the asserted relation. We will discuss this distinction in the Section 1.2, where we formally study relations between statements. The importance and soundness of the conditional form \( P \rightarrow Q \) will become clearer then.

The logical **biconditional** is an operator connecting two logical propositions that is true if the statements are both true or both false, and it is false otherwise. The biconditional from \( P \) to \( Q \), denoted \( P \leftrightarrow Q \), is precisely defined by

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \leftrightarrow Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

We read \( P \leftrightarrow Q \) as “\( P \) if and only if \( Q \).” The phrase “if and only if” is often abbreviated as “iff”.

Using the five basic operations defined above, it is possible to form more complicated compound statements. We sometimes need parentheses to avoid ambiguity in writing compound statements. We use the convention that \( \neg \) takes precedence over the other four operations, but none of these operations takes precedence over the others. For example, let \( P, Q \) and \( R \) be three propositions. We wish to make a truth table for the following statement,

\[
(P \rightarrow R) \land (Q \lor \neg R). \tag{1.1}
\]

We can form the true table for this statement, using simple steps, as follows
We conclude this section with a brief mention of two important concepts. A **tautology** is a statement that is true in every valuation of its propositional variables, independent of the truth values assigned to these variables. The proverbial tautology is \( P \lor \neg P \),

\[
\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c}
P & P & \lor & \neg P \\
T & T & T & F \\
F & F & T & T \\
\end{array}
\]

For instance, the statement “The Aggies won their last football game or the Aggies did not win their last football game” is true regardless of whether the Aggies actually defeated their latest opponent.

The negation of a tautology is a **contradiction**, a statement that is necessarily false regardless of the truth values of its propositional variables. The statement \( P \land \neg P \) is a contradiction, and its truth table is

\[
\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c}
P & P & \land & \neg P \\
T & T & F & F \\
F & F & T & T \\
1 & 3 & 2 & 2 \\
\end{array}
\]

Of course, most statements we encounter are neither tautologies nor contradictions. For example, (1.1) is not necessarily either true or false. Its truth value depends on the values of \( P, Q \) and \( R \). Try to see whether the statement

\[( (P \land Q) \rightarrow R ) \rightarrow ( P \rightarrow ( Q \rightarrow R ) ) \]

is a tautology, a contradiction, or neither.
1.2 Relations between Statements

Strictly speaking, relations between statements are not formal statements themselves. They are *meta-statements* about some propositions. We study two types of relations between statements, *implication* and *equivalence*. An example of an implication meta-statement is the observation that “if the statement ‘Robert graduated from Texas A&M University’ is true, then it implies that the statement ‘Robert is an Aggie’ is also true.” Another example of a meta-statement is “the statement ‘Fred is an Aggie and Fred is honest’ being true is equivalent to the statement ‘Fred is honest and Fred is an Aggie’ being true.” These two examples illustrate how meta-statements describe the relationship between statements. It is also instructive to note that implications and equivalences are the meta-statement analogs of conditionals and biconditionals.

Consider two compound statements $P$ and $Q$ that depend on other logical statements (e.g., $P = (R \rightarrow S) \land (S \rightarrow T)$ and $Q = R \rightarrow T$). A *logical implication* from $P$ to $Q$, read as “$P$ implies $Q$”, asserts that $Q$ must be true whenever $P$ is true (i.e., for all possible truth values of the dependent statements $R, S, T$). Necessity is the key aspect of this sentence; the fact that $P$ and $Q$ both happen to be true cannot be coincidental. To state that $P$ implies $Q$, denoted by $P \Rightarrow Q$, one needs the conditional $P \rightarrow Q$ to be true under all possible circumstances.

Meta-statements, such as “$P$ implies $Q$”, can be defined formally only when $P$ and $Q$ are both logical functions of other propositions. For example, consider $P = R \land (R \rightarrow S)$ and $Q = S$. Then, the truth of the statement $P \rightarrow Q$ depends only on the truth of external propositions $R$ and $S$.

The notion of implication can be rigorously defined as follows, $P$ implies $Q$ if the statement $P \rightarrow Q$ is a tautology. We abbreviate $P$ implies $Q$ by writing $P \Rightarrow Q$. It is important to understand the difference between “$P \Rightarrow Q$” and “$P \Rightarrow Q$.” The former, $P \rightarrow Q$, is a compound statement that may or may not be true. On the other hand, $P \Rightarrow Q$ is a relation stating that the compound statement $P \rightarrow Q$ is true under all instances of the external propositions.

While the distinction between implication and conditional may seem extraneous, we will soon see that meta-statements become extremely useful in building valid arguments. In particular, the following implications are used extensively in constructing proofs.
### 1.2. RELATIONS BETWEEN STATEMENTS

**Fact 1.2.1.** Let $P$, $Q$, $R$ and $S$ be statements.

1. $(P \rightarrow Q) \land P \Rightarrow Q$.
2. $(P \rightarrow Q) \land \neg Q \Rightarrow \neg P$.
3. $P \land Q \Rightarrow P$.
4. $(P \lor Q) \land \neg P \Rightarrow Q$.
5. $P \leftrightarrow Q \Rightarrow P \rightarrow Q$.
6. $(P \rightarrow Q) \land (Q \rightarrow P) \Rightarrow P \rightarrow Q$.
7. $(P \rightarrow Q) \land (Q \rightarrow R) \Rightarrow P \rightarrow R$.
8. $(P \rightarrow Q) \land (R \rightarrow S) \land (P \lor R) \Rightarrow Q \lor S$.

As an illustrative example, we show that $(P \rightarrow Q) \land (Q \rightarrow R)$ implies $P \rightarrow R$.

To demonstrate this assertion, we need to show that

$$((P \rightarrow Q) \land (Q \rightarrow R)) \rightarrow (P \rightarrow R) \quad (1.2)$$

is a tautology. This is accomplished in the truth table below

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$R$</th>
<th>$((P \rightarrow Q) \land (Q \rightarrow R)) \rightarrow (P \rightarrow R)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Column 11 has the truth values for statement (1.2). Since (1.2) is true under all circumstances, it is a tautology and the implication holds. Showing that the other relations are valid is left to the reader as an exercise.

Reversing the arrow in a conditional statement gives the **converse** of that statement. For example, the statement $Q \rightarrow P$ is the converse of $P \rightarrow Q$. This reversal
may not preserve the truth of the statement though and therefore logical implications are not always reversible. For instance, although \((P \rightarrow Q) \land (Q \rightarrow R)\) implies \(P \rightarrow R\), the converse is not always true. It can easily be seen from columns 9 & 10 above that
\[
(P \rightarrow R) \rightarrow ((P \rightarrow Q) \land (Q \rightarrow R))
\]
is not a tautology. That is, \(P \rightarrow R\) certainly does not imply \((P \rightarrow Q) \land (Q \rightarrow R)\).

A logical implication that is reversible is called a **logical equivalence**. More precisely, \(P\) is equivalent to \(Q\) if the statement \(P \iff Q\) is a tautology. We denote the sentence “\(P\) is equivalent to \(Q\)” by simply writing “\(P \iff Q\).” The meta-statement \(P \iff Q\) holds if and only if \(P \Rightarrow Q\) and \(Q \Rightarrow P\) are both true. Being able to recognize that two statements are equivalent will become handy. It is sometime possible to demonstrate a result by finding an alternative, equivalent form of the statement that is easier to prove than the original form. A list of important equivalences appears below.

**Fact 1.2.2.** Let \(P\), \(Q\) and \(R\) be statements.

1. \(\neg(\neg P) \iff P\).
2. \((P \lor Q) \iff Q \lor P\).
3. \((P \land Q) \iff Q \land P\).
4. \((P \lor Q) \lor R \iff P \lor (Q \lor R)\).
5. \((P \land Q) \land R \iff P \land (Q \land R)\).
6. \((P \lor Q) \lor R \iff (P \lor Q) \lor (P \lor R)\).
7. \((P \land Q) \land R \iff (P \land Q) \land (P \land R)\).
8. \(P \rightarrow Q \iff \neg P \lor Q\).
9. \(P \rightarrow Q \iff \neg Q \rightarrow \neg P\) (**Contrapositive**).
10. \(P \iff Q \iff (P \rightarrow Q) \land (Q \rightarrow P)\).
11. \(\neg(P \land Q) \iff \neg P \lor \neg Q\) (**De Morgan’s Law**).
12. \(\neg(P \lor Q) \iff \neg P \land \neg Q\) (**De Morgan’s Law**).
1.2. RELATIONS BETWEEN STATEMENTS

Given a conditional statement of the form $P \rightarrow Q$, we call $\neg Q \rightarrow \neg P$ the **contrapositive** of the original statement. The equivalence $P \rightarrow Q \iff \neg Q \rightarrow \neg P$ noted above is used extensively in constructing mathematical proofs.

One must be careful not to allow contradictions in logical arguments because, starting from a contradiction, anything can be proven true. For example, one can verify that $P \land \neg P \Rightarrow Q$ is a valid logical equivalence. But, $Q$ doesn’t appear on the LHS. Thus, a contradiction in your assumptions can lead to a “correct” proof for an arbitrary statement.

Fortunately, propositional logic has an axiomatic formulation that is consistent, complete, and decidable. In this context, the term **consistent** means that the logical implications generated by the axioms do not contain a contradiction, the term **complete** means that any valid logical implication can be generated by applying the axioms, and the term **decidable** means there is a terminating method that always determines whether a postulated implication is valid or invalid.

1.2.1 Fallacious Arguments

A **fallacy** is a component of an argument that is demonstrably flawed in its logic or form, thus rendering the argument invalid. Recognizing fallacies in mathematical proofs may be difficult since arguments are often structured using convoluted patterns that obscure the logical connections between assertions. We give below examples for three types of fallacies that are often found in attempted mathematical proofs.

**Affirming the Consequent:** If the Indian cricket team wins a test match, then all the players will drink tea together. All the players drank tea together. Therefore the Indian cricket team won a test match.

**Denying the Antecedent:** If Diego Maradona drinks coffee, then he will be fidgety. Diego Maradona did not drink coffee. Therefore, he is not fidgety.

**Unwarranted Assumptions:** If Yao Ming gets close to the basket, then he scores a lot of points. Therefore, Yao Ming scores a lot of points.
1.2.2 Quantifiers

Consider the statements “Socrates is a person” and “Every person is mortal”. In propositional logic, there is no formal way to combine these statements to deduce that “Socrates is mortal”. In the first statement, the noun “Socrates” is called the subject and the phrase “is a person” is called the **predicate**. Likewise, in predicate logic, the statement \( P(x) = \text{“}x \text{ is a person}\) is called a predicate and \( x \) is called a **free variable** because its value is not fixed in the statement \( P(x) \).

Let \( U \) be a specific collection of elements and let \( P(x) \) be a statement that can be applied to any \( x \in U \). In first-order predicate logic, quantifiers are applied to predicates in order to make statements about collections of elements. Later, we will see that quantifiers are of paramount importance in rigorous proofs.

The **universal quantifier** is typically denoted by \( \forall \) and it is informally read “for all.” It follows that the statement \( \forall x \in U, P(x) \) is true if \( P(x) \) is true for all values of \( x \) in \( U \). It can be seen as shorthand for an iterated conjunction because
\[
\forall x \in U, P(x) \iff \bigwedge_{x \in U} P(x),
\]
where \( \iff \) indicates that these statements are equivalent for all sets \( U \) and predicates \( P \). If \( U = \emptyset \) is the empty set, then \( \forall x \in U, P(x) \) is vacuously true by convention because there are no elements in \( U \) to test with \( P(x) \).

Returning to the motivating example, let us also define \( Q(x) = \text{“}x \text{ is mortal}\)”. With these definitions, we can write the statement “Every person is mortal” as \( \forall x, (P(x) \rightarrow Q(x)) \). In logic, this usage implies that \( x \) ranges over the universal set. In engineering mathematics, however, the range of free variables is typically stated explicitly.

The other type of quantifier often seen in mathematical proofs is the **existential quantifier**, denoted \( \exists \). The statement \( \exists x \in U, P(x) \) is true if \( P(x) \) is true for at least one value of \( x \) in \( U \). It can be seen as shorthand for an iterated disjunction because
\[
\exists x \in U, P(x) \iff \bigvee_{x \in U} P(x),
\]
If \( U = \emptyset \) is the empty set, then \( \exists x \in U, P(x) \) is false by convention because there are no elements in \( U \).

The idea of **universal instantiation** is that, if a statement \( P(x) \) is true for all \( x \in U \), then there must exist some \( x_0 \in U \) such that \( P(x_0) \) is true. However, this
1.2. RELATIONS BETWEEN STATEMENTS

implicitly assumes that $U$ is not empty. In fact, universal instantiation does not hold when $U$ is empty. If $U$ is not empty though, then universal instantiation implies that $\forall x \in U, P(x) \Rightarrow \exists x \in U, P(x)$.

Based on the meaning of these quantifiers, one can infer the logical implications

$$
\neg (\forall x \in U, P(x)) \iff \exists x \in U, \neg P(x)
$$

$$
\neg (\exists x \in U, P(x)) \iff \forall x \in U, \neg P(x).
$$

Using the connection to conjunction and disjunction, these rules are actually equivalent to De Morgan’s law for iterated conjunctions and disjunctions.

One can also define predicates with multiple free variables such as $P(x, y) = "x contains y"$. Once again, these statements are assumed to be true or false for every choice of $x, y$. There are 8 possible quantifiers for a 2-variable predicate and they can be arranged according based on some natural implications. Assuming that $x, y$ are taken from non-empty sets, one finds that

$$
\forall x, \forall y, P(x, y) \Rightarrow \exists x, \forall y, P(x, y) \Rightarrow \forall y, \exists x, P(x, y) \Rightarrow \exists y, \exists x, P(x, y)
$$

$$
\forall y, \forall x, P(x, y) \Rightarrow \exists y, \forall x, P(x, y) \Rightarrow \forall x, \exists y, P(x, y) \Rightarrow \exists x, \exists y, P(x, y)
$$

All of these implications follow from $\forall x \forall y = \forall y \forall x, \exists x \exists y = \exists y \exists x$, and the single variable inference rule $\forall x, P(x) \Rightarrow \exists x, P(x)$ except for two: $\exists x, \forall y, P(x, y) \Rightarrow \forall y, \exists x, P(x, y)$ and its symmetric pair.

To understand this last implication, consider an example where $x$ is in a set $I$ of images and $y$ is in a set $C$ of colors. Then, $\exists x, \forall y, P(x, y)$ means “there is an image that contains all the colors” (e.g., an image of a rainbow) and $\forall y, \exists x, P(x, y)$ means “for each color there is an image containing that color”. The first statement implies the second because, in the second, the rainbow image satisfies the $\exists x$ quantifier for all $y$. To see that the implication is not an equivalence, consider a set of pictures where each image contains exactly one color and there is one such image for each color. In this case, it is true that “for each color there is an image containing that color” but it is not true that “there is an image that contains all the colors”.

In quantified statements, such as $\exists x \in U, P(x)$, the variable $x$ is called a **bound variable** because its value cannot be chosen freely. Similarly, in the statement $\exists y \in U, P(x, y)$, $x$ is a free variable and $y$ is a bound variable.
Finally, we note that first-order predicate logic has an axiomatic formulation that is consistent, complete, and semidecidable. In this context, \textit{semidecidable} means that there is an algorithm that, if it terminates, correctly determines the truth of any postulated implication. But, it is only guaranteed to terminate for true postulates.

\subsection{1.3 Strategies for Proofs}

The relation between intuition and formal rigor is not a trivial matter. Intuition tells us what is important, what might be true, and what mathematical tools may be used to prove it. Rigorous proofs are used to verify that a given statement which appears intuitively true is indeed true. Ultimately, a mathematical proof is a convincing argument that starts from some premises, and logically deduces the desired conclusion. Most proofs do not mention the logical rules of inference used in the derivation. Rather, they focus on the mathematical justification of each step, leaving to the reader the task of filling the logical gaps. The mathematics is the major issue. Yet, it is essential that you understand the underlying logic behind the derivation as to not get confused while reading or writing a proof.

True statements in mathematics have different names. They can be called theorems, propositions, lemmas, corollaries and exercises. A \textit{theorem} is a statement that can be proved on the basis of explicitly stated or previously agreed assumptions. A \textit{proposition} is a statement not associated with any particular theorem; this term sometimes connotes a statement with a simple proof. A \textit{lemma} is a proven proposition which is used as a stepping stone to a larger result rather than an independent statement in itself. A \textit{corollary} is a mathematical statement which follows easily from a previously proven statement, typically a mathematical theorem. The distinction between these names and their definitions is somewhat arbitrary. Ultimately, they are all synonymous to a true statement.

A proof should be written in grammatically correct English. Complete sentences should be used, with full punctuation. In particular, every sentence should end with a period, even if the sentence ends in a displayed equation. Mathematical formulas and symbols are parts of sentences, and are treated no differently than words. One way to learn to construct proofs is to read a lot of well written proofs, to write progressively more difficult proofs, and to get detailed feedback on the proofs you write.
Direct Proof: The simplest form of proof for a statement of the form \( P \rightarrow Q \) is the direct proof. First assume that \( P \) is true. Produce a series of steps, each one following from the previous ones, that eventually leads to conclusion \( Q \). It warrants the name “direct proof” only to distinguish it from other, more intricate, methods of proof.

Proof by Contrapositive: A proof by contrapositive takes advantage of the mathematical equivalence \( P \rightarrow Q \iff \neg Q \rightarrow \neg P \). That is, a proof by contrapositive begins by assuming that \( Q \) is false (i.e., \( \neg Q \) is true). It then produces a series of direct implications leading to the conclusion that \( P \) is false (i.e., \( \neg P \) is true). It follows that \( Q \) cannot be false when \( P \) is true, so \( P \rightarrow Q \).

Proof by Contradiction: A proof by contradiction is based on the mathematical equivalence \( \neg(P \rightarrow Q) \iff P \land \neg Q \). In a proof by contradiction, one starts by assuming that both \( P \) and \( \neg Q \) are true. Then, a series of direct implications are given that lead to a logical contradiction. Hence, \( P \land \neg Q \) cannot be true and \( P \rightarrow Q \).

Example 1.3.1. We wish to show that \( \sqrt{2} \) is an irrational number.

First, suppose that \( \sqrt{2} \) is a rational number. This would imply that there exist integers \( p \) and \( q \) with \( q \neq 0 \) such that \( \frac{p}{q} = \sqrt{2} \). In fact, we can further assume that the fraction \( \frac{p}{q} \) is irreducible. That is, \( p \) and \( q \) are coprime integers (they have no common factor greater than 1). From \( \frac{p}{q} = \sqrt{2} \), it follows that \( p = \sqrt{2}q \), and so \( p^2 = 2q^2 \). Thus \( p^2 \) is an even number, which implies that \( p \) itself is even (only even numbers have even squares). Because \( p \) is even, there exists an integer \( r \) satisfying \( p = 2r \). We then obtain the equation \((2r)^2 = 2q^2\), which is equivalent to \( 2r^2 = q^2 \) after simplification. Because \( 2r^2 \) is even, it follows that \( q^2 \) is even, which means that \( q \) is also even. We conclude that \( p \) and \( q \) are both even. This contradicts the fact that \( \frac{p}{q} \) is irreducible. Hence, the initial assumption that \( \sqrt{2} \) is a rational number must be false. That is to say, \( \sqrt{2} \) is irrational.

Example 1.3.2. Consider the following statement, which is related to Example 1.3.1. “If \( \sqrt{2} \) is rational, then \( \sqrt{2} \) can be expressed as an irreducible fraction.” The contrapositive of this statement is “If \( \sqrt{2} \) cannot be expressed as an irreducible fraction, then \( \sqrt{2} \) is not rational.” Above, we proved that \( \sqrt{2} \) cannot be expressed as an irreducible fraction and therefore \( \sqrt{2} \) is not a rational number.
The final proof strategy we discuss is finite induction.

**Definition 1.3.3.** Let \( P(n) \) be a logical statement for each \( n \in \mathbb{N} \). The principle of mathematical induction states that \( P(n) \) is true all \( n \in \mathbb{N} \) if:

1. \( P(1) \) is true, and
2. \( P(n) \rightarrow P(n + 1) \) for all \( n \in \mathbb{N} \).

From a foundational perspective, this statement is essentially equivalent to the existence and uniqueness of the natural numbers. It is taken as an axiom in the Peano axiomatic formulation of arithmetic. In contrast, the ZF axiomatic formulation of set theory defines the natural numbers as the smallest inductive set and the existence of an inductive set is taken as an axiom.

**Example 1.3.4.** Let \( S_n = \sum_{i=1}^{n} i \). We wish to show that the statement \( P(n) = \text{"}S_n = \frac{n^2 + n}{2}\text{"} \) is true for all \( n \in \mathbb{N} \). For \( n = 1 \), this is true because both expressions equal 1. For \( P(n + 1) \), we are given \( P(n) \) and can write

\[
S_{n+1} = S_n + (n + 1) = \frac{n^2 + n}{2} + n + 1 = \frac{n^2 + 3n + 2}{2} = \frac{(n + 1)^2 + (n + 1)}{2}.
\]

Thus, the result follows from mathematical induction.

More general forms of finite induction are also quite common but they can reduced to the original form. For example, let \( Q(m) \) be a predicate for \( m \in \mathbb{N} \) and define \( P(n) = \text{"}\forall m \in S_n, Q(m)\text{"} \) for a sequence nested finite sets \( S_1 \subset S_2 \subset \cdots \subset \mathbb{N} \). Defining \( S_{\infty} = \bigcup_{n \in \mathbb{N}} S_n \), we see that \( \forall n \in \mathbb{N}, P(n) \leftrightarrow \forall m \in S_{\infty}, Q(m) \) follows from \( P(1) = \text{"}\forall m \in S_1, Q(m)\text{"} \) and \( P(n) \rightarrow P(n + 1) \leftrightarrow \forall m \in S_n, Q(m) \rightarrow \forall m \in S_{n+1}, Q(m) \).

### 1.4 Set Theory

Set theory is generally considered to be the foundation of all modern mathematics. This means that most mathematical objects (numbers, relations, functions, etc.) are defined in terms of sets. Unfortunately for engineers, set theory is not quite as simple as it seems. It turns out that simple approaches to set theory include paradoxes (e.g., statements which are both true and false). These paradoxes can
be resolved by putting set theory in a firm axiomatic framework, but that exercise is rather unproductive for engineers. Instead, we adopt what is called naive set theory which rigorously defines the operations of set theory without worrying about possible contradictions. This approach is sufficient for most of mathematics and also acts as a stepping-stone to more formal treatments.

A set is taken to be any collection of objects, mathematical or otherwise. For example, one can think of “the set of all books published in 2007”. The objects in a set are referred to as elements or members of the set. The logical statement “a is a member of the set \( A \)” is written

\[ a \in A. \]

Likewise, its logical negation “a is not a member of the set \( A \)” is written \( a \notin A \). Therefore, exactly one of these two statements is true. In naive set theory, one assumes the existence of any set that can be described in words. Later, we will see that this can be problematic when one considers objects like the “set of all sets”.

One may present a set by listing its elements. For example, \( A = \{a, e, i, o, u\} \) is the set of standard English vowels. It is important to note that the order elements are presented is irrelevant and the set \( \{i, o, u, a, e\} \) is the same as \( A \). Likewise, repeated elements have no effect and the set \( \{a, e, i, o, u, e, o\} \) is the same as \( A \). A singleton set is a set containing exactly one element such as \( \{a\} \).

There are a number of standard sets worth mentioning: the integers \( \mathbb{Z} \), the real numbers \( \mathbb{R} \), and the complex numbers \( \mathbb{C} \). It is possible to construct these sets in a rigorous manner, but instead we will assume their meaning is intuitively clear. New sets can be defined in terms of old sets using set-builder notation. Let \( P(x) \) be a logical statement about objects \( x \) in the set \( X \), then the “set of elements in \( X \) such that \( P(x) \) is true” is denoted by

\[ \{x \in X | P(x)\}. \]

For example, the set of even integers is given by

\[ \{x \in \mathbb{Z} | “x \ is \ even”\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}. \]

If no element \( x \in X \) satisfies the condition, then the result is the empty set which is denoted \( \emptyset \). Using set-builder notation, we can also recreate the natural numbers...
N and the rational numbers Q with

\[ N = \{ n \in \mathbb{Z} | n \geq 1 \} \]
\[ Q = \{ q \in \mathbb{R} | q = a/b, a \in \mathbb{Z}, b \in \mathbb{N} \}. \]

The following standard notation is used for interval subsets of the real numbers:

- Open interval: \((a, b) \triangleq \{ x \in \mathbb{R} | a < x < b \}\)
- Closed interval: \([a, b] \triangleq \{ x \in \mathbb{R} | a \leq x \leq b \}\)
- Half-open intervals:
  - \((a, b] \triangleq \{ x \in \mathbb{R} | a < x \leq b \}\)
  - \([a, b) \triangleq \{ x \in \mathbb{R} | a \leq x < b \}\)

**Definition 1.4.1.** For a finite set \(A\), the cardinality \(|A|\) equals the number of elements in \(A\). If there is a bijective mapping between the set \(A\) and the natural numbers \(\mathbb{N}\), then \(|A| = \infty\) and the set is called countably infinite. If \(|A| = \infty\) and the set is not countably infinite, then \(A\) is called uncountably infinite.

**Example 1.4.2.** The set of rational numbers is countably infinite while the set of real numbers is uncountably infinite.

**Example 1.4.3 (Russell’s Paradox).** Let \(R\) be the set of all sets that do not contain themselves or \(R = \{ S | S \notin S \}\). Such a set is said to exist in naive set theory (though it may empty) simply because it can be described in words. The paradox arises from the fact that the definition leads to the logical contradiction \(R \in R \leftrightarrow R \notin R\).

What this proves is that naive set theory is not consistent because it allows constructions that lead to contradictions. Axiomatic set theory eliminates this paradox by disallowing self-referential and other problematic constructions. Thus, another reasonable conclusion is that Russell’s paradox shows that the set \(R\) cannot exist in any consistent theory of sets.

Another common question is whether there are sets that contains themselves. In naive set theory, the answer is yes and some examples are the “set of all sets” and the “set of all abstract ideas”. On the other hand, in the ZF axiomatic formulation of set theory, it is a theorem that no set contains itself.

There are a few standard relationships defined between any two sets \(A, B\).
1.4. SET THEORY

Definition 1.4.4. We say that A equals B (denoted $A = B$) if, for all $x$, $x \in A$ iff $x \in B$. This means that

$$A = B \iff \forall x ((x \in A) \leftrightarrow (x \in B)).$$

Definition 1.4.5. We say that A is a subset of B (denoted $A \subseteq B$) if, for all $x$, if $x \in A$ then $x \in B$. This means that

$$A \subseteq B \iff \forall x ((x \in A) \rightarrow (x \in B)).$$

It is a proper subset (denoted $A \subset B$) if $A \subseteq B$ and $A \neq B$.

There are also a number of operations between sets. Let $A, B$ be any two sets.

Definition 1.4.6. The union of A and B (denoted $A \cup B$) is the set of elements in either $A$ or $B$. This means that $A \cup B = \{x \in A \text{ or } x \in B\}$ is also defined by

$$x \in A \cup B \iff (x \in A) \lor (x \in B).$$

Definition 1.4.7. The intersection of A and B (denoted $A \cap B$) is the set of elements in both $A$ and $B$. This means that $A \cap B = \{x \in A \mid x \in B\}$ is also defined by

$$x \in A \cap B \iff (x \in A) \land (x \in B).$$

Two sets are said to be disjoint if $A \cap B = \emptyset$.

Definition 1.4.8. The set difference between A and B (denoted $A - B$ or $A \setminus B$) is the set of elements in A but not in B. This means that

$$x \in A - B \iff (x \in A) \land (x \notin B).$$

If there is some implied universal set $U$, then the complement (denoted $A^c$) is defined by $A^c = U - A$

One can apply De Morgan’s Law in set theory to verify that

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c,$$

which allows us to interchange union or intersection with set difference.
We can also form the union or the intersection of arbitrarily many sets. This is defined in a straightforward way,

\[ S = \{ x \mid x \in S_\alpha \text{ for some } \alpha \in I \} \]

\[ \bigcap_{\alpha \in I} S_\alpha = \{ x \mid x \in S_\alpha \text{ for all } \alpha \in I \}. \]

It is worth noting that the definitions apply whether the index set is finite, countably infinite, or even uncountably infinite.

Another way to build sets is by grouping elements into pairs, triples, and vectors.

**Definition 1.4.9.** The **Cartesian Product**, denoted \( A \times B \), of two sets is the set of ordered pairs \( \{(a, b) \mid a \in A, b \in B\} \). For \( n \)-tuples taken from the same set, the notation \( A^n \) denotes the \( n \)-fold product \( A \times A \times \cdots \times A \).

**Example 1.4.10.** If \( A = \{a, b\} \), then the set of all 3-tuples from \( A \) is given by

\[ A^3 = \{(a, a, a), (a, a, b), (a, b, a), (b, a, a), (b, a, b), (b, b, a), (b, b, b)\}. \]

The countably infinite product of \( X \), denoted \( X^\omega \), is the set of infinite sequences \((x_1, x_2, x_3, \ldots)\) where \( x_n \in X \) is arbitrary for \( n \in \mathbb{N} \). If the sequences are restricted to have only a finite number of non-zero terms, then the set is usually denoted \( X^\infty \).

One can also formalize relationships between elements of a set. A **relation** \( \sim \) between elements of the set \( A \) is defined by the pairs \((x, y) \in A \times A\) for which the relation holds. Specifically, the relation is defined by the subset of ordered pairs \( E \subseteq A \times A \) where the relation \( a \sim b \) holds; so \( x \sim y \) if and only if \((x, y) \in E\). A relation on \( A \) is said to be:

1. Reflexive if \( x \sim x \) holds for all \( x \in A \)
2. Symmetric if \( x \sim y \) implies \( y \sim x \) for all \( x, y \in A \)
3. Transitive if \( x \sim y \) and \( y \sim z \), then \( x \sim z \) for all \( x, y, z \in A \)

A relation is called an **equivalence relation** if it is reflexive, symmetric, and transitive. For example, let \( A \) be a set of people and \( P(x, y) \) be the statement “\( x \) has the same birthday (month and day) as \( y \).” Then, we can define \( \sim \) such that \( a \sim b \) holds if and only if \( P(x, y) \) is true. In this case, the set \( E \) is given by
1.5. FUNCTIONS

\[ E = \{(x, y) \in A \times A | P(x, y)\} \]. One can verify that this is an equivalence relation by checking that it is reflexive, symmetric, and transitive.

One important characteristic of an equivalence relation is that it partitions the entire set \( A \) into disjoint equivalence classes. The equivalence class associated with \( a \in A \) is given by \([a] = \{x \in A | x \sim a\}\). In the birthday example, there is a natural equivalence class associated with each day of the year. The set of all equivalence classes is called the quotient set and is denoted \( A/\sim \triangleq \{[a] | a \in A\}\).

In fact, there is a natural equivalence relation defined by any disjoint partition of a set. For example, let \( A_{i,j} \) be the set of people in \( A \) whose birthday was on the \( j \)-th day of the \( i \)-th month. It follows that \( x \sim y \) if and only if there exists a unique pair \( i, j \) such that \( x, y \in A_{i,j} \). In this case, the days of year are used as equivalence classes to define the equivalence relation.

**Example 1.4.11.** Consider the set \( \mathbb{N} \times \mathbb{N} = \{(a, b) | a, b \in \mathbb{N}\} \) of ordered pairs of natural numbers. If one associates the element \((a, b)\) with the fraction \( a/b \), then the entire set is associated with the set of (possibly reducible) fractions. Now, consider the equivalence relation \((a, b) \sim (c, d)\) if \( ad = bc \). In this case, two ordered pairs are equivalent if their associated fractions evaluate to the same real number. The quotient set \( \mathbb{N}/\sim \) can therefore be associated with the set of reduced fractions.

Unfortunately, this section will not end on a happy note by saying that the ZFC axiomatic formulation of set theory is consistent. Instead, we observe that Kurt Gödel’s Incompleteness Theorems imply that, if ZFC is consistent, then this cannot be proven using statements in ZFC and, moreover, it cannot be complete. On the other hand, if ZFC is inconsistent, then it contains a paradox and one can prove anything using statements in ZFC. Since ZFC manages to avoid all known paradoxes and no contradictions have been so far, it is still the most popular formal system in which to define mathematics.

1.5 Functions

In elementary mathematics, functions are typically described in terms of graphs and formulas. The drawback of this approach is that one tends to picture only “nice” functions. In fact, Cauchy himself published in 1821 an incorrect proof of the false assertion that “a sequence of continuous functions that converges everywhere has a
continuous limit function.” Nowadays, every teacher warns their students that one must be careful because the world is filled with “not so nice” functions.

The modern approach to defining functions is based on set theory. A function \( f: X \rightarrow Y \) is a rule that assigns a single value \( f(x) \in Y \) to each element \( x \in X \).

The notation \( f: X \rightarrow Y \) is used to emphasize the role of the domain \( X \) and the codomain \( Y \). The range of \( f \) is the subset of \( Y \) which is actually achieved by \( f \), \( \{ f(x) \in Y | x \in X \} \). Since the term codomain is somewhat uncommon, people often use the term range instead of codomain either intentionally (for simplicity) or unintentionally (due to confusion).

**Definition 1.5.1.** Formally, a function \( f: X \rightarrow Y \) from \( X \) to \( Y \) is defined by a subset \( F \subset X \times Y \) such that \( A_x = \{ y \in Y | (x, y) \in F \} \) has exactly one element for each \( x \in X \). The value of \( f \) at \( x \in X \), denoted \( f(x) \), is the unique element of \( Y \) contained in \( A_x \).

Two functions are said to be equal if they have the same domain, codomain, and value for all elements of the domain. A function \( f \) is called:

1. **one-to-one** or injective if, for all \( x, x' \in X \), if \( f(x) = f(x') \) then \( x = x' \);

2. **onto** or surjective if its range \( \{ f(x) | x \in X \} \) equals \( Y \);

3. a **one-to-one correspondence** or bijective if it is both one-to-one and onto.

A bijective function \( f: X \rightarrow Y \) has a unique inverse function \( f^{-1}: Y \rightarrow X \) such that \( f^{-1}(f(x)) = x \) for all \( x \in X \) and \( f(f^{-1}(y)) = y \) for all \( y \in Y \). In fact, any one-to-one function \( f: X \rightarrow Y \) can be transformed into a bijective function \( g: X \rightarrow R \) with \( g(x) = f(x) \) by restricting its codomain \( Y \) to its range \( R \).

Functions can also be applied to sets in a natural way. For a function \( f: X \rightarrow Y \) and subset \( A \subseteq X \), the **image** of \( A \) under \( f \) is

\[
 f(A) \triangleq \{ y \in Y | \exists x \in A \text{ s.t. } f(x) = y \} = \{ f(x) | x \in A \}.
\]

Using this definition, we see that the range of \( f \) is simply \( f(X) \). One benefit of allowing functions to have set-valued images is that a set-valued inverse function always exists. The **inverse image** or preimage of a subset \( B \subseteq Y \) is

\[
 f^{-1}(B) \triangleq \{ x \in X | f(x) \in B \}.
\]
1.5. FUNCTIONS

For a one-to-one function \( f \), the inverse image of any singleton set \( \{ f(x) \} \) is the singleton set \( \{ x \} \). It is worth noting that the notation \( f^{-1}(B) \) for the preimage of \( B \) can be somewhat misleading because, in some cases, \( f^{-1}(f(A)) \neq A \). In general, a function gives rise to the following property, \( f(f^{-1}(B)) \subseteq B \) and \( f^{-1}(f(A)) \supseteq A \).

**Example 1.5.2.** Let the function \( f : \mathbb{R} \to \mathbb{R} \) be defined by \( f(x) = x^2 \). Let \( A = [1, 2] \) and notice that \( B = f(A) = [1, 4] \). Then,

\[
f^{-1}(B) = f^{-1}([1, 4]) = [-2, -1] \cup [1, 2] \supseteq A.
\]

**Example 1.5.3.** Let the function \( f : \mathbb{R} \to \mathbb{R} \) be defined by \( f(x) = x^2 + 1 \). Let \( B = [0, 2] \) and notice that \( A = f^{-1}(B) = [-1, 1] \). Then,

\[
f(A) = f([-1, 1]) = [1, 2] \subseteq B.
\]

**Problem 1.5.4.** For all \( f : X \to Y, A \subseteq X, \) and \( B \subseteq Y \), we have the rules:

\[(a) \ x \in A \Rightarrow f(x) \in f(A) \quad (b) \ y \in f(A) \Rightarrow \exists x \in A \text{ s.t. } f(x) = y \]

\[(c) \ x \in f^{-1}(B) \Rightarrow f(x) \in B \quad (d) \ f(x) \in B \Rightarrow x \in f^{-1}(B).\]

Use these rules to show that \( f^{-1}(f(A)) \supseteq A \) and \( f(f^{-1}(B)) \subseteq B \).

**Solution 1.5.4.** The first result follows from

\[
x \in A \overset{(a)}{\Rightarrow} f(x) \in f(A) \overset{(d)}{\Rightarrow} x \in f^{-1}(f(A)),
\]

and the definition of subset. The second result follows from

\[
y \in f(f^{-1}(B)) \overset{(b)}{\Rightarrow} \exists x \in f^{-1}(B) \text{ s.t. } f(x) = y \overset{(c)}{\Rightarrow} y \in B,
\]

and the definition of subset.

**Problem 1.5.5.** Let \( f : X \to Y, A_i \subseteq X \) for all \( i \in I, \) and \( B_i \subseteq Y \) for all \( i \in I \). Show that the following expressions hold:

\[(1) \quad f \left( \bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} f \left( A_i \right) \quad (2) \quad f \left( \bigcap_{i \in I} A_i \right) \subseteq \bigcap_{i \in I} f \left( A_i \right) \]

\[(3) \quad f^{-1} \left( \bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} f^{-1} \left( B_i \right) \quad (4) \quad f^{-1} \left( \bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} f^{-1} \left( B_i \right).\]
Chapter 2

Metric Spaces and Topology

We initiate this chapter with a brief discussion of key mathematical concepts and motivate how they can be generalized to address important challenges. We assume that the intended reader has experience with the real numbers, convergent sequences, and continuous functions. Specifically, the reader should be familiar with the following notions.

• **Convergence:** Suppose \( x_1, x_2, \ldots \) is a sequence of real numbers. This sequence converges to a point \( x \) if, for any \( \epsilon > 0 \), there exists a number \( N \) such that \( |x_n - x| < \epsilon \) for all \( n > N \).

• **Continuity:** Suppose \( f : \mathbb{R} \to \mathbb{R} \) is a real-valued function over the real numbers. This function is continuous at \( x_0 \) if, for any \( \epsilon > 0 \), there exists a \( \delta > 0 \) such that \( |f(x) - f(x_0)| < \epsilon \) for all \( x \in \mathbb{R} \) satisfying \( |x - x_0| < \delta \).

One scenario where convergence plays an important role is in the design of iterative methods applied to optimization. Therein, convergence properties can ensure that the iterative process leads to a well-defined answer. Likewise, continuity is a cornerstone of calculus, differential equations, and probability. These related concepts give rise to many practical mathematical tools like gradient descent and Newton’s method.

The definitions above are empowering when dealing with the real numbers. Yet, we are interested in exploring spaces that contain objects such as vectors, time series, images, arrays of data, polynomials, matrices, and functions. This brings up an important question: How can we extend the notions of convergence and continuity
to more general spaces? Answering this question is key in better understanding the structure of abstract spaces and, also, in designing algorithms and iterative methods attuned to a rich class of problems.

A first step in developing a more powerful theory is to identify what makes these definitions work for the real numbers. Based on the insights we gain from familiar examples, we can then extract key attributes and build intuition on how we can define similar concepts for abstract spaces. We begin with pertinent questions. First off, what are the real numbers and why do we use them all the time, as opposed to, say, the rational numbers? Second, in the definition of convergence above, we need to know the limit of the sequence to show convergence. However, when we design an iterative algorithm, we most likely do not know its limit; else we would not need to use an iteration process to get there. Is there a notion of convergent sequence for which we do not need to possess an explicit characterization of its limit beforehand? Interestingly, both definitions rely on proximity, respectively $|x_n - x|$ and $|f(x) - f(x_0)|$. We have a pretty good grasp of the distance between two points on the real line. How can we define the distance between two points in more general setting? These are the questions we seek to address below, in the hope of leveraging our familiarity with real numbers into understanding more general spaces.

2.1 Metric Spaces

From an applied perspective, the quintessential way to construct a topology on a space is to define the open sets in terms of a metric. This approach underlies our intuitive understanding of open and closed sets on the real line. Generally speaking, a metric captures the notion of a distance between two elements of a set. Topologies that are defined through metrics possess a number of properties that make them suitable for analysis. Identifying these common properties permits the unified treatment of different spaces that are useful in solving practical problems. To gain better insight into metric spaces, we review the notion of a metric and we introduce a formal definition for topology.

A metric space is a set with a well-defined distance between any two elements. In some sense, such a space abstracts a few basic properties of Euclidean space. Formally, a metric space $(X,d)$ is a set $X$ and a function $d$ called a metric. The function $d(\cdot, \cdot)$ must fulfill the following properties.
2.1. METRIC SPACES

Definition 2.1.1. A metric on a set $X$ is a function

$$d: X \times X \to \mathbb{R}$$

that satisfies the following properties,

1. $d(x, y) \geq 0 \quad \forall x, y \in X$; equality holds if and only if $x = y$
2. $d(x, y) = d(y, x) \quad \forall x, y \in X$
3. $d(x, y) + d(y, z) \geq d(x, z) \quad \forall x, y, z \in X$.

Example 2.1.2. The collection of real numbers equipped with the metric of absolute distance, $d(x, y) = |x - y|$, defines the standard metric space for the real numbers $\mathbb{R}$.

Example 2.1.3. The set of vectors in $\mathbb{R}^n$ can also be endowed with a metric. Suppose $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are elements in $\mathbb{R}^n$. The Euclidean metric $d$ on $\mathbb{R}^n$ is defined by

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}.$$

As implied by its name, the function $d(\cdot, \cdot)$ given above possesses all the properties of a metric.

It may be beneficial to also look at metrics that are less common. The following two problems introduce alternate distances between points.

Problem 2.1.4. Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ and consider the function $\rho$ given by

$$\rho(x, y) = \max \{|x_1 - y_1|, \ldots, |x_n - y_n|\}.$$

Show that $\rho$ is a metric.

Problem 2.1.5. Let $X$ be a metric space with metric $d$. Define $\bar{d}: X \times X \to \mathbb{R}$ by

$$\bar{d}(x, y) = \min \{d(x, y), 1\}.$$

Show that $\bar{d}$ is also a metric.
2.1.1 Convergence

Let \((X, d)\) be a metric space. Then, elements of \(X\) are called **points** and the number \(d(x, y)\) is called the **distance** between \(x\) and \(y\). Let \(\epsilon > 0\) and consider the set \(B_d(x, \epsilon) = \{y \in X \mid d(x, y) < \epsilon\}\). This set is called the \(d\)-**open ball** (or open ball) of radius \(\epsilon\) centered at \(x\).

**Problem 2.1.6.** Suppose \(a \in B_d(x, \epsilon)\) with \(\epsilon > 0\). Show that there exists a \(d\)-open ball centered at \(a\) of radius \(\delta\), say \(B_d(a, \delta)\), that is contained in \(B_d(x, \epsilon)\).

One of the main benefits of having a metric is that it provides some notion of “closeness” between points in a set. This allows one to discuss limits, convergence, open sets, and closed sets.

**Definition 2.1.7.** A **sequence** of elements from a set \(X\) is an infinite list \(x_1, x_2, \ldots\) where \(x_i \in X\) for all \(i \in \mathbb{N}\). Formally, a sequence is equivalent to a function \(f : \mathbb{N} \to X\) where \(x_i = f(i)\) for all \(i \in \mathbb{N}\).

**Definition 2.1.8.** Consider a sequence \(x_1, x_2, \ldots\) of points in a metric space \((X, d)\). We say that \(x_n\) **converges** to \(x \in X\) (denoted by \(x_n \to x\)) if, for any \(\epsilon > 0\), there is natural number \(N\) such that \(d(x, x_n) < \epsilon\) for all \(n > N\).

**Problem 2.1.9.** For a sequence \(x_n\), show that \(x_n \to a\) and \(x_n \to b\) implies \(a = b\).

**Definition 2.1.10.** A sequence \(x_1, x_2, \ldots\) in \((X, d)\) is a **Cauchy sequence** if, for any \(\epsilon > 0\), there is a natural number \(N\) (depending on \(\epsilon\)) such that, for all \(m, n > N\),

\[
   d(x_m, x_n) < \epsilon.
\]

**Theorem 2.1.11.** Every convergent sequence is a Cauchy sequence.

**Proof.** Since \(x_1, x_2, \ldots\) converges to some \(x\), there is an \(N\), for any \(\epsilon > 0\), such that \(d(x, x_n) < \epsilon/2\) for all \(n > N\). The triangle inequality for \(d(x_m, x_n)\) shows that, for all \(m, n > N\),

\[
   d(x_m, x_n) \leq d(x_m, x) + d(x, x_n) \leq \epsilon/2 + \epsilon/2 = \epsilon.
\]

Therefore, \(x_1, x_2, \ldots\) is a Cauchy sequence. \(\Box\)

**Example 2.1.12.** Let \((X, d)\) be the metric space of rational numbers defined by \(X = \mathbb{Q}\) and \(d(x, y) = |x - y|\). The sequence \(x_1 = 2, x_{n+1} = \frac{1}{2}x_n + \frac{1}{x_n}\) satisfies \(x_n \in \mathbb{Q}\) and, using \(x_{n+1} - \sqrt{2} = \frac{1}{2x_n}(x_n - \sqrt{2})^2\), one can show it is Cauchy. But, it does not converge in \((X, d)\) because its limit point is the irrational number \(\sqrt{2} \notin \mathbb{Q}\).
2.1. METRIC SPACES

2.1.2 Metric Topology

Definition 2.1.13. Let \( W \) be a subset of a metric space \((X, d)\). The set \( W \) is called open if, for every \( w \in W \), there is an \( \epsilon > 0 \) such that \( B_d(w, \epsilon) \subseteq W \).

Theorem 2.1.14. For any metric space \((X, d)\),

1. \( \emptyset \) and \( X \) are open
2. any union of open sets is open
3. any finite intersection of open sets is open

Proof. This proof is left as an exercise for the reader. \( \square \)

One might be curious why only finite intersections are allowed in Theorem 2.1.14. The following example highlights the problem with allowing infinite intersections.

Example 2.1.15. Let \( I_n = \left(-\frac{1}{n}, \frac{1}{n}\right) \subseteq \mathbb{R} \), for \( n \in \mathbb{N} \), be a sequence of open real intervals. The infinite intersection

\[
\bigcap_{n \in \mathbb{N}} I_n = \{x \in \mathbb{R} | \forall n \in \mathbb{N}, x \in I_n\} = \{0\}.
\]

But, it is easy to verify that \( \{0\} \) is not an open set.

Definition 2.1.16. A subset \( W \) of a metric space \((X, d)\) is closed if its complement \( W^c = X - W \) is open.

Corollary 2.1.17. For any metric space \((X, d)\),

1. \( \emptyset \) and \( X \) are closed
2. any intersection of closed sets is closed
3. any finite union of closed sets is closed

Sketch of proof. Using the definition of closed, one can apply De Morgan’s Laws to Theorem 2.1.14 verify this result. \( \square \)
Actually, the sets ∅ and X are both open and closed. Such sets are called clopen. For a non-trivial example, consider the standard metric space of rational numbers and choose \( W = \{ x \in \mathbb{Q} \mid x < \sqrt{2} \} \). This set is open because, for all \( x \in W \), we have \( B(x, \sqrt{2} - x) \subseteq W \). Since \( \sqrt{2} \notin \mathbb{Q} \), it follows that \( U = \{ x \in \mathbb{Q} \mid x \geq \sqrt{2} \} = \{ x \in \mathbb{Q} \mid x > \sqrt{2} \} \) which is open by the same argument. But \( U^c = W \), so \( W \) is also closed.

**Definition 2.1.18.** For any metric space \((X, d)\) and subset \( W \subseteq X \), a point \( x \in X \) is a limit point of \( W \) if there is a sequence \( w_1, w_2, \ldots \in W \setminus \{ x \} \) of distinct elements that converges to \( x \). Equivalently, \( x \) is a limit point of \( W \) if, for all \( \delta > 0 \), the set \( \{ w \in W \mid d(x, w) < \delta \} \) contains some point besides \( x \).

**Problem 2.1.19.** Prove that the two definitions of a limit point are equivalent.

By this definition (which is standard), an isolated point \( w \in W \) is not a limit point because there is no sequence of distinct elements that converges to it. Instead, for any sequence that converges to an isolated point \( w \), there must be an \( N \in \mathbb{N} \) such that \( w_n = w \) for all \( n > N \).

**Theorem 2.1.20.** For any metric space \((X, d)\), a subset \( W \subseteq X \) is closed if and only if it contains all of its limit points.

**Proof.** Assume \( W \) is closed and suppose \( x \notin W \) (i.e., \( x \in W^c \)) is a limit point of \( W \). Since \( W^c \) is open, there is a \( \delta > 0 \) such that \( B(x, \delta) \subseteq W^c \) and no sequence in \( W \) can approach \( x \). This contradicts the supposition that \( x \notin W \) is a limit point and implies all limit points must be in \( W \). On the other hand, if \( W \) contains all its limit points, then no \( x \notin W \) (i.e., \( x \in W^c \)) can be a limit point. Negating the second definition of a limit point and applying it to any \( x \in W^c \), we see that there is a \( \delta > 0 \) such that \( \{ w \in W \mid d(x, w) < \delta \} \) is empty. Thus, \( B_d(x, \delta) \subseteq W^c \) and this implies that \( W^c \) is open. Thus, \( W \) is closed. \( \square \)

It follows that, for a closed subset \( W \subseteq X \), any sequence \( w_n \in W \) that converges must converge to a point \( w \in W \).

**Definition 2.1.21.** For any metric space \((X, d)\) and subset \( W \subseteq X \), a point \( w \in W \) is in the interior of \( W \) if and only if there is a \( \delta > 0 \) such that, for all \( x \in X \) with \( d(x, w) < \delta \), it follows that \( x \in W \).
2.1. METRIC SPACES

Problem 2.1.22. Prove that the interior of a set is open.

Definition 2.1.23. For any metric space \((X, d)\) and subset \(W \subseteq X\), a point \(x \in X\) is in the closure of \(W\) if and only if, for all \(\delta > 0\), there is a \(w \in W\) such that \(d(x, w) < \delta\).

Problem 2.1.24. Prove that the closure of a set contains all its limit points and, thus, is closed.

The interior of \(A\) is denoted by \(A^\circ\) and the closure of \(A\) is denoted by \(\overline{A}\). The boundary \(\partial A\) of a set \(A\) is defined by \(\partial A \equiv \overline{A} \setminus A^\circ\).

2.1.3 Continuity

Let \(f : X \to Y\) be a function between the metric spaces \((X, d_X)\) and \((Y, d_Y)\).

Definition 2.1.25. The function \(f\) is continuous at \(x_0\) if, for any \(\epsilon > 0\), there exists a \(\delta > 0\) such that, for all \(x \in X\) satisfying \(d_X(x_0, x) < \delta\),

\[
d_Y(f(x_0), f(x)) < \epsilon.
\]

In precise mathematical notation, one has

\[
(\forall \epsilon > 0)(\exists \delta > 0)(\forall x \in \{x' \in X \mid d_X(x_0, x') < \delta\}), d_Y(f(x_0), f(x)) < \epsilon.
\]

Theorem 2.1.26. If \(f\) is continuous at \(x_0\), then \(f(x_n) \to f(x_0)\) for all sequences \(x_1, x_2, \ldots \in X\) such that \(x_n \to x_0\). Conversely, if \(f(x_n) \to f(x_0)\) for all sequences \(x_1, x_2, \ldots \in X\) such that \(x_n \to x_0\), then \(f\) is continuous at \(x_0\).

Proof. If \(f\) is continuous at \(x_0\), then, for any \(\epsilon > 0\), there is a \(\delta > 0\) such that \(d_Y(f(x_0), f(x)) < \epsilon\) if \(d_X(x_0, x) < \delta\). If \(x_n \to x_0\), then there is an \(N \in \mathbb{N}\) such that \(d_X(x_n, x_0) < \delta\) for all \(n > N\). Thus, \(d_Y(f(x_0), f(x_n)) < \epsilon\) for all \(n > N\) and \(f(x_n) \to f(x_0)\).

For the converse, we show the contrapositive. If \(f\) is not continuous at \(x_0\), then there exists an \(\epsilon > 0\) such that, for all \(\delta > 0\), there is an \(x \in X\) with \(d_X(x_0, x) < \delta\) and \(d_Y(f(x_0), f(x)) \geq \epsilon\). For this \(\epsilon\) and any positive sequence \(\delta_n \to 0\), let \(x_n\) be the promised \(x\). Then, \(x_n \to x_0\) because \(d_X(x_0, x_n) < \delta_n \to 0\) but \(d_Y(f(x_0), f(x_n)) \geq \epsilon\). Thus, \(f(x_n)\) does not converge to \(f(x_0)\) for some sequence where \(x_n \to x_0\). \(\square\)
Definition 2.1.27. \textbf{The limit of $f$ at $x_0$}, \( \lim_{x \to x_0} f(x) \), exists and equals \( f(x_0) \) if \( f(x_n) \to f(x_0) \) for all sequences \( x_n \in X \) such that \( x_n \to x_0 \). Thus, Theorem 2.1.26 implies that the limit of $f$ exists at $x_0$ if and only if $f$ is continuous at $x_0$.

Definition 2.1.28. The function $f$ is called \textbf{continuous} if, for all $x_0 \in X$, it is continuous at $x_0$. In precise mathematical notation, one has
\[
(\forall x_0 \in X)(\forall \epsilon > 0)(\exists \delta > 0) (\forall x \in \{x' \in X \mid d_X(x_0, x') < \delta\}), d_Y(f(x_0), f(x)) < \epsilon.
\]

Definition 2.1.29. The function $f$ is called \textbf{uniformly continuous} if it is continuous and, for all \( \epsilon > 0 \), the \( \delta > 0 \) can be chosen independently of \( x_0 \). In precise mathematical notation, one has
\[
(\forall \epsilon > 0)(\exists \delta > 0)(\forall x_0 \in X) (\forall x \in \{x' \in X \mid d_X(x_0, x') < \delta\}), d_Y(f(x_0), f(x)) < \epsilon.
\]

Definition 2.1.30. A function $f: X \to Y$ is called \textbf{Lipschitz continuous} on $A \subseteq X$ if there is a constant $L \in \mathbb{R}$ such that \( d_Y(f(x), f(y)) \leq L d_X(x, y) \) for all \( x, y \in A \).

Let \( f_A \) denote the \textbf{restriction} of $f$ to $A \subseteq X$ defined by $f_A: A \to Y$ with $f_A(x) = f(x)$ for all $x \in A$. It is easy to verify that, if $f$ is Lipschitz continuous on $A$, then $f_A$ is uniformly continuous.

Problem 2.1.31. Let \((X, d) \) be a metric space and define $f : X \to \mathbb{R}$ by $f(x) = d(x, x_0)$ for some fixed $x_0 \in X$. Show that $f$ is Lipschitz continuous with $L = 1$.

2.1.4 Properties of the Real Numbers

First, we review notions of extreme values for sets of real numbers. To do this, we will define the \textbf{extended real numbers} \( \mathbb{R} \) by augmenting the real numbers to include limit points for unbounded sequences \( \mathbb{R} \triangleq \mathbb{R} \cup \{\infty, -\infty\} \). Using the metric $d_\mathbb{R}(x, y) \triangleq \left|\frac{x}{1+|x|} - \frac{y}{1+|y|}\right|$, this set is a metric space. Later, we will see that it is actually a compact metric space. The main difference from \( \mathbb{R} \) is that, for \( x_n \in \mathbb{R} \), the statement \( x_n \to \infty \) is well defined and equivalent to \( \forall M > 0, \exists N \in \mathbb{N}, \forall n > N, x_n > M \).

Definition 2.1.32. \textbf{The supremum} (or least upper bound) of $X \subseteq \mathbb{R}$, denoted $\sup X$, is the smallest extended real number $M \in \mathbb{R}$ such that $x \leq M$ for all $x \in X$. It is always well-defined and equals $-\infty$ if $X = \emptyset$. 
Definition 2.1.33. The **maximum** of \( X \subseteq \mathbb{R} \), denoted \( \max X \), is the largest value achieved by the set. It equals \( \sup X \) if \( \sup X \in X \) and is undefined otherwise.

Definition 2.1.34. The **infimum** (or greatest lower bound) of \( X \subseteq \mathbb{R} \), denoted \( \inf X \), is the largest extended real number \( m \in \mathbb{R} \) such that \( x \geq m \) for all \( x \in X \). It is always well-defined and equals \( \infty \) if \( X = \emptyset \).

Definition 2.1.35. The **minimum** of \( X \subseteq \mathbb{R} \), denoted \( \min X \), is the smallest value achieved by the set. It equals \( \inf X \) if \( \inf X \in X \) and is undefined otherwise.

Lemma 2.1.36. Let \( X \) be a set and \( f : X \to \mathbb{R} \) be a function from \( X \) to the real numbers. Let \( M = \sup f(A) \) for some non-empty \( A \subseteq X \). Then, there exists a sequence \( x_1, x_2, \ldots \in A \) such that \( \lim_{n} f(x_n) = M \).

Proof. If \( M = \infty \), then \( f(A) \) has no finite upper bound and, for any \( y \in \mathbb{R} \), there exists an \( x \in A \) such that \( f(x) > y \). In this case, we can let \( x_1 \) be any element of \( A \) and \( x_{n+1} \) be any element of \( A \) such that \( f(x_{n+1}) > f(x_n) + 1 \). In the metric space \((\mathbb{R}, d_{\mathbb{R}})\), this implies that \( d_{\mathbb{R}}(f(x_n), \infty) = |\frac{f(x_n)}{1+|f(x_n)|} - 1| \to 0 \) and thus \( f(x_n) \to \infty \).

If \( M < \infty \), then \( f(A) \) has a finite upper bound and, for any \( \epsilon > 0 \), there is an \( x \) such that \( M - f(x) < \epsilon \). Otherwise, one arrives at the contradiction \( \sup f(A) < M \). Therefore, we can construct the sequence \( x_1, x_2, \ldots \) by choosing \( x_n \in A \) to be any point that satisfies \( M - f(x_n) \leq \frac{1}{n} \).

Theorem 2.1.37. Any bounded non-decreasing sequence of real numbers converges to its supremum.

Proof. Let \( x_1, x_2, \ldots \in \mathbb{R} \) be a sequence satisfying \( x_{n+1} \geq x_n \) and \( x_n \leq M < \infty \) for all \( n \in \mathbb{N} \). Without loss of generality, we can choose the upper bound \( M \) to be the supremum \( \sup \{x_1, x_2, \ldots \} \). Now, we will prove directly that \( x_n \to M \).

First, we note that the definition of the supremum implies that \( x_n \leq M \) for all \( n \in \mathbb{N} \) and, for any \( \epsilon > 0 \), there is an \( N \in \mathbb{N} \) such that \( x_N > M - \epsilon \). Since \( x_n \) is non-decreasing, this implies that \( x_n > M - \epsilon \) for all \( n > N \). Next, it follows from \( x_n \leq M \) that \( |M - x_n| = M - x_n < \epsilon \) for all \( n > N \). Thus, the constructed \( N \) satisfies all elements in the definition of \( x_n \to M \).

Lemma 2.1.38. Let \( y_n \in \mathbb{R} \) be a real sequence. If \( \sum_{i=1}^{\infty} |y_i| = M < \infty \), then \( x_n = \sum_{i=1}^{n} y_i \) satisfies \( x_n \to x \) with \( |x| < M \).
Proof. Let \( w_n = \sum_{i=1}^{n} |y_i| \) and observe that the following inequality holds,

\[
|x_m - x_n| = \left| \sum_{i=n+1}^{m} y_i \right| \leq \sum_{i=n+1}^{m} |y_i| = |w_m - w_n|.
\]

Since \( w_n \) converges, it is Cauchy and the inequality implies that \( x_m \) is Cauchy. Thus, \( x_n \) converges to some \( x \in \mathbb{R} \) and \( |x| < M \) follows from \( |x_n| \leq w_n \leq M \).

Lemma 2.1.39. Let \( y_n \in \mathbb{R} \) be a real sequence and \( x_n = \sum_{i=1}^{n} y_i \) be its sequence of partial sums. Then, \( \sum_{i=1}^{\infty} y_i \triangleq \lim_{n \to \infty} x_n \) exists if and only if the tail of the sum is negligible:

\[
\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall m, n > N, \quad \sum_{i=n+1}^{m} y_i < \epsilon.
\]

Proof. Since \( \mathbb{R} \) is complete, \( \lim_{n \to \infty} x_n \) exists if and only if \( x_n \) is a Cauchy sequence. Thus, \( x_n \) converges if and only if “\( \forall \epsilon > 0, \exists N \in \mathbb{N}, \forall m, n > N, |x_m - x_n| < \epsilon \)”. Thus, the result follows from the fact that \( |x_m - x_n| = \left| \sum_{i=n+1}^{m} y_i \right| \).

2.1.5 Sequences of Functions

Let \( (X, d_X) \) and \( (Y, d_Y) \) be metric spaces and \( f_n : X \to Y \) for \( n \in \mathbb{N} \) be a sequence of functions mapping \( X \) to \( Y \).

Definition 2.1.40. The sequence \( f_n \) converges pointwise to \( f : X \to Y \) if

\[
\lim_{n \to \infty} f_n(x) = f(x)
\]

for all \( x \in X \). Using mathematical symbols, we can write

\[
\forall x \in X, \forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \in \{n' \in \mathbb{N} \mid n' > N\}, d_Y(f_n(x), f(x)) < \epsilon.
\]

Definition 2.1.41. The sequence \( f_n \) converges uniformly to \( f : X \to Y \) if

\[
\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \in \{n' \in \mathbb{N} \mid n' > N\}, \forall x \in X, d_Y(f_n(x), f(x)) < \epsilon.
\]

This condition is also equivalent to

\[
\lim_{n \to \infty} \sup_{x \in X} d_Y(f_n(x), f(x)) = 0.
\]

Theorem 2.1.42. If each \( f_n \) is continuous and \( f_n \) converges uniformly to \( f : X \to Y \), then \( f \) is continuous.
2.1. METRIC SPACES

Proof. The goal is to show that, for all $x \in X$ and any $\epsilon > 0$, there is a $\delta > 0$ such that $d_Y(f(x), f(y)) < \epsilon$ if $d_X(x, y) < \delta$. Since $f_n \to f$ uniformly, for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that $d_Y(f_n(x), f(x)) < \epsilon/3$ for all $n > N$ and all $x \in X$. Now, we can fix $\epsilon > 0$ use the $N$ promised above. Then, for any $n > N$, the continuity of $f_n$ implies that, for all $x \in X$ and any $\epsilon > 0$, there is a $\delta > 0$ such that $d_Y(f_n(x), f_n(y)) < \epsilon/3$ if $d_X(x, y) < \delta$. Thus, if $d_X(x, y) < \delta$, then

\[
\begin{align*}
    d_Y(f(x), f(y)) &\leq d_Y(f(x), f_n(x)) + d_Y(f_n(x), f_n(y)) + d_Y(f_n(y), f(y)) \\
    &< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon.
\end{align*}
\]

\[
\square
\]

2.1.6 Completeness

Suppose $(X, d)$ is a metric space. From Definition 2.1.8, we know that a sequence $x_1, x_2, \ldots$ of points in $X$ converges to $x \in X$ if, for every $\delta > 0$, there exists an integer $N$ such that $d(x_i, x) < \delta$ for all $i \geq N$.

![Figure 2.1](image.jpg)

Figure 2.1: The sequence of continuous functions in Example 2.1.43 satisfies the Cauchy criterion. But, it does not converge to a continuous function in $C[-1, 1]$.

It is possible for a sequence in a metric space $X$ to satisfy the Cauchy criterion, but not to converge in $X$. 
Example 2.1.43. Let $X = C[-1,1]$ be the space of continuous functions that map $[-1,1]$ to $\mathbb{R}$ and satisfy $\|f\|_2 < \infty$, where $\|f\|_2$ denotes the $L^2$ norm

$$\|f\|_2 \triangleq \left( \int_{-1}^{1} |f(t)|^2 dt \right)^{\frac{1}{2}}.$$

This set forms a metric space $(X,d)$ when equipped with the distance

$$d(f, g) \triangleq \|f - g\|_2 = \left( \int_{-1}^{1} |f(t) - g(t)|^2 dt \right)^{\frac{1}{2}}.$$

Consider the sequence of functions $f_n(t)$ given by

$$f_n(t) \triangleq \begin{cases} 0 & t \in [-1, -\frac{1}{n}] \\ \frac{nt^2}{2} + \frac{1}{2} & t \in (-\frac{1}{n}, \frac{1}{n}) \\ 1 & t \in [\frac{1}{n}, 1]. \end{cases}$$

Assuming that $m \geq n$, a bit of calculus shows that

$$d(f_n, f_m) = \|f_n(t) - f_m(t)\|_2 = \left( \int_{-1}^{1} |f_n(t) - f_m(t)|^2 dt \right)^{\frac{1}{2}} = \frac{(m - n)^2}{6mn^2}.$$

Since $m \geq n$, this distance is upper bounded by $\frac{1}{6n}$ and the sequence satisfies the Cauchy criterion. But, it does not converge to a continuous function in $C[-1,1]$.

Definition 2.1.44. A metric space $(X,d)$ is said to be complete if every Cauchy sequence in $(X,d)$ converges to a limit $x \in X$.

The standard metric space of real numbers with absolute distance is a complete metric space. This fact and other foundational properties of the real numbers can be derived formally using the techniques described below. However, a formal construction of the real numbers will not be provided in these notes.

Example 2.1.45. Consider the sequence $x_1 = 2$, $x_{n+1} = \frac{1}{2}x_n + \frac{1}{x_n}$ and observe that $x_n \in \mathbb{Q}$ for all $n \in \mathbb{N}$. We saw earlier that $x_n$ is a Cauchy sequence with limit point $\sqrt{2} \in \mathbb{R}$. But, $\sqrt{2}$ is irrational and thus the rational numbers $\mathbb{Q}$ are not complete.

Theorem 2.1.46. A closed subset $A$ of a complete metric space $X$ is itself a complete metric space.

Proof. Any Cauchy sequence $x_1, x_2, \ldots \in A$ is also a Cauchy sequence in $X$. This implies that $x_n \to x \in X$ and it follows that $x \in \overline{A}$. Since $A$ is closed, $x \in A$. \qed
**Definition 2.1.47.** An isometry is a mapping \( \phi: X \to Y \) between two metric spaces \((X, d_X)\) and \((Y, d_Y)\) that is distance preserving (i.e., it satisfies \(d_X(x, x') = d_Y(\phi(x), \phi(x'))\) for all \(x, x' \in X\)).

**Definition 2.1.48.** A subset \(A\) of a metric space \((X, d)\) is dense in \(X\) if every \(x \in X\) is a limit point of the set \(A\). This is equivalent to its closure \(\overline{A}\) being equal to \(X\).

**Definition 2.1.49.** The completion of a metric space \((X, d_X)\) consists of a complete metric space \((Y, d_Y)\) and an isometry \(\phi: X \to Y\) such that \(\phi(X)\) is a dense subset of \(Y\). Moreover, the completion is unique up to isometry.

**Example 2.1.50.** Consider the metric space \(\mathbb{Q}\) of rational numbers equipped with the metric of absolute distance. The completion of this metric space is \(\mathbb{R}\) because the isometry is given by the identity mapping and \(\mathbb{Q}\) is a dense subset of \(\mathbb{R}\).

Cauchy sequences have many applications in analysis and signal processing. For example, they can be used to construct the real numbers from the rational numbers. In fact, the same approach is used to construct the completion of any metric space.

**Definition 2.1.51.** Two Cauchy sequences \(x_1, x_2, \ldots\) and \(y_1, y_2, \ldots\) are equivalent if, for every \(\epsilon > 0\), there exists an integer \(N\) such that \(d(x_k, y_k) \leq \epsilon\) for all \(k \geq N\).

**Example 2.1.52.** Let \(\mathcal{C}(\mathbb{Q})\) denote the set of all Cauchy sequences \(q_1, q_2, \ldots\) of rational numbers where \(\sim\) represents the equivalence relation on this set defined above. Then, the set of equivalence classes (or quotient set) \(\mathcal{C}(\mathbb{Q})/\sim\) is in one-to-one correspondence with the real numbers. This construction is the standard completion of \(\mathbb{Q}\). Since every Cauchy sequence of rationals converges to a real number, the isometry is given by mapping each equivalence class to its limit point in \(\mathbb{R}\).

**Definition 2.1.53.** Let \(A\) be a subset of a metric space \((X, d)\) and \(f: X \to X\) be a function. Then, \(f\) is a contraction on \(A\) if \(f(A) \subseteq A\) and there exists a constant \(\gamma < 1\) such that \(d(f(x), f(y)) \leq \gamma d(x, y)\) for all \(x, y \in A\).

Consider the following important results in applied mathematics: Picard’s uniqueness theorem for differential equations, the implicit function theorem, and the existence of stationary optimal policies for Markov decision processes. What do they
have in common? They each establish the existence and uniqueness of a function and have relatively simple proofs based on the contraction mapping theorem.

**Theorem 2.1.54** (Contraction Mapping Theorem). Let $(X, d)$ be a complete metric space and $f$ be contraction on a closed subset $A \subseteq X$. Then, $f$ has a unique fixed point $x^*$ in $A$ such that $f(x^*) = x^*$ and the sequence $x_{n+1} = f(x_n)$ converges to $x^*$ for any point $x_1 \in A$. Moreover, $x_n$ satisfies the error bounds $d(x^*, x_n) \leq \gamma^{n-1}d(x^*, x_1)$ and $d(x^*, x_{n+1}) \leq d(x_n, x_{n+1})\gamma/(1-\gamma)$.

**Proof.** Suppose $f$ has two fixed points $y, z \in A$. Then, $d(y, z) = d(f(y), f(z)) \leq \gamma d(y, z)$ and $d(y, z) = 0$ because $\gamma \in [0, 1)$. This shows that $y = z$ and any two fixed points in $A$ must be identical. If $x^*$ is a fixed point, then $d(x^*, x_{n+1}) = d(f(x^*), f(x_n)) \leq \gamma d(x^*, x_n)$ and, by induction, one gets the first error bound.

Since $d(f(x_n), f(x_{n+1})) \leq \gamma d(x_n, x_{n+1})$, induction shows that $d(x_n, x_{n+1}) \leq \gamma^{n-1}d(x_1, x_2)$. Using this, we can bound the distance $d(x_m, x_n)$ (for $m < n$) with

$$d(x_m, x_n) \leq d(x_m, x_{m+1}) + d(x_{m+1}, x_n)$$

$$\leq \sum_{i=m}^{n-1} d(x_i, x_{i+1}) \leq \sum_{i=m}^{n-1} \gamma^{i-1}d(x_1, x_2)$$

$$\leq \sum_{i=m}^{\infty} \gamma^{i-1}d(x_1, x_2) \leq \frac{\gamma^{m-1}}{1-\gamma}d(x_1, x_2). \quad (2.1)$$

The sequence $x_n$ is Cauchy because $d(x_m, x_n)$ can be made arbitrarily small (for all $n > m$) by increasing $m$. As $(X, d)$ is complete, it follows that $x_n \to x^*$ for some $x^* \in X$. Since $f$ is Lipschitz continuous, this implies that $x^* = \lim_n x_n = \lim_n f(x_n) = f(x^*)$ the unique fixed point of $f$ in $A$. Since $x_n \to x^*$, we can use essentially the same argument to get the second error bound

$$d(x_{n+1}, x^*) \leq \sum_{i=n+1}^{\infty} d(x_i, x_{i+1}) \leq \sum_{i=n+1}^{\infty} \gamma^{i-n}d(x_n, x_{n+1}) = \frac{\gamma}{1-\gamma}d(x_n, x_{n+1}). \quad \square$$

**Example 2.1.55.** Consider the cosine function restricted to the subset $[0, 1] \subseteq \mathbb{R}$. Since $\cos(x)$ is decreasing for $0 \leq x < \pi$, we have $\cos([0, 1]) = [\cos(1), 1]$ with $\cos(1) \approx 0.54$. The mean value theorem of calculus also tells us that $\cos(y) - \cos(x) = \cos'(t)(y - x)$ for some $t \in [x, y]$. Since $\cos'(t) = -\sin(t)$ and $\sin(t)$ is increasing on $[0, 1]$, we find that $\sin([0, 1]) = [0, \sin(1)]$ with $\sin(1) \approx 0.84$. 

2.1. Metric Spaces

Figure 2.2: Starting from $x_1 = 0.2$, the iteration in Example 2.1.55 maps $x_n$ to $x_{n+1} = \cos(x_n)$. The points are also connected to the slope-1 line to show the path.

Taking the absolute value, shows that $|\cos(y) - \cos(x)| \leq 0.85|y - x|$. Therefore, $\cos(t)$ is a contraction on $[0, 1]$ and the sequence $x_{n+1} = \cos(x_n)$ (e.g., see Figure 2.2) converges to the unique fixed point $x^* = \cos(x^*)$ for all $x_1 \in [0, 1]$.

2.1.7 Compactness

Definition 2.1.56. A metric space $(X, d)$ is totally bounded if, for any $\epsilon > 0$, there exists a finite set of $B_d(x, \epsilon)$ balls that cover (i.e., whose union equals) $X$.

Definition 2.1.57. A metric space is compact if it is complete and totally bounded.

The closed interval $[0, 1] \subset \mathbb{R}$ is compact. In fact, a subset of $\mathbb{R}^n$ is compact if and only if it is closed and bounded. On the other hand, the standard metric space of real numbers is not compact because it is not totally bounded.

Theorem 2.1.58. A closed subset $A$ of a compact space $X$ is itself a compact space.

The following theorem highlights one of the main reasons that compact spaces are desirable in practice.

Theorem 2.1.59. Let $(X, d)$ be a compact metric space and $x_1, x_2, \ldots \in X$ be a sequence. Then, there is a subsequence $x_{n_1}, x_{n_2}, \ldots$, defined by some increasing sequence $n_1, n_2, \ldots \in \mathbb{N}$, that converges.
Proof. We proceed by recursively constructing subsequences \( z_n^{(k)} \) starting from \( z_n^{(0)} = x_n \). Since \( X \) is totally bounded, let \( C_k \subset X \) be the centers of a finite set of balls with radius \( 2^{-k} \) that cover \( X \) (i.e., \( \bigcup_{x \in C_k} B(x, 2^{-k}) = X \)). Then, one of these balls (say centered at \( x' \)) must contain infinitely many elements in \( z_n^{(k-1)} \) (i.e., \( \exists x' \in C_k, |\{ n \in \mathbb{N} | z_n^{(k-1)} \in B(x', 2^{-k}) \}| = \infty \)). Next, we extract the subsequence contained in this ball by choosing \( z_n^{(k)} \) to be the subsequence of \( z_n^{(k-1)} \) contained in \( B(x', 2^{-k}) \). From the triangle inequality, it follows that \( d(y, y') < 2(2^{-k}) \) for all \( y, y' \in B(x', 2^{-k}) \). Thus, \( d(z_m^{(k')}, z_n^{(k)}) < 2^{-k+1} \) for all \( m > n \geq 1 \) and \( k' \geq k \geq 1 \).

Let \( I(k, n) \) be the index in the original sequence associated with \( z_n^{(k)} \). Since each stage only removes elements from the previous subsequence and relabels, it follows that \( I(k+1, k+1) \geq I(k, k+1) > I(k, k) \). This implies that the sequence \( y_k = z_k^{(k)} = x_{I(k,k)} \) is a subsequence of \( x_n \) and \( d(y_m, y_k) \leq 2^{-k+1} \) for all \( m > k \) and \( k \geq 1 \). Thus, for any \( \epsilon > 0 \), choosing \( N = \lceil \log_2 \frac{1}{\epsilon} \rceil + 1 \) shows that \( y_k \) is a Cauchy sequence. Since \( X \) is complete, it follows that \( y_k \) converges to some \( y \in X \). \( \square \)

Functions from compact sets to the real numbers are very important in practice.

**Theorem 2.1.60.** Let \( X \) be a metric space and \( f : X \to \mathbb{R} \) be a continuous function from \( X \) to the real numbers. If \( A \) is a compact subset of \( X \), then there exists \( x \in A \) such that \( f(x) = \sup f(A) \) (i.e., \( f \) achieves a maximum on \( A \)).

**Proof.** Using Lemma 2.1.36 one finds that there is a sequence \( x_1, x_2, \ldots \in A \) such that \( \lim_n f(x_n) = \sup f(A) \). Since \( A \) is compact, there must also be a subsequence \( x_{n_1}, x_{n_2}, \ldots \) that converges. As \( A \) is closed, this subsequence must converge to some \( x^* \in A \). Finally, the continuity of \( f \) shows that

\[
\sup f(A) = \lim_n f(x_n) = \lim_k f(x_{n_k}) = f(\lim_k x_{n_k}) = f(x^*).
\]

**Corollary 2.1.61.** Let \((X, d)\) be a metric space. Then, a continuous function from a compact subset \( A \subseteq X \) to the real numbers achieves a minimum on \( A \).

### 2.2 General Topology*

While topology originated with the study of sets of finite-dimensional real vectors, its mathematical abstraction can also be useful. We note that some of the terms used
2.2. GENERAL TOPOLOGY*

above, for metric spaces, are redefined below. Fortunately, these new definitions are compatible with the old ones when the topology is generated by a metric.

**Definition 2.2.1.** A **topology** on a set $X$ is a collection $\mathcal{J}$ of subsets of $X$ that satisfies the following properties,

1. $\emptyset$ and $X$ are in $\mathcal{J}$
2. the union of the elements of any subcollection of $\mathcal{J}$ is in $\mathcal{J}$
3. the intersection of the elements of any finite subcollection of $\mathcal{J}$ is in $\mathcal{J}$.

A subset $A \subseteq X$ is called an **open set** of $X$ if $A \in \mathcal{J}$. Using this terminology, a topological space is a set $X$ together with a collection of subsets of $X$, called open sets, such that $\emptyset$ and $X$ are both open and such that arbitrary unions and finite intersections of open sets are open.

**Definition 2.2.2.** If $X$ is a set, a **basis** for a topology on $X$ is a collection $\mathcal{B}$ of subsets of $X$ (called basis elements) such that:

1. for each $x \in X$, there exists a basis element $B$ containing $x$.
2. if $x \in B_1$ and $x \in B_2$ where $B_1, B_2 \in \mathcal{B}$, then there exists a basis element $B_3$ containing $x$ such that $B_3 \subseteq B_1 \cap B_2$.
3. a subset $A \subseteq X$ is open in the topology on $X$ generated by $\mathcal{B}$ if and only if, for every $x \in A$, there exists a basis element $B \in \mathcal{B}$ such that $x \in B$ and $B \subseteq A$.

Probably the most important and frequently used way of imposing a topology on a set is to define the topology in terms of a metric.

**Example 2.2.3.** If $d$ is a metric on the set $X$, then the collection of all $\epsilon$-balls

$$\{B_d(x, \epsilon) | x \in X, \epsilon > 0\}$$

is a basis for a topology on $X$. This topology is called the **metric topology** induced by $d$.

Applying the meaning of open set from Definition 2.2.2 to this basis, one finds that a set $A$ is open if and only if, for each $x \in A$, there exists a $\delta > 0$ such that $B_d(x, \delta) \subseteq A$. Clearly, this condition agrees with the definition of $d$-open from Definition 2.1.13.
**Definition 2.2.4.** Let $X$ be a topological space. This space is said to be **metrizable** if there exists a metric $d$ on the set $X$ that induces the topology of $X$.

We note that definitions and results in Sections 2.1.6 and 2.1.7 for metric spaces actually apply to any metrizable space. For example, a metrizable space is complete if and only if there the metric that induces its topology also defines a complete metric space.

**Example 2.2.5.** While most of the spaces discussed in these notes are metrizable, there is a very common notion of convergence that is not metrizable. The topology on the set of functions $f : [0, 1] \to \mathbb{R}$ where the open sets are defined by pointwise convergence is not metrizable.

### 2.2.1 Closed Sets and Limit Points

**Definition 2.2.6.** A subset $A$ of a topological space $X$ is **closed** if the set

$$A^c = X - A = \{x \in X | x \notin A\}$$

is open.

Note that a set can be open, closed, both, or neither! It can be shown that the collection of closed subsets of a space $X$ has properties similar to those satisfied by the collection of open subsets of $X$.

**Fact 2.2.7.** Let $X$ be a topological space. The following conditions hold,

1. $\emptyset$ and $X$ are closed
2. arbitrary intersections of closed sets are closed
3. finite unions of closed sets are closed.

**Definition 2.2.8.** Given a subset $A$ of a topological space $X$, the **interior** of $A$ is defined as the union of all open sets contained in $A$. The **closure** of $A$ is defined as the intersection of all closed sets containing $A$.

The interior of $A$ is denoted by $A^\circ$ and the closure of $A$ is denoted by $\overline{A}$. We note that $A^\circ$ is open and $\overline{A}$ is closed. Furthermore, $A^\circ \subseteq A \subseteq \overline{A}$. 
2.2. GENERAL TOPOLOGY*

Theorem 2.2.9. Let $A$ be a subset of the topological space $X$. The element $x$ is in $\overline{A}$ if and only if every open set $B$ containing $x$ intersects $A$.

Proof. We prove instead the equivalent contrapositive statement: $x \notin \overline{A}$ if and only if there is an open set $B$ containing $x$ that does not intersect $A$. Clearly, if $x \notin \overline{A}$, then $\overline{A}^c = X - \overline{A}$ is an open set containing $x$ that does not intersect $A$. Conversely, if there is an open set $B$ containing $x$ that does not intersect $A$, then $B^c = X - B$ is a closed set containing $A$. The definition of closure implies that $B^c$ must also contain $\overline{A}$. But $x \notin B^c$, so $x \notin \overline{A}$. $\square$

Definition 2.2.10. An open set $O$ containing $x$ is called a neighborhood of $x$.

Definition 2.2.11. Suppose $A$ is a subset of the topological space $X$ and let $x$ be an element of $X$. Then $x$ is a limit point of $A$ if every neighborhood of $x$ intersects $A$ in some point other than $x$ itself.

In other words, $x \in X$ is a limit point of $A \subset X$ if $x \in \overline{A - \{x\}}$, the closure of $A - \{x\}$. The point $x$ may or may not be in $A$.

Theorem 2.2.12. A subset of a topological space is closed if and only if it contains all its limit points.

Definition 2.2.13. A subset $A$ of a topological space $X$ is dense in $X$ if every $x \in X$ is a limit point of the set $A$. This is equivalent to its closure $\overline{A}$ being equal to $X$.

Definition 2.2.14. A topological space $X$ is separable if it contains a countable subset that is dense in $X$.

Example 2.2.15. Since every real number is a limit point of rational numbers, it follows that $\mathbb{Q}$ is a dense subset of $\mathbb{R}$. This also implies that $\mathbb{R}$, the standard metric space of real numbers, is separable.

2.2.2 Continuity

Definition 2.2.16. Let $X$ and $Y$ be topological spaces. A function $f : X \rightarrow Y$ is continuous if for each open subset $O \subseteq Y$, the set $f^{-1}(O)$ is an open subset of $X$.

Recall that $f^{-1}(B)$ is the set $\{x \in X | f(x) \in B\}$. Continuity of a function depends not only upon the function $f$ itself, but also on the topologies specified for its domain and range!
Theorem 2.2.17. Let $X$ and $Y$ be topological spaces and consider a function $f : X \to Y$. The following are equivalent:

1. $f$ is continuous
2. for every subset $A \subseteq X$, $f(\overline{A}) \subseteq \overline{f(A)}$
3. for every closed set $C \subseteq Y$, the set $f^{-1}(C)$ is closed in $X$.

Proof. ($1 \Rightarrow 2$). Assume $f$ is a continuous function. We wish to show $f(\overline{A}) \subseteq \overline{f(A)}$ for every subset $A \subseteq X$. To begin, suppose $A$ is fixed and let $y \in f(\overline{A})$. Then, there exists $x \in \overline{A}$ such that $f(x) = y$. Let $O \subseteq Y$ be a neighborhood of $f(x)$. Preimage $f^{-1}(O)$ is an open set containing $x$ because $f$ is continuous. Since $x \in \overline{A} \cap f^{-1}(O)$, we gather that $f^{-1}(O)$ must intersect with $A$ in some point $x'$. Moreover, $f(x') \in f(f^{-1}(O)) \subseteq O$ and $f(x') \in f(A)$. Thus, $O$ intersects with $f(A)$ in the point $f(x')$. Since $O$ is an arbitrary neighborhood of $f(x)$, we deduce that $f(x) \in \overline{f(A)}$ by Theorem 2.2.9. Collecting these results, we get that any $y \in f(A)$ is also in $\overline{f(A)}$.

($2 \Rightarrow 3$). For this step, we assume that $f(\overline{A}) \subseteq \overline{f(A)}$ for every subset $A \subseteq X$. Let $C \subseteq Y$ be a closed set and let $A = f^{-1}(C)$. Then, $f(A) = f(f^{-1}(C)) \subseteq C$. If $x \in \overline{A}$, we get

$$f(x) \in f(\overline{A}) \subseteq \overline{f(A)} \subseteq C = C.$$ 

So that $x \in f^{-1}(C) = A$ and, as a consequence, $\overline{A} \subseteq A$. Thus, $A = \overline{A}$ is closed.

($3 \Rightarrow 1$). Let $O$ be an open set in $Y$. Let $O^c = Y - O$; then $O^c$ is closed in $Y$. By assumption, $f^{-1}(O^c)$ is closed in $X$. Using elementary set theory, we have

$$X - f^{-1}(O^c) = \{x \in X | f(x) \notin O^c\} = \{x \in X | f(x) \in O\} = f^{-1}(O).$$

That is, $f^{-1}(O)$ is open. 

\[\square\]

Theorem 2.2.18. Suppose $X$ and $Y$ are two metrizable spaces with metrics $d_X$ and $d_Y$. Consider a function $f : X \to Y$. The function $f$ is continuous if and only if it is $d$-continuous with respect to these metrics.

Proof. Suppose that $f$ is continuous. For any $x_1 \in X$ and $\epsilon > 0$, let $O_y = B_{d_Y}(f(x_1), \epsilon)$ and consider the set

$$O_x = f^{-1}(O_y)$$
2.2. GENERAL TOPOLOGY*

Figure 2.3: The function \( f(x) = \frac{1}{1+|x|} \) is continuous. The set of integers \( \mathbb{Z} \) is closed. Yet, the image of this set, \( f(\mathbb{Z}) = \{1/n : n \in \mathbb{N}\} \), is not closed. Thus, this is an example of a continuous function along with a set for which \( f(\mathbb{Z}) \not\subseteq f(\overline{\mathbb{Z}}) \).

which is open in \( X \) and contains the point \( x_1 \). Since \( O_x \) is open and \( x_1 \in O_x \), there exists a \( d \)-open ball \( B_{d_X}(x_1, \delta) \) of radius \( \delta > 0 \) centered at \( x_1 \) such that \( B_{d_X}(x_1, \delta) \subset O_x \). We also see that \( f(x_2) \in O_y \) for any \( x_2 \in B_{d_X}(x_1, \delta) \) because \( A \subseteq O_x \) implies \( f(A) \subseteq O_y \). It follows that \( d_Y(f(x_1), f(x_2)) < \epsilon \) for all \( x_2 \in B_{d_X}(x_1, \delta) \).

Conversely, let \( O_y \) be an open set in \( Y \) and suppose that the function \( f \) is \( d \)-continuous with respect to \( d_X \) and \( d_Y \). For any \( x \in f^{-1}(O_y) \), there exists a \( d \)-open ball \( B_{d_Y}(f(x), \epsilon) \) of radius \( \epsilon > 0 \) centered at \( f(x) \) that is entirely contained in \( O_y \). By the definition of \( d \)-continuous, there exits a \( d \)-open ball \( B_{d_X}(x, \delta) \) of radius \( \delta > 0 \) centered at \( x \) such that \( f(B_{d_X}(x, \delta)) \subset B_{d_Y}(f(x), \epsilon) \). Therefore, every \( x \in f^{-1}(O_y) \) has a neighborhood in the same set, and that implies \( f^{-1}(O_y) \) is open.

\[ \square \]

**Definition 2.2.19.** A sequence \( x_1, x_2, \ldots \) of points in \( X \) is said to converge to \( x \in X \) if for every neighborhood \( O \) of \( x \) there exists a positive integer \( N \) such that \( x_i \in O \) for all \( i \geq N \).

A sequence need not converge at all. However, if it converges in a metrizable space, then it converges to only one element.

**Theorem 2.2.20.** Suppose that \( X \) is a metrizable space, and let \( A \subseteq X \). There
exists a sequence of points of $A$ converging to $x$ if and only if $x \in \overline{A}$.

Proof. Suppose $x_n \to x$, where $x_n \in A$. Then, for every open set $O$ containing $x$, there is an $N$, such that $x_n \in O$ for all $n > N$. By Theorem 2.2.9, this implies that $x \in \overline{A}$. Let $d$ be a metric for the topology of $X$ and $x$ be a point in $\overline{A}$. For each positive integer $n$, consider the neighborhood $B_d \left( x, \frac{1}{n} \right)$. Since $x \in \overline{A}$, the set $A \cap B_d \left( x, \frac{1}{n} \right)$ is not empty and we choose $x_n$ to be any point in this set. It follows that the sequence $x_1, x_2, \ldots$ converges to $x$. Notice that the “only if” proof holds for any topological space, while “if” requires a metric.

Theorem 2.2.21. Let $f : X \to Y$ where $X$ is a metrizable space. The function $f$ is continuous if and only if for every convergent sequence $x_n \to x$ in $X$, the sequence $f(x_n)$ converges to $f(x)$.

Proof. Suppose that $f$ is continuous. Let $O$ be a neighborhood of $f(x)$. Then $f^{-1}(O)$ is a neighborhood of $x$, and so there exists an integer $N$ such that $x_n \in f^{-1}(O)$ for $n \geq N$. Thus, $f(x_n) \in O$ for all $n \geq N$ and $f(x_n) \to f(x)$.

To prove the converse, assume that the convergent sequence condition is true. Let $A \subseteq X$. Since $X$ is metrizable, one finds that $x \in \overline{A}$ implies that there exists a sequence $x_1, x_2, \ldots$ of points of $A$ converging to $x$. By assumption, $f(x_n) \to f(x)$.
Since \( f(x_n) \in f(A) \), Theorem 2.2.17 implies that \( f(x) \in \overline{f(A)} \). Hence \( f(A) \subseteq \overline{f(A)} \) and \( f \) is continuous.
Chapter 3

Linear Algebra

3.1 Fields

This section focuses on key properties of the real and complex numbers that make them useful for linear algebra. Consider a set $F$ of objects and two operations on the elements of $F$, addition and multiplication. For every pair of elements $s, t \in F$ then their sum $(s + t) \in F$. For every pair of elements $s, t \in F$ then their product $st \in F$. Suppose that these two operations satisfy

1. addition is commutative: $s + t = t + s \forall s, t \in F$
2. addition is associative: $r + (s + t) = (r + s) + t \forall r, s, t \in F$
3. to each $s \in F$ there exists a unique element $(-s) \in F$ such that $s + (-s) = 0$
4. multiplication is commutative: $st = ts \forall s, t \in F$
5. multiplication is associative: $r(st) = (rs)t \forall r, s, t \in F$
6. there is a unique non-zero element $1 \in F$ such that $s1 = s \forall s \in F$
7. to each $s \in F - 0$ there exists a unique element $s^{-1} \in F$ such that $ss^{-1} = 1$
8. multiplication distributes over addition: $r(s + t) = rs + rt \forall r, s, t \in F$.

Then, the set $F$ together with these two operations is a field.
Example 3.1.1. The real numbers with the usual operations of addition and multiplication form a field. The complex numbers with these two operations also form a field.

Example 3.1.2. The set of integers with addition and multiplication is not a field.

Problem 3.1.3. Is the set of rational numbers a subfield of the real numbers?

Example 3.1.4. Is the set of all real numbers of the form \( s + t\sqrt{2} \), where \( s \) and \( t \) are rational, a subfield of the complex numbers?

The set \( F = \{ s + t\sqrt{2} : s, t \in \mathbb{Q} \} \) together with the standard addition and multiplication is a field. Let \( s, t, u, v \in \mathbb{Q} \),

\[
( s + t\sqrt{2} ) ( u + v\sqrt{2} ) = (su + 2tv) + (sv + tu)\sqrt{2} \in F
\]

\[
( s + t\sqrt{2} )^{-1} = \frac{s - t\sqrt{2}}{s^2 + 2t^2} = \frac{s}{s^2 + 2t^2} - \frac{t}{s^2 + 2t^2}\sqrt{2} \in F
\]

Again, the remaining properties are straightforward to prove. The field \( s + t\sqrt{2} \), where \( s \) and \( t \) are rational, is a subfield of the complex numbers.

3.2 Matrices

Let \( F \) be a field and consider the problem of finding \( n \) scalars \( x_1, \ldots, x_n \) which satisfy the conditions

\[
\begin{align*}
  a_{11}x_1 &+ a_{12}x_2 + \cdots + a_{1n}x_n = y_1 \\
  a_{21}x_1 &+ a_{22}x_2 + \cdots + a_{2n}x_n = y_2 \\
  \vdots &+ \vdots + \vdots = \vdots \\
  a_{m1}x_1 &+ a_{m2}x_2 + \cdots + a_{mn}x_n = y_m
\end{align*}
\]

(3.1)

where \( y_1, \ldots, y_n \in F \) and \( a_{ij} \in F \) for \( 1 \leq i \leq m \) and \( 1 \leq j \leq n \). These conditions form a system of \( m \) linear equations in \( n \) unknowns. A shorthand notation for (3.1) is the matrix equation

\[ Ax = y. \]
where \( x = (x_1, \ldots, x_n)^T \), \( y = (y_1, \ldots, y_m)^T \), and \( A \) is the matrix given by

\[
A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}.
\]

We also use \([A]_{i,j}\) to denote the entry of \( A \) in the \( i \)-th row and \( j \)-th column (i.e., \( a_{ij} \)) and \([x]_i\) to denote the \( i \)-th entry in \( x \) (i.e., \( x_i \)).

**Definition 3.2.1.** Let \( A \) be an \( m \times n \) matrix over \( F \) and let \( B \) be an \( n \times p \) matrix over \( F \). The **matrix product** \( AB \) is the \( m \times p \) matrix \( C \) whose \( i, j \) entry is

\[
c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}. \tag{3.2}
\]

**Remark 3.2.2.** Consider (3.2) when \( j \) is fixed and \( i \) is eliminated by grouping the elements of \( C \) and \( A \) into column vectors \( c_1, \ldots, c_p \) and \( a_1, \ldots, a_n \). For this case, (3.2) shows that the \( j \)-th column of \( C \) is a linear combination of the columns of \( A \),

\[
c_j = \sum_{r=1}^{n} a_r b_{rj},
\]

Similarly, one can fix \( i \) and eliminate the index \( j \) by grouping the elements of \( C \) and \( B \) into row vectors \( c_1, \ldots, c_m \) and \( b_1, \ldots, b_n \). Then, (3.2) shows that the \( i \)-th row of \( C \) is a linear combination of the rows of \( B \),

\[
c_i = \sum_{r=1}^{n} a_{ir} b_r.
\]

**Definition 3.2.3.** Consider an \( m \times n \) matrix \( A \) with elements \( a_{ij} \in F \). The **transpose** of \( A \) is the \( n \times m \) matrix \( B = A^T \) with elements defined by \( b_{ij} = a_{ji} \).

**Definition 3.2.4.** Consider a complex \( m \times n \) matrix \( A \) with elements \( a_{ij} \in \mathbb{C} \). Its **Hermitian transpose** \( B = A^H \) is the \( n \times m \) matrix with elements defined \( b_{ij} = \overline{a_{ji}} \), where \( \overline{a} \) denotes the complex conjugate of \( a \).

**Problem 3.2.5.** For matrices \( A \in \mathbb{C}^{m \times p} \) and \( B \in \mathbb{C}^{p \times n} \), show \((AB)^H = B^H A^H\).

**Definition 3.2.6.** An \( m \times n \) matrix \( A \) over \( F \) is in **row echelon form** if
1. all rows containing only zeros, if they exist, are the bottom of the matrix, and

2. For rows with non-zero entries, the leading coefficient (i.e., the first non-zero element from the left) is strictly to the right of the leading coefficient of the row above it.

These two conditions imply that entries below the leading coefficient in a column are zero. A matrix is **column echelon form** if its transpose is in row echelon form.

**Definition 3.2.7.** An \( m \times n \) matrix \( A \) over \( F \) is in **reduced row echelon form** if it is in row echelon form and

1. every leading coefficient is 1, and

2. every leading coefficient is the only non-zero element in its column.

**Definition 3.2.8.** Let \( A \) be an \( n \times n \) matrix over \( F \). An \( n \times n \) matrix \( B \) is called the **inverse** of \( A \) if

\[
AB = BA = I.
\]

In this case, \( A \) is called **invertible** and its inverse is denoted by \( A^{-1} \).

**Problem 3.2.9.** For a matrix \( A \in \mathbb{C}^{n\times n} \), show that \((A^H)^{-1} = (A^{-1})^H \) if \( A^{-1} \) exists.

**Definition 3.2.10.** An **elementary row operation** on an \( m \times n \) matrix consists of

1. multiplying a row by a non-zero scalar,

2. swapping two rows, or

3. adding a scalar multiple of one row to another row.

An **elementary column operation** is the same but applied to the columns.

**Lemma 3.2.11.** For any \( m \times n \) matrix \( A \) over \( F \), there is an invertible \( m \times m \) matrix \( P \) over \( F \) such that \( R = PA \) is in reduced row echelon form.

**Sketch of Proof.** This follows from the fact that elementary row operations (i.e., Gaussian elimination) can be used to reduce any matrix to reduced row echelon form. To construct the \( P \) matrix, one applies Gaussian elimination to the augmented matrix \( A' = [A \ I] \). This results in an augmented matrix \( R' = [R \ P] \) in reduced row echelon form. It follows that \( R \) is also in reduced row echelon form. Since elementary row operations can be implemented by (invertible) matrix multiplies on the left side, one also finds that \( R' = PA' \), \( R = PA \), and \( P \) is invertible. \( \square \)
3.3. VECTOR SPACES

**Lemma 3.2.12.** Let $A$ be an $m \times n$ matrix over $F$ with $m < n$. Then, there exists a length-$n$ column vector $\mathbf{x} \neq \mathbf{0}$ (over $F$) such that $A\mathbf{x} = \mathbf{0}$.

**Proof.** First, we use row reduction to compute the reduced row echelon form $R = PA$ of $A$, where $P$ is invertible. Then, we observe that the columns of $R$ containing leading elements can be combined in a linear combination to cancel any other column of $R$. This allows us to construct a vector $\mathbf{x}$ satisfying $R\mathbf{x} = \mathbf{0}$ and thus $A\mathbf{x} = P^{-1}R\mathbf{x} = \mathbf{0}$.

3.3 Vector Spaces

**Definition 3.3.1.** A vector space consists of the following,

1. a field $F$ of scalars
2. a set $V$ of objects, called vectors
3. an operation called vector addition, which associates with each pair of vectors $\mathbf{v}, \mathbf{w} \in V$ a vector $\mathbf{v} + \mathbf{w} \in V$ such that
   (a) addition is commutative: $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$
   (b) addition is associative: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
   (c) there is a unique vector $\mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$, $\forall \mathbf{v} \in V$
   (d) to each $\mathbf{v} \in V$ there is a unique vector $-\mathbf{v} \in V$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
4. an operation called scalar multiplication, which associates with each $s \in F$ and $\mathbf{v} \in V$ a vector $s\mathbf{v} \in V$ such that
   (a) $1\mathbf{v} = \mathbf{v}$, $\forall \mathbf{v} \in V$
   (b) $(s_1s_2)\mathbf{v} = s_1(s_2\mathbf{v})$
   (c) $s(\mathbf{v} + \mathbf{w}) = s\mathbf{v} + s\mathbf{w}$
   (d) $(s_1 + s_2)\mathbf{v} = s_1\mathbf{v} + s_2\mathbf{v}$.

**Example 3.3.2.** Let $F$ be a field, and let $V$ be the set of all $n$-tuples $\mathbf{v} = (v_1, \ldots, v_n)$ of scalar $v_i \in F$. If $\mathbf{w} = (w_1, \ldots, w_n)$ with $w_i \in F$, the sum of $\mathbf{v}$ and $\mathbf{w}$ is defined by

$$\mathbf{v} + \mathbf{w} = (v_1 + w_1, \ldots, v_n + w_n).$$
The product of a scalar \( s \in F \) and vector \( v \) is defined by
\[
sv = (sv_1, \ldots, sv_n).
\]
The set of \( n \)-tuples, denoted by \( F^n \), with the vector addition and scalar product defined above forms a vector space. This is the standard vector space for \( F^n \).

**Example 3.3.3.** Let \( X \) be a non-empty set and let \( Y \) be a vector space over \( F \). Consider the set \( V \) of all functions from \( X \) into \( Y \). The sum of two vectors \( f, g \in V \) is the function from \( X \) into \( Y \) defined by
\[
(f + g)(x) = f(x) + g(x) \quad \forall x \in X,
\]
where the RHS uses vector addition from \( Y \). The product of scalar \( s \in F \) and the function \( f \in V \) is the function \( sf \) defined by
\[
(sf)(x) = sf(x) \quad \forall x \in X,
\]
where the RHS uses scalar multiplication from \( Y \). This is the standard vector space of functions from a set \( X \) to a vector space \( Y \).

**Definition 3.3.4.** A vector \( w \in V \) is said to be a **linear combination** of the vectors \( v_1, \ldots, v_n \in V \) provided that there exist scalars \( s_1, \ldots, s_n \in F \) such that
\[
w = \sum_{i=1}^{n} s_i v_i.
\]

### 3.3.1 Subspaces

**Definition 3.3.5.** Let \( V \) be a vector space over \( F \). A **subspace** of \( V \) is a subset \( W \subset V \) which is itself a vector space over \( F \).

**Fact 3.3.6.** A non-empty subset \( W \subset V \) is a subspace of \( V \) if and only if for every pair \( w_1, w_2 \in W \) and every scalar \( s \in F \) the vector \( sw_1 + w_2 \) is again in \( W \).

If \( V \) is a vector space then the intersection of any collection of subspaces of \( V \) is a subspace of \( V \).

**Example 3.3.7.** Let \( A \) be an \( m \times n \) matrix over \( F \). The set of all \( n \times 1 \) column vectors \( V \) such that
\[
v \in V \implies Av = 0
\]
is a subspace of \( F^{n \times 1} \).
3.3. VECTOR SPACES

Definition 3.3.8. Let $U$ be a set (or list) of vectors in $V$. The \textbf{span} of $U$, denoted $\text{span}(U)$, is defined to be the set of all finite linear combinations of vectors in $U$.

The subspace spanned by $U$ can be defined equivalently as the intersection of all subspaces of $V$ that contain $U$. To see this, we note that the intersection of all subspaces containing $U$ is a subspace containing $U$ because the intersection of subspaces is also a subspace. The intersection cannot be larger than $\text{span}(U)$, however, because $\text{span}(U)$ is a subspace containing $U$.

Definition 3.3.9. Let $V$ be a vector space and $U, W$ be subspaces. If $U, W$ are disjoint (i.e., $U \cap W = \{0\}$), their \textbf{direct sum} $U \oplus W$ is defined by

$$U \oplus W \triangleq \{ u + w | u \in U, w \in W \}.$$  

An important property of a direct sum is that any vector $v \in U \oplus W$ has a unique decomposition $v = u + w$ where $u \in U$ and $w \in W$.

3.3.2 Bases and Dimensions

The dimension of a vector space is defined using the concept of a basis.

Definition 3.3.10. Let $V$ be a vector space over $F$. A list of vectors $u_1, \ldots, u_n \in V$ is called \textbf{linearly dependent} if there are scalars $s_1, \ldots, s_n \in F$, not all of which are 0, such that

$$\sum_{i=1}^{n} s_i u_i = 0.$$  

A list that is not linearly dependent is called \textbf{linearly independent}. Similarly, a subset $U \subset V$ is called linearly dependent if there is a finite list $u_1, \ldots, u_n \in U$ of distinct vectors that is linearly dependent. Otherwise, it is called linearly independent.

A few important consequences follow immediately from this definition. Any subset of a linearly independent set is also linearly independent. Any set which contains the $0$ vector is linearly dependent. A set $U \subset V$ is linearly independent if and only if each finite subset of $U$ is linearly independent.

Definition 3.3.11. Let $V$ be a vector space over $F$. Let $B = \{ v_\alpha | \alpha \in A \}$ be a subset of linearly independent vectors from $V$ such that every $v \in V$ can be written
as a finite linear combination of vectors from \( B \). Then, the set \( B \) is a **Hamel basis** for \( V \). The space \( V \) is **finite-dimensional** if it has a finite basis.

Using this definition, we note that a basis decomposition \( v = \sum_{i=1}^{n} s_i v_\alpha_i \) must be unique because the difference between any two distinct decompositions produces a finite linear dependency in the basis and, hence, a contradiction.

**Theorem 3.3.12.** Every vector space has a Hamel basis.

**Proof.** Let \( X \) be the set of linearly independent subsets of \( V \). Furthermore, for \( x, y \in X \) consider the strict partial order defined by proper inclusion. By the maximum principle, if \( x \) is an element of \( X \), then there exists a maximal simply ordered subset \( Z \) of \( X \) containing \( x \). This element is a Hamel basis for \( V \).

**Example 3.3.13.** Let \( F \) be a field and let \( U \subset F^n \) be the subset consisting of the vectors \( e_1, \ldots, e_n \) defined by

\[
\begin{align*}
e_1 &= (1, 0, \ldots, 0) \\
e_2 &= (0, 1, \ldots, 0) \\
\vdots &= \vdots \\
e_n &= (0, 0, \ldots, 1).
\end{align*}
\]

For any \( v = (v_1, \ldots, v_n) \in F^n \), we have

\[
v = \sum_{i=1}^{n} v_i e_i. \tag{3.3}
\]

Thus, the collection \( U = \{e_1, \ldots, e_n\} \) spans \( F^n \). Since \( v = 0 \) in \( \text{(3.3)} \) if and only if \( v_1 = \cdots = v_n = 0 \), \( U \) is linearly independent. Accordingly, the set \( U \) is a basis for \( F^n \times 1 \). This basis is termed the **standard basis** of \( F^n \).

**Lemma 3.3.14.** Let \( A \in F^{n \times n} \) be an invertible matrix. Then, the columns of \( A \) form a basis for \( F^n \). Similarly, the rows of \( A \) will also form a basis for \( F^n \).

**Proof.** If \( v = (v_1, \ldots, v_n)^T \) is a column vector, then

\[
Av = \sum_{i=1}^{n} v_i a_i,
\]

where the columns of \( A \) are denoted by \( a_1, \ldots, a_n \). Since \( A \) is invertible,

\[
Av = 0 \implies Iv = A^{-1}0 \implies v = 0.
\]
Thus, \( \{a_1, \ldots, a_n\} \) is a linearly independent set. Next, for any column vector \( w \in F^n \), let \( v = A^{-1}w \). It follows that \( w = Aw \) and, thus, \( \{a_1, \ldots, a_n\} \) is a basis for \( F^n \).

If \( A \) is invertible, then \( (A^T)^{-1} \) exists. Thus, the same holds for the rows. \( \square \)

**Theorem 3.3.15.** Let \( V \) be a finite-dimensional vector space that is spanned by a finite set of vectors \( W = \{w_1, \ldots, w_n\} \). If \( U = \{u_1, \ldots, u_m\} \subset V \) is a linearly independent set of vectors, then \( m \leq n \).

**Proof.** Suppose that \( U = \{u_1, \ldots, u_m\} \subset V \) is linearly independent and \( m > n \).

Since \( W \) spans \( V \), there exists scalars \( a_{ij} \) such that

\[
    u_j = \sum_{i=1}^{n} a_{ij}w_i.
\]

For any \( m \) scalars \( s_1, \ldots, s_m \) we have

\[
    \sum_{j=1}^{m} s_j u_j = \sum_{j=1}^{m} s_j \sum_{i=1}^{n} a_{ij}w_i = \sum_{j=1}^{m} \sum_{i=1}^{n} (a_{ij}s_j)w_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} a_{ij}s_j \right) w_i.
\]

Collecting the \( a_{ij} \) coefficients into an \( n \) by \( m \) matrix \( A \) shows that

\[
    \begin{bmatrix}
    t_1 \\
    \vdots \\
    t_n
    \end{bmatrix}
    =
    A
    \begin{bmatrix}
    s_1 \\
    \vdots \\
    s_m
    \end{bmatrix}
    .
\]

Since \( A \in F^{n \times m} \) with \( n < m \), Lemma 3.2.12 implies there are scalars \( s_1, \ldots, s_n \), not all 0, such that \( t_1 = t_2 = \cdots = t_m = 0 \). For these scalars, \( \sum_{j=1}^{m} s_j u_j = 0 \).

Thus, the set \( U \) is linearly dependent. and the contradiction implies \( m \leq n \). \( \square \)

Now, suppose that \( V \) is a finite-dimensional vector space with bases \( U = \{u_1, \ldots, u_n\} \) and \( W = \{w_1, \ldots, w_m\} \) where \( m \neq n \). Then, without loss of generality, we can assume \( m > n \) and apply Theorem 3.3.15 to see that \( W \) must be linearly dependent. Since a basis must be linearly independent, this gives a contradiction and implies that \( m = n \). Hence, if \( V \) is a finite-dimensional vector space, then any two bases of \( V \) have the same number of elements. Therefore, the dimension of a finite-dimensional vector space is uniquely defined. Thus, our intuition about dimension from \( \mathbb{R}^n \) does not break down for other vector spaces and fields.
Definition 3.3.16. The dimension of a finite-dimensional vector space is the number of elements in any basis for $V$. We denote the dimension of a finite-dimensional vector space $V$ by $\dim(V)$.

The zero subspace of a vector space $V$ is the subspace spanned by the vector $0$. Since the set $\{0\}$ is linearly dependent and not a basis, we assign a dimension $0$ to the zero subspace. Alternatively, it can be argue that the empty set $\emptyset$ spans $\{0\}$ because the intersection of all the subspaces containing the empty set is $\{0\}$. Though this is only a minor point.

Theorem 3.3.17. Let $A$ be an $n \times n$ matrix over $F$ whose columns, denoted by $a_1, \ldots, a_n$, form a linearly independent set of vectors in $F^n$. Then $A$ is invertible.

Proof. Let $W$ be the subspace of $V = F^n$ spanned by $a_1, \ldots, a_n$. Since $a_1, \ldots, a_n$ are linearly independent, $\dim(W) = n = \dim(V)$. Now, suppose $W \neq V$. Since $W \subseteq V$, that implies there is a vector $v \in V$ such that $v \notin W$. It would follow that $\dim(V) > \dim(W)$ but this contradicts $\dim(V) = \dim(W)$. Thus, $W = V$.

Since $W = V$, one can write the standard basis vectors $e_1, \ldots, e_n \in F^n$ in terms of the columns of $A$. In particular, there exist scalars $b_{ij} \in F$ such that

$$e_j = \sum_{i=1}^{n} b_{ij} a_i, \quad 1 \leq j \leq n.$$  

Then, for the matrix $B$ with entries $b_{ij}$, we have $AB = I$.

Next, suppose that the columns of $B$ are linearly dependent. Then, there is a non-zero $v \in F^n$ such that $Bv = 0$. But, that gives the contradiction that $A(Bv) = 0$ and $(AB)v = Iv = v$. Thus, the columns of $B$ are linearly independent.

Using the first argument again, one finds that there is a matrix $C$ such that $BC = I$. This also implies that $A = AI = A(BC) = (AB)C = IC = C$. Thus, $A^{-1}$ exists and equals $B$.\hfill $\square$

3.3.3 Coordinates System

Let $\{v_1, \ldots, v_n\}$ be a basis for the $n$-dimensional vector space $V$ and recall that every vector $w \in V$ can be expressed uniquely as

$$w = \sum_{i=1}^{n} s_i v_i.$$
3.3. VECTOR SPACES

While standard vector and matrix notation requires that the basis elements be ordered, a set is an unordered collection of objects. Ordering this set (e.g., \( v_1, \ldots, v_n \)) allows the first element in the coordinate vector to be associated with the first vector in our basis and so on.

**Definition 3.3.18.** If \( V \) is a finite-dimensional vector space, an **ordered basis** for \( V \) is a finite list of vectors that is linearly independent and spans \( V \).

In particular, if the sequence \( v_1, \ldots, v_n \) is an ordered basis for \( V \), then the set \( \{ v_1, \ldots, v_n \} \) is a basis for \( V \). The ordered basis \( B \), denoted by \( (v_1, \ldots, v_n) \), defines the set and a specific ordering of the vectors. Based on this ordered basis, a vector \( v \in V \) can be unambiguously represented as an \( n \)-tuple \( (s_1, \ldots, s_n) \in F^n \) such that

\[
v = \sum_{i=1}^{n} s_i v_i.
\]

**Definition 3.3.19.** For a finite-dimensional vector space \( V \) with ordered basis \( B = (v_1, \ldots, v_n) \), the **coordinate vector** of \( v \in V \) is denoted by \( [v]_B \) and equals the unique vector \( s = F^n \) such that

\[
v = \sum_{i=1}^{n} s_i v_i.
\]

The dependence of the coordinate vector \( [v]_B \) on the basis is explicitly specified using the subscript. This can be particularly useful when multiple coordinate systems are involved.

**Example 3.3.20.** The canonical example of an ordered basis is the standard basis for \( F^n \) introduced in Section 3.3.2. Note that the standard basis contains a natural ordering: \( e_1, \ldots, e_n \). Vectors in \( F^n \) can therefore be unambiguously expressed as \( n \)-tuples.

**Problem 3.3.21.** Suppose that \( A = v_1, \ldots, v_n \) is an ordered basis for \( V \). Let \( P \) be an \( n \times n \) invertible matrix. Show that there exists an ordered basis \( B = w_1, \ldots, w_n \) for \( V \) such that

\[
[u]_A = P [u]_B
\]

\[
[u]_B = P^{-1} [u]_A
\]

for every \( u \in V \).
Consider the ordered basis $A = v_1, \ldots, v_n$ and let $Q = P^{-1}$. For all $u \in V$, we have $u = \sum_{i=1}^{n} s_i v_i$, where

$$[u]_A = \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}.$$

If we define

$$w_i = \sum_{k=1}^{n} p_{ki} v_k$$

and

$$t_i = \sum_{j=1}^{n} q_{ij} s_j,$$

then we find that

$$\sum_{i=1}^{n} t_i w_i = \sum_{i=1}^{n} \sum_{j=1}^{n} q_{ij} s_j w_i = \sum_{i=1}^{n} \sum_{j=1}^{n} q_{ij} s_j \sum_{k=1}^{n} p_{ki} v_k$$

$$= \sum_{j=1}^{n} s_j \sum_{k=1}^{n} v_k \sum_{i=1}^{n} p_{ki} q_{ij} = \sum_{j=1}^{n} s_j \sum_{k=1}^{n} v_k \delta_{jk}$$

$$= \sum_{j=1}^{n} s_j v_j = u.$$

This shows that $B = w_1, \ldots, w_n$ is an ordered basis for $V$ and

$$[u]_B = \begin{bmatrix} t_1 \\ \vdots \\ t_n \end{bmatrix}.$$

The definition of $t_i$ also shows that $[u]_B = P^{-1} [u]_A$ and therefore $[u]_A = P [u]_B$.

### 3.4 Linear Transformations

#### 3.4.1 Definitions

**Definition 3.4.1.** Let $V$ and $W$ be vector spaces over a field $F$. A **linear transform** from $V$ to $W$ is a function $T$ from $V$ into $W$ such that

$$T(s v_1 + v_2) = s T v_1 + T v_2$$

for all $v_1$ and $v_2$ in $V$ and all scalars $s$ in $F$. 
Definition 3.4.2. Let $L(V, W)$ denote the set of all linear transforms from $V$ into $W$, where $V$ and $W$ are vector spaces over a field $F$.

Example 3.4.3. Let $A$ be a fixed $m \times n$ matrix over $F$. The function $T$ defined by $T(v) = Av$ is a linear transformation from $F^{n \times 1}$ into $F^{m \times 1}$.

Example 3.4.4. Let $P \in F^{m \times m}$ and $Q \in F^{n \times n}$ be fixed matrices. Define the function $T$ from $F^{m \times n}$ into itself by $T(A) = PAQ$. Then $T$ is a linear transformation from $F^{m \times n}$ into $F^{m \times n}$. In particular,

$$T(sA + B) = P(sA + B)Q = sPAQ + PBQ = sT(A) + T(B).$$

Example 3.4.5. Let $V$ be the space of continuous functions from $[0, 1]$ to $\mathbb{R}$, and define $T$ by

$$(Tf)(x) = \int_0^x f(t)dt.$$ 

Then $T$ is a linear transformation from $V$ into $V$. The function $Tf$ is continuous and differentiable.

It is important to note that if $T$ is a linear transformation from $V$ to $W$, then $T(0) = 0$. This is essential since

$$T(0) = T(0 + 0) = T(0) + T(0).$$

Definition 3.4.6. A linear transformation $T : V \to W$ is singular if there is a non-zero vector $v \in V$ such that $Tv = 0$. Otherwise, it is called non-singular.

### 3.4.2 Properties

The following theorem illuminates a very important structural element of linear transformations: they are uniquely defined by where they map a set of basis vectors for their domain.

Theorem 3.4.7. Let $V, W$ be vector spaces over $F$ and $\mathcal{B} = \{v_\alpha | \alpha \in A\}$ be a Hamel basis for $V$. For each mapping $G : \mathcal{B} \to W$, there is a unique linear transformation $T : V \to W$ such that $T_{v_\alpha} = G(v_\alpha)$ for all $\alpha \in A$. 
Proof. Since \( B \) is a Hamel basis for \( V \), every vector \( w \in V \) has a unique expansion

\[
    w = \sum_{\alpha \in A} s_{\alpha}(w) \cdot v_{\alpha},
\]

where \( s_{\alpha}(w) \) is the unique \( \alpha \) coefficient for \( w \) and \( s_{\alpha}(w) \neq 0 \) only for a finite subset of \( A \). Using the unique expansion and vector space properties, one can show that

\[
    s_{\alpha}(tw_1 + w_2) = ts_{\alpha}(w_1) + s_{\alpha}(w_2).
\]

Next, we define the mapping \( T: V \to W \) in terms of \( s_{\alpha}(\cdot) \) and \( G(\cdot) \) with

\[
    Tw = \sum_{\alpha \in A} s_{\alpha}(w) \cdot G(v_{\alpha}).
\]

Using the linearity of \( s_{\alpha}(\cdot) \), it is easy to verify that \( T \) is a linear transform.

To show that \( T \) is unique, we let \( U: V \to W \) be any other linear mapping satisfying \( Uv_{\alpha} = G(v_{\alpha}) \) for all \( \alpha \in A \). In this case, the linearity of \( U \) guarantees that

\[
    Uw = U \left( \sum_{\alpha \in A} s_{\alpha}(w) \cdot v_{\alpha} \right) = \sum_{\alpha \in A} s_{\alpha}(w) \cdot U(v_{\alpha}) = \sum_{\alpha \in A} s_{\alpha}(w) \cdot G(v_{\alpha}).
\]

From this, we see that \( Uw = Tw \) for all \( w \in V \) and therefore that \( U = T \). \( \square \)

**Definition 3.4.8.** Let \( V \) and \( W \) be vector spaces with ordered bases \( A \) and \( B \). Then, the coordinate matrix for the linear transform \( T: V \to W \) with respect to \( A \) and \( B \) is denoted \([T]_{A,B}\) and, for all \( v \in V \), satisfies

\[
    [Tv]_B = [T]_{A,B} [v]_A.
\]

If \( V = W \) and \( A = B \), then the coordinate matrix \([T]_{A,A}\) is denoted by \([T]_A\).

**Definition 3.4.9.** If \( T \) is a linear transformation from \( V \) into \( W \), the range of \( T \) is the set of all vectors \( w \in W \) such that \( w = Tv \) for some \( v \in V \). We denote the range of \( T \) by

\[
    \mathcal{R}(T) \triangleq \{ w \in W | \exists v \in V, Tv = w \} = \{ Tv | v \in V \}.
\]

The set \( \mathcal{R}(T) \) is a subspace of \( W \). Let \( w_1, w_2 \in \mathcal{R}(T) \) and let \( s \) be a scalar. By definition, there exist vectors \( v_1 \) and \( v_2 \) in \( V \) such that \( Tv_1 = w_1 \) and \( Tv_2 = w_2 \). Since \( T \) is a linear transformation, we have

\[
    T(sv_1 + v_2) = sTv_1 + Tv_2 = sw_1 + w_2,
\]

which shows that \( sw_1 + w_2 \) is also in \( \mathcal{R}(T) \).
Definition 3.4.10. If $T$ is a linear transformation from $V$ into $W$, the nullspace of $T$ is the set of all vectors $v \in V$ such that $Tv = 0$. We denote the nullspace of $T$ by

$$\mathcal{N}(T) \triangleq \{v \in V | Tv = 0\}.$$ 

It can easily be verified that $\mathcal{N}(T)$ is a subspace of $V$.

Furthermore, if $Tv_1 = Tv_2 = 0$ then

$$T(sv_1 + v_2) = sTv_1 + (v_2) = s0 + 0 = 0,$$

so that $sv_1 + v_2 \in \mathcal{N}(T)$.

Definition 3.4.11. Let $V$ and $W$ be vector spaces over a field $F$, and let $T$ be a linear transformation from $V$ into $W$. If $V$ is finite-dimensional, the rank of $T$ is the dimension of the range of $T$ and the nullity of $T$ is the dimension of the nullspace of $T$.

Theorem 3.4.12. Let $V$ and $W$ be vector spaces over the field $F$ and let $T$ be a linear transformation from $V$ into $W$. If $V$ is finite-dimensional, then

$$\text{rank}(T) + \text{nullity}(T) = \dim(V)$$

Proof. Let $v_1, \ldots, v_k$ be a basis for $\mathcal{N}(T)$, the nullspace of $T$. There are vectors $v_{k+1}, \ldots, v_n \in V$ such that $v_1, \ldots, v_n$ is a basis for $V$. We want to show that $Tv_{k+1}, \ldots, Tv_n$ is a basis for the range of $T$. The vectors $Tv_1, \ldots, Tv_n$ certainly span $\mathcal{R}(T)$ and, since $Tv_j = 0$ for $j = 1, \ldots, k$, it follows that $Tv_{k+1}, \ldots, v_n$ span $\mathcal{R}(T)$. Suppose that there exist scalars $s_{k+1}, \ldots, s_n$ such that

$$\sum_{j=k+1}^{n} s_jTv_j = 0.$$ 

This implies that

$$T \left( \sum_{j=k+1}^{n} s_jv_j \right) = 0,$$

and accordingly the vector $v = \sum_{j=k+1}^{n} s_jv_j$ is in the nullspace of $T$. Since $v_1, \ldots, v_k$ form a basis for $\mathcal{N}(T)$, there must be a linear combination such that

$$v = \sum_{j=1}^{k} t_jv_j.$$
But then,
\[ \sum_{j=1}^{k} t_j v_j - \sum_{j=k+1}^{n} s_j v_j = 0. \]
Since the vectors \( v_1, \ldots, v_n \) are linearly independent, this implies that
\[ t_1 = \cdots = t_k = s_{k+1} = \ldots = s_n = 0. \]
That is, the set \( T v_{k+1}, \ldots, T v_n \) is linearly independent in \( W \) and therefore forms a basis for \( \mathcal{R}(T) \). In turn, this implies that \( n = \text{rank}(T) + \text{nullity}(T) \). \( \square \)

**Theorem 3.4.13.** If \( A \) is an \( m \times n \) matrix with entries in the field \( F \), then
\[
\text{row rank}(A) \triangleq \dim(\mathcal{R}(A^T)) = \dim(\mathcal{R}(A)) \triangleq \text{rank}(A).
\]

**Proof.** Let \( R = P A \) be the reduced row echelon form of \( A \), where \( P \) is invertible. Let \( r \) be the number of non-zero rows in \( R \) and observe that \( \text{row rank}(A) = r \) because the rows of \( R \) form a basis for the row space of \( A \). Next, we write \( A = P^{-1} R \) and observe that each column of \( R \) has non-zero entries only in the first \( r \) rows. Thus, each column of \( A \) is a linear combination of the first \( r \) columns in \( P^{-1} \). Thus, the column space of \( A \) is spanned by \( r \) vectors and \( \text{rank}(A) \leq \text{row rank}(A) \).

The proof is completed by applying the above bound to both \( A \) and \( A^T \) to get
\[ \text{rank}(A) \leq \text{row rank}(A) = \text{rank}(A^T) \leq \text{row rank}(A^T) = \text{rank}(A). \] \( \square \)

When \( F = \mathbb{C} \), the space \( \mathcal{R}(A^H) \) has many nice properties and can also be called the row space of \( A \). Regardless, it holds that \( \text{rank}(A) = \text{rank}(A^T) = \text{rank}(A^H) \).

### 3.5 Norms

Let \( V \) be a vector space over the real numbers or the complex numbers.

**Definition 3.5.1.** A **norm** on vector space \( V \) is a real-valued function \( \| \cdot \| : V \to \mathbb{R} \) that satisfies the following properties.

1. \( \| v \| \geq 0 \quad \forall v \in V \); equality holds if and only if \( v = 0 \)
2. \( \| s v \| = |s| \| v \| \quad \forall v \in V, s \in F \)
3. \( \| v + w \| \leq \| v \| + \| w \| \quad \forall v, w \in V. \)
The concept of a norm is closely related to that of a metric. For instance, a metric can be defined from any norm. Let $\|v\|$ be a norm on vector space $V$, then

$$d(v, w) = \|v - w\|$$

is the metric induced by the norm.

Normed vector spaces are very useful because they have all the properties of a vector space and all the benefits of a topology generated by the norm. Therefore, one can discuss limits and convergence in a meaningful way.

**Example 3.5.2.** Consider vectors in $\mathbb{R}^n$ with the euclidean metric

$$d(v, w) = \sqrt{(v_1 - w_1)^2 + \cdots + (v_n - w_n)^2}.$$ 

Recall that the standard bounded metric introduced in Problem 2.1.5 is given by

$$\bar{d}(v, w) = \min\{d(v, w), 1\}.$$ 

Define the function $f : \mathbb{R}^n \to \mathbb{R}$ by $f(v) = \bar{d}(v, 0)$. Is the function $f$ a norm?

By the properties of a metric, we have

1. $\bar{d}(v, 0) \geq 0 \quad \forall v \in V$; equality holds if and only if $v = 0$
2. $\bar{d}(v, 0) + \bar{d}(w, 0) = \bar{d}(v + w, 0) \geq \bar{d}(v, w) \quad \forall v, w \in V.$

However, $\bar{d}(sv, 0)$ is not necessarily equal to $s\bar{d}(v, 0)$. For instance, $\bar{d}(2e_1, 0) = 1 < 2\bar{d}(e_1, 0)$. Thus, the function $f : \mathbb{R}^n \to \mathbb{R}$ defined by

$$f(v) = \bar{d}(v, 0).$$

is not a norm.

**Example 3.5.5.** The following functions are examples of norms for $\mathbb{R}^n$ and $\mathbb{C}^n$:

1. the $l^1$ norm: $\|v\|_1 = \sum_{i=1}^n |v_i|$
2. the $l^p$ norm: $\|v\|_p = (\sum_{i=1}^n |v_i|^p)^{\frac{1}{p}}$, $p \in (1, \infty)$
3. the $l^\infty$ norm: $\|v\|_\infty = \max_{1,\ldots,n} \{|v_i|\}$.

**Example 3.5.6.** Similarly, norms can be defined for the vector space of functions from $[a, b]$ to $\mathbb{R}$ (or $\mathbb{C}$) with
What are $L^p$ spaces? What is the Lebesgue Integral?

Many important spaces include functions that are not Riemann integrable. The Lebesgue integral is defined using measure theory and is often used in advanced probability courses. Since there are many non-zero Lebesgue-integrable functions whose integral is zero, this definition has a subtlety. The Lebesgue integral of a function is zero if and only if the function is zero almost everywhere (abbreviated a.e.). Therefore, two functions are equal almost everywhere if the norm of their difference is zero. Strictly speaking, a vector space of “functions” with the $L^p$ norm actually contains elements that are equivalence classes of functions defined by equality almost everywhere.

Consider the set of all functions $f: X \to \mathbb{R}$ from $X$ to the real numbers. The normed vector space $L^p(X)$ (with $1 \leq p < \infty$) is the subset where the Lebesgue integral
\[
\|f\|_{L^p} \triangleq \left( \int_X |f(x)|^p \, dx \right)^{1/p}
\]
exists and is finite. Of course, this definition begs the question, “What is the Lebesgue integral?” The following definition is sufficient for these notes:

**Definition 3.5.3.** The Lebesgue integral is a generalization of the Riemann integral that applies to wider class of functions. The values of these two integrals coincide on the set of Riemann integrable functions. Loosely speaking, one can construct any non-negative function $f \in L^p(X)$ by considering sequences $f_1, f_2, \ldots$ of “simple” functions formed by rounding values of $f$ down to values in a finite set $S_i \subset [0, \infty)$ where $\{0\} \subset S_1 \subset S_2 \subset \cdots \subset [0, \infty)$. By construction, the sequence of functions is non-decreasing (i.e., $f_{n+1}(x) \geq f_n(x)$ for all $x \in X$) and, therefore, it converges pointwise to a limit function $f(x)$. Moreover, the Lebesgue integral of each simple function is easy to define. Thus, this sequence of simple functions gives rise to a non-decreasing sequence of Lebesgue integrals and one defines the Lebesgue integral of $f(x)$ to be the limit of this sequence. In fact, the non-negative functions in $L^p(X)$ are in one-to-one correspondence with the limits of non-decreasing sequences of simple functions that satisfy $\|f_n\|_{L^p} \to M < \infty$, up to a.e. equivalence.

**Definition 3.5.4.** The Lebesgue measure of a set is equal to the Lebesgue integral of its indicator function when both quantities exist. In particular, a set is measurable if and only if the Lebesgue integral of its indicator function exists.
3.5. NORMS

1. the $L^1$ norm: $\|f(t)\|_1 = \int_a^b |f(t)| \, dt$

2. the $L^p$ norm: $\|f(t)\|_p = \left( \int_a^b |f(t)|^p \, dt \right)^{\frac{1}{p}}, \quad p \in (1, \infty)$

3. the $L^\infty$ norm: $\|f(t)\|_\infty = \text{ess sup}_{[a,b]} \{|f(t)|\}$.

In this example, the integral notation refers to the Lebesgue integral (rather than the Riemann integral).

Example 3.5.7. Consider any set $W$ of real-valued random variables, defined on a common probability space, such that $\|X\|_p \triangleq \mathbb{E}[|X|^p]^{1/p} < \infty$ for all $X \in W$ and some fixed $p \in [1, \infty)$. Then, $V = \text{span}(W)$ is a normed vector space over $\mathbb{R}$ and $X, Y \in V$ are considered to be equal if $\|X - Y\|_p = \mathbb{E}[|X - Y|^p] = 0$ (or equivalently $\Pr(X \neq Y) = 0$). In addition, the closure of $V$ is a Banach space.

Remark 3.5.8. We have not shown that the $\ell^p$ and $L^p$ norm definitions above satisfy all the required properties. In particular, to prove the triangle inequality, one requires the Minkowski inequality which is deferred until Theorem 3.5.20.

Definition 3.5.9. A vector $v \in V$ is said to be normalized if $\|v\| = 1$. Any vector can be normalized, except the zero vector:

$$u = \frac{v}{\|v\|}$$

has norm $\|u\| = 1$. A normalized vector is also referred to as a unit vector.

Definition 3.5.10. A complete normed vector space is called a Banach space.

Banach spaces are the standard setting for many problems because completeness is a powerful tool for solving problems.

Example 3.5.11. The vector spaces $\mathbb{R}^n$ (or $\mathbb{C}^n$) with any well-defined norm are Banach spaces.

Example 3.5.12. The vector space of all continuous functions from $[a, b]$ to $\mathbb{R}$ is a Banach space under the supremum norm

$$\|f(t)\| = \sup_{t \in [a,b]} f(t).$$
Definition 3.5.13. A Banach space $V$ has a Schauder basis, $v_1, v_2, \ldots$, if every $v \in V$ can be written uniquely as
\[ v = \sum_{i=1}^{\infty} s_i v_i. \]

Lemma 3.5.14. If $\sum_{i=1}^{\infty} \|v_i\| = a < \infty$, then $u_n = \sum_{i=1}^{n} v_i$ satisfies $u_n \to u$.

Proof. This is left as an exercise for the reader because it is a straightforward generalization of the proof of Lemma 2.1.38.

Example 3.5.15. Let $V = \mathbb{R}^\omega$ be the vector space of semi-infinite real sequences. The standard Schauder basis is the countably infinite extension $\{e_1, e_2, \ldots\}$ of the standard basis.

Definition 3.5.16. A closed subspace of a Banach space is a subspace that is a closed set in the topology generated by the norm.

Theorem 3.5.17. All finite dimensional subspaces of a Banach space are closed.

Proof. This proof requires material from later in the notes, but is given here for completeness. Let $w_1, w_2, \ldots, w_n$ be a basis for a finite dimensional subspace $W$ of a Banach space $V$ over $F$. Let $U = F^n$ be the standard Banach space, which is closed by definition, and consider the mapping $f : U \to W$ defined by
\[ f(s) = \sum_{i=1}^{n} s_i w_i. \]

It is easy to verify that this linear mapping is non-singular and onto. Therefore, it has a linear inverse mapping $g = f^{-1}$ that must be continuous (i.e., bounded) because $U, W$ are finite dimensional. Since $g$ is continuous, we find that $W = g^{-1}(U) = f(U)$ is closed because $U$ is closed.

Example 3.5.18. Let $V = L^p([a, b])$, for $1 \leq p < \infty$, be the set of real Lebesgue-integrable functions on $[a, b]$. We say that $f \in V$ is continuous if the equivalence class generated by equality almost everywhere contains a continuous function. It is easy to verify that the subset $W \subset V$ of continuous functions is a subspace. It is not closed, however, because sequences in $W$ may converge to discontinuous functions. In fact, the set of continuous functions is dense in $L^p([a, b])$ for $p \in [1, \infty)$. 

Example 3.5.19. Let $W = \{w_1, w_2, \ldots \}$ be a linearly independent sequence of normalized vectors in a Banach space. The span of $W$ only includes finite linear combinations. However, a sequence of finite linear combinations, like

$$u_n = \sum_{i=1}^{n} \frac{1}{i^2} w_i,$$

converges to the infinite linear combination $u = \lim_{n \to \infty} u_n$ if the limit exists. Applying Lemma 3.5.14 to $v_i = \frac{1}{i^2} w_i$ shows that the limit exists if $\sum_{i=1}^{\infty} i^{-2} < \infty$ and that this can be shown by induction. Thus, the span of any infinite set of linearly independent vectors is not closed.

Theorem 3.5.20 (Hölder and Minkowski Inequalities). Consider the following weighted versions of the $\ell^p$ and $L^p$ norms defined by

$$\|u\|_{\ell^p(w)} = \left( \sum_{i=1}^{n} w_i |v_i|^p \right)^{\frac{1}{p}},$$

$$\|f\|_{L^p(X,w)} = \left( \int_X w(x) |f(x)|^p \, dx \right)^{\frac{1}{p}},$$

where the vector $w$ and function $w(x)$ define real positive weights and $X$ is chosen so that the Lebesgue integral is well-defined. For $p \in [1, \infty)$, the Minkowski inequality states that

$$\|u + v\|_{\ell^p(w)} \leq \|u\|_{\ell^p(w)} + \|v\|_{\ell^p(w)}$$

$$\|f + g\|_{L^p(X,w)} \leq \|f\|_{L^p(X,w)} + \|g\|_{L^p(X,w)}.$$

Now, choose $p, q \in [1, \infty]$ such that $\frac{1}{p} + \frac{1}{q} = 1$, where $1/\infty = 0$. For the $\ell^p$ case, assume $u, v \in \ell^p(w)$ (i.e., $\|u\|_{\ell^p(w)} < \infty$ and $\|v\|_{\ell^p(w)} < \infty$) and define the product vector $t = (u_1 v_1, \ldots, u_n v_n)$. For the $L^p$ case, assume that $f, g \in L^p(X, w)$ (i.e., $\|f\|_{L^p(X,w)} < \infty$ and $\|g\|_{L^p(X,w)} < \infty$) and define the product function $h(x) = f(x)g(x)$. Then, the Hölder inequality states that

$$\|t\|_{\ell^1(w)} \leq \|u\|_{\ell^p(w)} \|v\|_{\ell^{q}(w)}$$

$$\|h\|_{L^1(X,w)} \leq \|f\|_{L^p(X,w)} \|g\|_{L^{q}(X,w)}.$$


3.6 Inner Products

An inner product space is a vector space with an inner product, defined below. Such spaces have an inherent structure that admits the rigorous development of geometrical notions such as the length of a vector and the angle between two vectors. They offer a means to define the projection of a vector onto another vector, and the orthogonality of a pair of vectors. In some sense, inner product spaces generalize Euclidean spaces with their dot products. Importantly, an inner product naturally induces a norm and, hence, a metric. Consequently, they are necessarily equipped with a metric topology, open sets, and a definition of convergence.

In practice, one often encounters inner product space that are finite dimensional. Therein, vectors can be expressed as linear combinations of elements within a Hamel basis. Yet, an inner product space can also be of infinite dimension. Hilbert spaces are complete inner product spaces, which makes them suitable to discuss Cauchy sequences of vectors and their limits. Furthermore, when an inner product space is separable (in the induced metric topology), then it will have a countable Schauder basis. Intuitively, a separable Hilbert space with its Schauder basis can be handled mathematically in a way similar to a finite-dimensional inner product space. For this reason, our treatment of infinite-dimensional inner product spaces is largely restricted to separable Hilbert spaces. More general spaces require a higher level of mathematical sophistication, beyond this treatment.

Definition 3.6.1. Let $F$ be the field of real numbers or the field of complex numbers, and assume $V$ is a vector space over $F$. An inner product on $V$ is a function which assigns to each ordered pair of vectors $v, w \in V$ a scalar $\langle v, w \rangle \in F$ in such a way that for all $u, v, w \in V$ and any scalar $s \in F$

1. $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
2. $\langle sv, w \rangle = s\langle v, w \rangle$
3. $\langle v, w \rangle = \overline{\langle w, v \rangle}$, where the overbar denotes complex conjugation;
4. $\langle v, v \rangle \geq 0$ with equality iff $v = 0$.

We emphasize that the conditions of Definition 3.6.1 imply

$$\langle u, sv + w \rangle = s\overline{\langle u, v \rangle} + \langle u, w \rangle.$$
Thus, an inner product is linear in the first argument and conjugate linear in the second argument.

**Definition 3.6.2.** A real or complex vector space equipped with an inner product is called an **inner-product space**.

**Example 3.6.3.** Consider the inner product on $F^n$ defined by

$$\langle v, w \rangle = \langle (v_1, \ldots, v_n), (w_1, \ldots, w_n) \rangle = \sum_{j=1}^{n} v_j w_j.$$

This inner product is called the **standard inner product**. When $F = \mathbb{R}$, the standard inner product can also be written as

$$\langle v, w \rangle = \sum_{j=1}^{n} v_j w_j.$$

In this context it is often called the dot product, denoted by $v \cdot w$. In either case, it can also be written in terms of the Hermitian transpose as $\langle v, w \rangle = w^H v$.

**Problem 3.6.4.** For $v = (v_1, v_2)$ and $w = (w_1, w_2)$ in $\mathbb{R}^2$, show that

$$\langle v, w \rangle = v_1 w_1 - v_2 w_1 - v_1 w_2 + 4v_2 w_2$$

is an inner product.

**S 3.6.4** For all $u, v, w \in V$ and all scalars $s$

$$\langle u + v, w \rangle = (u_1 + v_1)w_1 - (u_2 + v_2)w_1 - (u_1 + v_1)w_2 + 4(u_2 + v_2)w_2$$

$$= u_1 w_1 - u_2 w_1 - u_1 w_2 + 4u_2 w_2 + v_1 w_1 - v_2 w_1 - v_1 w_2 + 4v_2 w_2$$

$$= \langle u, w \rangle + \langle v, w \rangle.$$

Also, we have

$$\langle sv, w \rangle = sv_1 w_1 - sv_2 w_1 - sv_1 w_2 + 4sv_2 w_2 = s \langle v, w \rangle.$$

Since $V = \mathbb{R}^2$, we have $\langle v, w \rangle = \langle w, v \rangle$. Furthermore,

$$\langle v, v \rangle = v_1^2 - 2v_1 v_2 + 4v_2^2 = (v_1 - v_2)^2 + 3v_2^2 \geq 0 \text{ with equality iff } v_2 = 0.$$

That is, $\langle v, v \rangle$ is an inner product.
Example 3.6.5. Let \( V \) be the vector space of all continuous complex-valued functions on the unit interval \([0, 1]\). Then,

\[
\langle f, g \rangle = \int_0^1 f(t)\overline{g(t)} \, dt
\]

is an inner product.

Example 3.6.6. Let \( V \) and \( W \) be two vector spaces over \( F \) and suppose that \( \langle \cdot, \cdot \rangle_W \) is an inner product on \( W \). If \( T \) is a non-singular linear transformation from \( V \) into \( W \), then the equation

\[
\langle v_1, v_2 \rangle_V = \langle Tv_1, Tv_2 \rangle_W
\]

defines an inner product on \( V \).

Example 3.6.7. Let \( V = F^{m \times n} \) be the space of \( m \times n \) matrices over \( F \) and define the inner product for matrices \( A, B \in V \) to be

\[
\langle A, B \rangle \triangleq \text{tr} \left( B^H A \right) = \sum_{i=1}^n \sum_{j=1}^m b_{j,i} a_{j,i}.
\]

This also equals \( \text{tr} \left( AB^H \right) \) and both are identical to writing the entries of the matrices as length-\( mn \) vectors and then applying the standard inner product.

Theorem 3.6.8. Let \( V \) be a finite-dimensional space, and suppose that

\[
\mathcal{B} = w_1, \ldots, w_n
\]

is an ordered basis for \( V \). Any inner product on \( V \) is determined by the values

\[
g_{ij} = \langle w_j, w_i \rangle
\]

that it takes on pairs of vectors in \( \mathcal{B} \).

Proof. If \( u = \sum_j s_j w_j \) and \( v = \sum_i t_i w_i \), then

\[
\langle u, v \rangle = \left\langle \sum_j s_j w_j, v \right\rangle = \sum_j s_j \langle w_j, v \rangle
\]

\[
= \sum_j s_j \left\langle w_j, \sum_i t_i w_i \right\rangle = \sum_j \sum_i s_j \overline{t_i} \langle w_j, w_i \rangle
\]

\[
= \sum_j \sum_i \overline{t_i} g_{ij} s_j = [\mathbf{u}]_B^H G [\mathbf{u}]_B
\]

where \([\mathbf{u}]_B\) and \([\mathbf{v}]_B\) are the coordinate matrices of \( u, v \) in the ordered basis \( \mathcal{B} \). The matrix \( G \) is called the weight matrix of the inner product in the ordered basis \( \mathcal{B} \). \( \square \)
Since \( g_{ij} = \langle w_j, w_i \rangle = \langle w_i, w_j \rangle = g_{ji} \), we see that \( G \) is a Hermitian matrix, i.e., \( G = G^H \). Furthermore, \( G \) must satisfy the additional condition

\[
\langle w^H G w \rangle > 0, \quad \forall w \neq 0
\]

(3.5)
so that the induced norm is non-negative and zero only for the zero vector. A Hermitian matrix that satisfies this condition is called positive definite and this also implies that \( G \) is invertible.

Conversely, if \( G \) is an \( n \times n \) Hermitian matrix over \( F \) which satisfies (3.5), then

\[
\langle u, v \rangle_G = [v]^H G [u]
\]
is a well-defined inner product on \( V \).

**Problem 3.6.9.** Let \( V \) be a vector space over \( F \). Show that the sum of two inner products on \( V \) is an inner product on \( V \). Show that a positive multiple of an inner product is also an inner product.

**Example 3.6.10.** Consider any set \( W \) of real-valued random variables, defined on a common probability space, that have finite 2nd moments. It turns out that \( V = \text{span}(W) \) is a vector space over \( \mathbb{R} \). In fact, one can define the inner product

\[
\langle X, Y \rangle = \mathbb{E}[XY],
\]
for any \( X, Y \in V \). Using the induced norm, this inner product provides the topology of mean-square convergence and two random variables \( X, Y \in V \) are considered equal if \( ||X - Y||^2 = \mathbb{E}[|X - Y|^2] = 0 \) (or equivalently \( \Pr(X \neq Y) = 0 \)).

In terms of abstract mathematics, the introduction of an inner product allows one to introduce the key concept of orthogonality.

**Definition 3.6.11.** Let \( v \) and \( w \) be vectors in an inner-product space \( V \). Then \( v \) is orthogonal to \( w \) (denoted \( v \perp w \)) if \( \langle v, w \rangle = 0 \). Since this relation is reflexive and \( w \) is also orthogonal to \( v \), we simply say that \( v \) and \( w \) are orthogonal.

### 3.6.1 Induced Norms

A finite-dimensional real inner-product space is often referred to as a Euclidean space. A complex inner-product space is sometimes called a unitary space.
Figure 3.1: The projection of $w$ onto $v$ is given by $u$ and $w - u$ is orthogonal to $v$.

**Definition 3.6.12.** Let $V$ be an inner-product space with inner product $\langle \cdot, \cdot \rangle$. This inner product can be used to define a norm, called the induced norm, where

$$
\|v\| = \langle v, v \rangle^{\frac{1}{2}}
$$

for every $v \in V$.

**Definition 3.6.13.** Let $w, v$ be vectors in an inner-product space $V$ with inner product $\langle \cdot, \cdot \rangle$. As shown in Figure 3.1, the projection of $w$ onto $v$ is defined to be

$$
u = \frac{\langle w, v \rangle}{\|v\|^2} v.
$$

**Lemma 3.6.14.** Let $u$ be the projection of $w$ onto $v$. Then, $\langle w - u, u \rangle = 0$ and

$$
\|w - u\|^2 = \|w\|^2 - \|u\|^2 = \|w\|^2 - \frac{\|\langle w, v \rangle\|^2}{\|v\|^2}.
$$

**Proof.** First, we observe that

$$
\langle w - u, v \rangle = \langle w, v \rangle - \langle u, v \rangle = \langle w, v \rangle - \frac{\langle w, v \rangle}{\|v\|^2} \|v\|^2 = 0.
$$

Since $u = sv$ for some scalar $s$, we gather that $\langle w - u, u \rangle = \langle w - u, sv \rangle = s\langle w - u, v \rangle = 0$. Using $\langle w - u, u \rangle = 0$, we can write

$$
\|w\|^2 = \|(w - u) + u\|^2 = \langle (w - u) + u, (w - u) + u \rangle
= \|w - u\|^2 + 2\text{Re} \langle w - u, u \rangle + \|u\|^2 = \|w - u\|^2 + \|u\|^2.
$$

The proof is completed by noting that $\|u\|^2 = \frac{\|\langle w, v \rangle\|^2}{\|v\|^2} \langle v, v \rangle = \frac{\|\langle w, v \rangle\|^2}{\|v\|^2}$.
3.6. INNER PRODUCTS

**Theorem 3.6.15.** If $V$ is an inner-product space and $\| \cdot \|$ is its associated induced norm, then for any $v, w \in V$ and any scalar $s$

1. $\|sv\| = |s| \|v\|$
2. $\|v\| > 0$ for $v \neq 0$
3. $|\langle v, w \rangle| \leq \|v\| \|w\|$ with equality iff $v = 0$, $w = 0$, or $v = sw$
4. $\|v + w\| \leq \|v\| + \|w\|$ with equality iff $v = 0$, $w = 0$, or $v = sw$.

**Proof.** The first two properties follow immediately from the definitions involved. The third property, $|\langle v, w \rangle| \leq \|v\| \|w\|$, is called the **Cauchy-Schwarz inequality**. When $v = 0$, then clearly $|\langle v, w \rangle| = \|v\| \|w\| = 0$. Assume $v \neq 0$ and let

$$u = \frac{\langle w, v \rangle}{\|v\|^2} v$$

be the projection $w$ onto $v$. By Lemma 3.6.14, we have

$$0 \leq \|w - u\|^2 = \|w\|^2 - \frac{|\langle w, v \rangle|^2}{\|v\|^2},$$

where equality holds iff $w - u = 0$, or equivalently iff $w = 0$ or $v = sw$. Rearranging (3.6) by isolating the inner product component and cross-multiplying, we find that

$$|\langle v, w \rangle|^2 = |\langle w, v \rangle|^2 \leq \|v\|^2 \|w\|^2,$$

with equality iff $v = 0$, $w = 0$, or $v = sw$. Using this, we get the fourth property

$$\|v + w\|^2 = \|v\|^2 + \langle v, w \rangle + \langle w, v \rangle + \|w\|^2$$

$$\leq \|v\|^2 + 2|\langle v, w \rangle| + \|w\|^2$$

$$\leq \|v\|^2 + 2\|v\| \|w\| + \|w\|^2,$$

where the first inequality holds with equality iff $Re\langle v, w \rangle = |\langle v, w \rangle|$ (i.e., $\langle v, w \rangle$ is real and non-negative) and the second inequality (i.e., Cauchy-Schwarz) holds with equality. Thus, $\|v + w\| \leq \|v\| + \|w\|$ with equality iff $v = 0$, $w = 0$, or $v = sw$ for real $s \geq 0$.

**Theorem 3.6.16.** Consider the vector space $\mathbb{R}^n$ with the standard inner product. Then, the function $f : V \to F$ defined by $f(w) = \langle w, v \rangle$ is continuous.
Proof. Let \( w_1, w_2, \ldots \) be a sequence in \( V \) converging to \( w \). Then,

\[
|\langle w_n, v \rangle - \langle w, v \rangle| = |\langle w_n - w, v \rangle| \leq \|w_n - w\| \|v\|.
\]

Since \( \|w_n - w\| \to 0 \), the convergence of \( \langle w_n, v \rangle \) is established. \( \Box \)

3.7 Sets of Orthogonal Vectors

Definition 3.7.1. Let \( V \) be an inner-product space and \( U, W \) be subspaces. Then, the subspace \( U \) is an orthogonal to the subspace \( W \) (denoted \( U \bot W \)) if \( u \bot w \) for all \( u \in U \) and \( w \in W \).

Definition 3.7.2. A collection \( W \) of vectors in \( V \) is an orthogonal set if all pairs of distinct vectors in \( W \) are orthogonal.

Example 3.7.3. The standard basis of \( \mathbb{R}^n \) is an orthonormal set with respect to the standard inner product.

Example 3.7.4. Let \( V \) be the vector space (over \( \mathbb{C} \)) of continuous complex-valued functions on the interval \( 0 \leq x \leq 1 \) with the inner product

\[
\langle f, g \rangle = \int_0^1 f(x) \overline{g(x)} \, dx.
\]

Let \( f_n(x) = \sqrt{2} \cos 2\pi nx \) and \( g_n(x) = \sqrt{2} \sin 2\pi nx \). Then \( \{1, f_1, g_1, f_2, g_2, \ldots \} \) is a countably infinite orthonormal set that is a Schauder basis for this vector space.

Theorem 3.7.5. An orthogonal set of non-zero vectors is linearly independent.

Proof. Let \( W \) be an orthogonal set of non-zero vectors in a given inner-product space \( V \). Suppose \( w_1, \ldots, w_n \) are distinct vectors in \( W \) and consider

\[
u = s_1 w_1 + \cdots + s_n w_n.
\]

The inner product \( \langle v, w_i \rangle \) is given by

\[
\langle v, w_i \rangle = \left\langle \sum_j s_j w_j, w_i \right\rangle = \sum_j s_j \langle w_j, w_i \rangle = s_i \langle w_i, w_i \rangle.
\]
3.7. SETS OF ORTHOGONAL VECTORS

Since \( \langle w_i, w_i \rangle \neq 0 \), it follows that

\[
s_i = \frac{\langle v, w_i \rangle}{\|w_i\|^2} \quad 1 \leq i \leq n.
\]

In particular, if \( v = 0 \) then \( s_j = 0 \) for \( 1 \leq j \leq n \) and the vectors in \( W \) are linearly independent.

**Corollary 3.7.6.** If \( v \in V \) is a linear combination of an orthogonal sequence of distinct, non-zero vectors \( w_1, \ldots, w_n \), then \( v \) satisfies the identity

\[
v = \sum_{i=1}^{n} \frac{\langle v, w_i \rangle}{\|w_i\|^2} w_i,
\]

and equals the sum of the projections of \( v \) onto \( w_1, \ldots, w_n \).

**Theorem 3.7.7.** Let \( V \) be an inner-product space and assume \( v_1, \ldots, v_n \) are linearly independent vectors in \( V \). Then it is possible to construct an orthogonal sequence of vectors \( w_1, \ldots, w_n \in V \) such that for each \( k = 1, \ldots, n \) the set

\[
\{ w_1, \ldots, w_k \}
\]

is a basis for the subspace spanned by \( v_1, \ldots, v_k \).

**Proof.** First, let \( w_1 = v_1 \). The remaining vectors are defined inductively as part during the proof. Suppose the vectors

\[
w_1, \ldots, w_m \quad (1 \leq m < n)
\]

have been chosen so that for every \( k \)

\[
\{ w_1, \ldots, w_k \} \quad 1 \leq k \leq m
\]

is an orthogonal basis for the subspace spanned by \( v_1, \ldots, v_k \). Let

\[
w_{m+1} = v_{m+1} - \sum_{i=1}^{m} \frac{\langle v_{m+1}, w_i \rangle}{\|w_i\|^2} w_i.
\]

Then \( w_{m+1} \neq 0 \), for otherwise \( v_{m+1} \) is a linear combination of \( w_1, \ldots, w_m \) and hence a linear combination of \( v_1, \ldots, v_m \). For \( j \in \{1, \ldots, m\} \), we also have

\[
\langle w_{m+1}, w_j \rangle = \langle v_{m+1}, w_j \rangle - \sum_{i=1}^{m} \frac{\langle v_{m+1}, w_i \rangle}{\|w_i\|^2} \langle w_i, w_j \rangle
\]

\[
= \langle v_{m+1}, w_j \rangle - \frac{\langle v_{m+1}, w_j \rangle}{\|w_j\|^2} \langle w_j, w_j \rangle
\]

\[
= 0.
\]
Clearly, \( \{w_1, \ldots, w_{m+1}\} \) is an orthogonal set consisting of \( m + 1 \) non-zero vectors in the subspace spanned by \( v_1, \ldots, v_{m+1} \). Since the dimension of the latter subspace is \( m + 1 \), this set is a basis for the subspace.

The inductive construction of the vectors \( w_1, \ldots, w_n \) is known as the Gram-Schmidt orthogonalization process.

**Corollary 3.7.8.** Every finite-dimensional inner-product space has a basis of orthonormal vectors.

**Proof.** Let \( V \) be a finite-dimensional inner-product space. Suppose that \( v_1, \ldots, v_n \) is a basis for \( V \). Apply the Gram-Schmidt process to obtain a basis of orthogonal vectors \( w_1, \ldots, w_n \). Then, a basis of orthonormal vectors is given by

\[
\begin{align*}
\vec{u}_1 &= \frac{w_1}{\|w_1\|}, & \vec{u}_n &= \frac{w_n}{\|w_n\|}.
\end{align*}
\]

**Example 3.7.9.** Consider the vectors

\[
\begin{align*}
v_1 &= (2, 2, 1) \\
v_2 &= (3, 6, 0) \\
v_3 &= (6, 3, 9)
\end{align*}
\]

in \( \mathbb{R}^3 \) equipped with the standard inner product. Apply the Gram-Schmidt process to \( v_1, v_2, v_3 \) to obtain an orthogonal basis.

Applying the Gram-Schmidt process to \( v_1, v_2, v_3 \), we get

\[
\begin{align*}
w_1 &= (2, 2, 1) \\
w_2 &= (3, 6, 0) - \frac{\langle (3, 6, 0), (2, 2, 1) \rangle}{9} (2, 2, 1) \\
&= (3, 6, 0) - 2(2, 2, 1) = (-1, 2, -2) \\
w_3 &= (6, 3, 9) - \frac{\langle (6, 3, 9), (2, 2, 1) \rangle}{9} (2, 2, 1) - \frac{\langle (6, 3, 9), (-1, 2, -2) \rangle}{9} (-1, 2, -2) \\
&= (6, 3, 9) - 3(2, 2, 1) + 2(-1, 2, -2) = (-2, 1, 2).
\end{align*}
\]

It is easily verified that \( w_1, w_2, w_3 \) is an orthogonal set of vectors.
3.7. SETS OF ORTHOGONAL VECTORS

Definition 3.7.10. Let \( V \) be an inner-product space and \( W \) be any set of vectors in \( V \). The orthogonal complement of \( W \) denoted by \( W^\perp \) is the set of all vectors in \( V \) that are orthogonal to every vector in \( W \) or

\[
W^\perp = \{ v \in V \mid \langle v, w \rangle = 0 \ \forall \ w \in W \}.
\]

Problem 3.7.11. Let \( W \) be any subset of vector space \( V \). Show that \( W^\perp \) is a closed subspace of \( V \) and that any vector in the subspace spanned by \( W \) is orthogonal to any vector in \( W^\perp \).

Let \( m_1, m_2 \in W^\perp \) and \( s \in F \). For any vector \( w \in W \), we have

\[
\langle m_1, w \rangle = \langle m_2, w \rangle = 0.
\]

This implies

\[
\langle sm_1 + m_2, w \rangle = s \langle m_1, w \rangle + \langle m_2, w \rangle = 0.
\]

That is, \( sm_1 + m_2 \in W^\perp \). Hence, \( W^\perp \) is a subspace of \( V \).

To see that \( W^\perp \) is closed, we let \( m \) be any point in the closure of \( W^\perp \) and \( m_1, m_2, \ldots \in W^\perp \) be a sequence that converges to \( m \). The continuity of the inner product, from Theorem 3.6.16, implies that, for all \( w \in W \),

\[
\langle m, w \rangle = \langle \lim_{n \to \infty} m_n, w \rangle = \lim_{n \to \infty} \langle m_n, w \rangle = 0.
\]

Therefore, \( m \in W^\perp \) and the orthogonal complement contains all of its limit points.

Notice also that any vector \( w \) in the subspace spanned by \( W \) can be written as \( w = \sum_i s_i w_i \) with \( w_i \in W \) and \( s_i \in F \). Therefore, the inner product of \( w \) with any \( w' \in W^\perp \) is given by

\[
\langle w, w' \rangle = \left\langle \sum_i s_i w_i, w' \right\rangle = \sum_i s_i \langle w_i, w' \rangle = 0.
\]

It follows that the subspace spanned by \( W \) is orthogonal to the subspace \( W^\perp \).

Definition 3.7.12. A complex matrix \( U \in \mathbb{C}^{n \times n} \) is called unitary if \( U^H U = I \). Similarly, a real matrix \( Q \in \mathbb{R}^{n \times n} \) is called orthogonal if \( Q^T Q = I \).

Theorem 3.7.13. Let \( V = \mathbb{C}^n \) be the standard inner product space and let \( U \in \mathbb{C}^{n \times n} \) define a linear operator on \( V \). Then, the following conditions are equivalent:
(i) The columns of $U$ form an orthonormal basis (i.e., $U^H U = I$),

(ii) the rows of $U$ form an orthonormal basis (i.e., $UU^H = I$),

(iii) $U$ preserves inner products (i.e., $\langle Uv, Uw \rangle = \langle v, w \rangle$ for all $v, w \in V$), and

(iv) $U$ is an isometry (i.e., $\|Uv\| = \|v\|$ for all $v \in V$).

Proof. If (i) holds, then $U$ is invertible because its columns are linearly independent. Thus, $U^H U = I$ implies $U^H = U^{-1}$ and (ii) follows. Likewise, (iii) holds because $\langle Uv, Uw \rangle = w^H U^H U v = w^H v = \langle v, w \rangle$ for all $v, w \in V$. Choosing $w = v$ gives (iv). Lastly, if $\|Uv\| = \|v\|$ for all $v \in V$, then $v^H (U^H U - I)v = \|Uv\|^2 - \|v\|^2 = 0$ for all $v \in V$. Since $U^H U - I$ is Hermitian, it must have a complete set of eigenvectors but all eigenvalues must be 0. Thus, $U^H U - I = 0$. □

3.7.1 Hilbert Spaces

Definition 3.7.14. A complete inner-product space is called a Hilbert space.

Definition 3.7.15. Recall that a subset $\{v_\alpha | \alpha \in A\}$ of a Hilbert space $V$ is said to be orthonormal if $\|v_\alpha\| = 1$ for every $\alpha \in A$ and $\langle v_\alpha, v_\beta \rangle = 0$ for all $\alpha \neq \beta$. If the subspace spanned by the family $\{v_\alpha | \alpha \in A\}$ is dense in $V$, we call this set an orthonormal basis.

Note that, according to this definition, an orthonormal basis for a Hilbert space $V$ is not necessarily a Hamel basis for $V$. However, it can be shown that any orthogonal basis is a subset of a Hamel basis. In practice it is the orthonormal basis, not the Hamel basis itself, which is of most use. None of these issues arise in finite-dimensional spaces, where an orthogonal basis is always a Hamel basis.

Let $\mathcal{B} = \{v_\alpha | \alpha \in A\}$ be an orthonormal basis for Hilbert space $V$. Then, each element $v \in V$ has a unique representation as

$$v = \sum_{\alpha \in A} s_\alpha v_\alpha.$$

Using orthogonality to compute $\langle v, v \rangle$, one gets the Parseval identity

$$\|v\|^2 = \sum_{\alpha \in A} |s_\alpha|^2.$$

Since $\|v\|^2 < \infty$ for all $v \in V$, the RHS also exists and is finite for all $v \in V$. 
3.8. LINEAR FUNCTIONALS

**Theorem 3.7.16.** Every orthonormal set in a Hilbert space $V$ can be enlarged to an orthonormal basis for $V$.

*Proof.* Let $x = \{v_\alpha | \alpha \in A_0\}$ be the initial orthonormal set. Let $X$ be the set of orthonormal subsets of $V$ and, for $x, y \in X$, consider the strict partial order defined by proper inclusion. Since $x$ is an element of $X$, the Hausdorff maximal principle implies that there exists a maximal simply ordered subset $Z$ of $X$ containing $x$. This shows the existence of a maximal orthonormal set $\{v_\alpha | \alpha \in A_0\}$, where $A_0 \subset A$.

Let $W$ be the closed subspace of $V$ generated by $\{v_\alpha | \alpha \in A_0\}$. If $W \neq V$, there is a unit vector $u \in W^\perp$, contradicting the maximality of the system $\{v_\alpha | \alpha \in A_0\}$. Thus, $W = V$ and we have enlarged the orthonormal set $x$ to a basis. $\square$

**Theorem 3.7.17.** A Hilbert space $V$ has a countable orthonormal basis if and only if $V$ is separable.

*Sketch of proof.* If $V$ is separable, then it contains a countable dense subset. Since this set is countable, it can be ordered into a sequence $v_1, v_2, \ldots$ such that, for every vector $v \in V$ and any $\epsilon > 0$, there exists an $n$ such that $\|v - v_n\| < \epsilon$. By removing all vectors that are linear combinations of previous vectors, this sequence can be pruned into a countable linearly independent set. Then, a countable orthonormal basis is generated by applying Gram-Schmidt orthogonalization to the pruned sequence of vectors. Conversely, if $V$ has a countable orthonormal basis, then linear combinations with rational coefficients can be used to construct a countable dense subset. $\square$

**Lemma 3.7.18.** Let $V$ be a Hilbert space and $v_1, v_2, \ldots$ be a countable orthogonal set. Then, $v = \sum_{i=1}^{\infty} v_i$ exists if and only if $\sum_{i=1}^{\infty} \|v_i\|^2 = M < \infty$.

*Proof.* For $u_n = \sum_{i=1}^{n} v_i$, and $w_n = \sum_{i=1}^{n} \|v_i\|^2$, orthogonality implies that

$$\|u_m - u_n\|^2 = \left\| \sum_{i=n+1}^{m} v_i \right\|^2 = \sum_{i=n+1}^{m} \|v_i\|^2 = |w_m - w_n|.$$ 

Thus, the sequence $u_n$ is Cauchy in $V$ if and only if $w_n$ is Cauchy in $\mathbb{R}$. $\square$

### 3.8 Linear Functionals

**Definition 3.8.1.** Let $V$ be a vector space over a field $F$. A linear transformation $f$ from $V$ into the scalar field $F$ is called a **linear functional** on $V$. 

That is, $f$ is a functional on $V$ such that

$$f(sv_1 + v_2) = sf(v_1) + f(v_2)$$

for all $v_1, v_2 \in V$ and $s \in F$.

**Example 3.8.2.** Let $F$ be a field and let $s_1, \ldots, s_n$ be scalars in $F$. Then the functional $f$ on $F^n$ defined by

$$f(v_1, \ldots, v_n) = s_1v_1 + \cdots + s_nv_n$$

is a linear functional. It is the linear functional which is represented by the matrix

$$\begin{bmatrix} s_1 & s_2 & \cdots & s_n \end{bmatrix}$$

relative to the standard ordered basis for $F^n$. Every linear functional on $F^n$ is of this form, for some scalars $s_1, \ldots, s_n$.

**Definition 3.8.3.** Let $n$ be a positive integer and $F$ a field. If $A$ is an $n \times n$ matrix with entries in $F$, the **trace** of $A$ is the scalar

$$\text{tr}(A) = A_{11} + A_{22} + \cdots + A_{nn}.$$ 

**Example 3.8.4.** The trace function is a linear functional on the matrix space $F^{n \times n}$ since

$$\text{tr}(sA + B) = \sum_{i=1}^{n} (sA_{ii} + B_{ii})$$

$$= s \sum_{i=1}^{n} A_{ii} + \sum_{i=1}^{n} B_{ii}$$

$$= s \text{tr}(A) + \text{tr}(B).$$

**Example 3.8.5.** Let $[a, b]$ be a closed interval on the real line and let $C([a, b])$ be the space of continuous real-valued functions on $[a, b]$. Then

$$L(g) = \int_{a}^{b} g(t)dt$$

defines a linear functional $L$ on $C([a, b])$. 
Theorem 3.8.6 (Riesz). Let $V$ be a finite-dimensional Hilbert space and $f$ be a linear functional on $V$. Then, there exists a unique vector $v \in V$ such that $f(w) = \langle w, v \rangle$ for all $w \in V$.

Proof. If we choose an orthonormal basis $B = v_1, \ldots, v_n$ for $V$, then the inner product of $w = t_1v_1 + \cdots + t_nv_n$ and $v = s_1v_1 + \cdots + s_nv_n$ will be

$$\langle w, v \rangle = t_1\bar{s}_1 + \cdots + t_n\bar{s}_n.$$ 

If $f$ is a linear functional on $V$, then $f$ has the form

$$f(w) = f(t_1v_1 + \cdots + t_nv_n) = t_1f(v_1) + \cdots + t_nf(v_n).$$

Thus, we can choose $s_j = f(v_j)$ to get $\langle w, v \rangle = f(w)$ and this gives

$$v = f(v_1)v_1 + \cdots + f(v_n)v_n.$$ 

Let $v'$ be any vector that satisfies $f(w) = \langle w, v' \rangle$ for all $w \in V$. Then, we see that $\langle w, v - v' \rangle = 0$ for all $w \in V$. This implies that $v - v' = 0$. \qed
Chapter 4

Representation and Approximation

4.1 Best Approximation

Suppose $W$ is a subspace of a Banach space $V$. For any $v \in V$, consider the problem of finding a vector $w \in W$ such that $\|v - w\|$ is as small as possible.

**Definition 4.1.1.** The vector $w \in W$ is a best approximation of $v \in V$ by vectors in $W$ if

$$\|v - w\| \leq \|v - w'\|$$

for all $w' \in W$.

If $W$ is spanned by the vectors $w_1, \ldots, w_n \in V$, then we can write

$$v = w + e = s_1 w_1 + \cdots + s_n w_n + e,$$

where $e$ is the approximation error.

Finding a best approximation is, in general, rather difficult. However, if the norm $\| \cdot \|$ corresponds to the induced norm of an inner product, then one can use orthogonal projection and the problem is greatly simplified. This chapter focuses mainly on computing the best approximation of arbitrary vectors in a Hilbert space.

A best approximation exists if $W$ is closed and the Banach space $V$ is reflexive (i.e., it equals its double dual). In addition, it is unique if the Banach space $V$ is strictly convex (i.e., $\|v + w\| < 2$ for all distinct $v, w \in V$ such that $\|v\| = \|w\| = 1$).
Theorem 4.1.2. Suppose $W$ is a subspace of a Hilbert space $V$ and $\mathbf{v}$ is a vector in $V$. Then, we have the following:

1. The vector $w \in W$ is a best approximation of $\mathbf{v} \in V$ by vectors in $W$ if and only if $\mathbf{v} - w$ is orthogonal to every vector in $W$.

2. If a best approximation of $\mathbf{v} \in V$ by vectors in $W$ exists, it is unique.

3. If $W$ has a countable orthogonal basis $w_1, w_2, \ldots$ and is closed, then

$$ w = \sum_{i=1}^{\dim(W)} \frac{\langle \mathbf{v}, w_i \rangle}{\| w_i \|^2} w_i \quad (4.1) $$

exists and equals the best approximation of $\mathbf{v}$ by vectors in $W$.

Proof. Let $w \in W$ and suppose $\mathbf{v} - w$ is orthogonal to every vector in $W$. For any $w' \in W$, we have $\mathbf{v} - w' = (\mathbf{v} - w) + (w - w')$ and

$$ \| \mathbf{v} - w' \|^2 = \| \mathbf{v} - w \|^2 + 2\Re \langle \mathbf{v} - w, w - w' \rangle + \| w - w' \|^2 $$

$$ = \| \mathbf{v} - w \|^2 + \| w - w' \|^2 \quad (4.2) $$

$$ \geq \| \mathbf{v} - w \|^2. $$

For the converse, we note that, if $\mathbf{v} - w$ is not orthogonal to all vectors in $W$, then there must be some $u \in W$ such that $\langle \mathbf{v} - w, u \rangle \neq 0$. Then, we let $w''$ be the projection of $\mathbf{v} - w$ onto $u$. Next, we define $w' = w + w''$ and observe that $w' \in W$.

Thus, Lemma 3.6.14 implies

$$ \| \mathbf{v} - w' \|^2 = \| \mathbf{v} - w - w'' \|^2 = \| \mathbf{v} - w \|^2 - \| \frac{\langle \mathbf{v} - w, u \rangle}{\| u \|^2} \langle \mathbf{v} - w, u \rangle \| < \| \mathbf{v} - w \|^2. $$

Thus, $w$ is not a best approximation of $\mathbf{v}$ by vectors in $W$.

For uniqueness, suppose $w, w' \in W$ are best approximations of $\mathbf{v}$ by vectors in $W$. Then $\| \mathbf{v} - w \| = \| \mathbf{v} - w' \|$ and (4.2) implies that $\| \mathbf{v} - w \| = 0$. That is, if a best approximation exists then it is unique.

Finally, assume $W$ is closed and $w_1, w_2, \ldots$ is a countable orthogonal basis. Then, for (4.1), let the sequence of partial sums be $u_n \triangleq \sum_{i=1}^{n} w_i \langle \mathbf{v}, w_i \rangle / \| w_i \|^2$. Next, observe that $\mathbf{v} - u_n$ is orthogonal to $w_j$ for $j \in \{1, \ldots, n\}$, i.e.,

$$ \langle \mathbf{v} - u_n, w_j \rangle = \langle \mathbf{v}, w_j \rangle - \sum_{i=1}^{n} \frac{\langle \mathbf{v}, w_i \rangle}{\| w_i \|^2} \langle w_i, w_j \rangle $$

$$ = \langle \mathbf{v}, w_j \rangle - \frac{\langle \mathbf{v}, w_j \rangle}{\| w_j \|^2} \langle w_j, w_j \rangle = 0. $$
4.1. BEST APPROXIMATION

Since \( v - u_n \) is orthogonal to every vector in \( W_n = \operatorname{span}\{w_1, \ldots, w_n\} \), we see that \( u_n \) is the best approximation of \( v \) by vectors in \( W_n \). If \( \dim(W) < \infty \), then this completes the proof.

If \( \dim(W) = \infty \), then we must argue that the limit of \( u_n \) exists and lies in \( W \). The orthogonality of \( w_1, \ldots, w_n \) implies \( \|v\|^2 = \|v - u_n\|^2 + \|u_n\|^2 \). From this, we see that \( \|u_n\|^2 = \sum_{i=1}^{n} |\langle v, w_i \rangle|^2 / \|w_i\|^2 \) is an increasing real sequence upper bounded by \( \|v\|^2 \). It follows that the RHS converges to a finite limit. Thus, we can apply Lemma 3.7.18 to show convergence \( u_n \to w \). Since \( W \) is closed, it follows that \( w \in W \). By construction, \( v - w \) is orthogonal to \( w_j \) for \( j \in \mathbb{N} \) and, thus, every vector in \( W \). Hence, \( w \) is the best approximation of \( v \) by vectors in \( W \).

**Definition 4.1.3.** Whenever the vector \( w \) in Theorem 4.1.2 exists, it is called the orthogonal projection of \( v \) onto \( W \). If every vector in \( V \) has an orthogonal projection onto \( W \), then the mapping \( E: V \to W \), which assigns to each vector in \( V \) its orthogonal projection onto \( W \), is called the orthogonal projection of \( V \) onto \( W \).

One can use Theorem 4.1.14 to verify that this is consistent with the concept of orthogonal projection from Definition 4.1.11. Theorem 4.1.2 also implies the following result, known as Bessel’s inequality.

**Corollary 4.1.4.** Let \( v_1, v_2, \ldots \) be a countable orthogonal set of distinct non-zero vectors in an inner-product space \( V \) and let \( W = \operatorname{span}\{v_1, v_2, \ldots\} \). If \( v \in V \), then

\[
\sum_{i=1}^{\dim(W)} \frac{|\langle v, v_i \rangle|^2}{\|v_i\|^2} \leq \|v\|^2.
\]

Moreover, equality holds if and only if

\[
v = \sum_{i=1}^{\dim(W)} \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i.
\]

**Proof.** Let the projection of \( v \) onto the closure of the span of \( v_1, v_2, \ldots \) (i.e., \( \overline{W} \)) be

\[
w = \sum_{i=1}^{\dim(W)} \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i.
\]

Then, the error \( u = v - w \) satisfies \( \langle u, v_i \rangle = 0 \) and \( \|u\|^2 = \|v\|^2 - \|w\|^2 \). Noting that \( \|u\|^2 \geq 0 \) and

\[
\|w\|^2 = \sum_{i=1}^{\dim(W)} \frac{|\langle v, v_i \rangle|^2}{\|v_i\|^2},
\]
we see that $\|w\|^2 \leq \|v\|^2$ with equality iff $u = 0$. \hfill \Box

**Problem 4.1.5.** Let $W$ be the subspace of $\mathbb{R}^2$ spanned by the vector $(1, 2)$. Using the standard inner product, let $E$ be the orthogonal projection of $\mathbb{R}^2$ onto $W$. Find

1. a formula for $E(x_1, x_2)$
2. the matrix of $E$ in the standard ordered basis, i.e., $E(x_1, x_2) = Ex$
3. $W^{\perp}$
4. an orthonormal basis in which $E$ is represented by the matrix

$$ E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}. $$

### 4.1.1 Projection Operators

**Definition 4.1.6.** A function $F : X \to Y$ with $Y \subseteq X$ is **idempotent** if $F(F(x)) = F(x)$. When $F$ is a linear transformation, this reduces to $F^2 = F \cdot F = F$.

**Definition 4.1.7.** Let $V$ be a vector space and $T : V \to V$ be a linear transformation. If $T$ is idempotent, then $T$ is called a **projection**.

**Example 4.1.8.** The idempotent matrix $A$ is a projection onto the first two coordinates.

$$ A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} $$

**Theorem 4.1.9.** Let $V$ be a vector space and $T : V \to V$ be a projection operator. Then, the range $\mathcal{R}(T)$ and the $\mathcal{N}(T)$ are disjoint subspaces of $V$.

**Proof.** For all $v \in V - \{0\}$, we need to prove that $v$ is not in both the range and nullspace. Let $v \in V$ be in the range of $T$ so that there is a $w \in V$ such that $Tw = v$. Then, $Tv = T^2w = Tw = v$ and $v$ is not in the null space unless $v = 0$.

Let $\_v$ be in the null space of $T$, then $Tv = 0$. But, $Tv = v$ for all $v$ in the range. Therefore, $v$ is not in the range unless $v = 0$. From this, we see that only $0 \in V$ is in both the range and nullspace. Therefore, they are disjoint subspaces. \hfill \Box
Example 4.1.10. Consider the linear transform \( T : V \to V \) defined by \( T = I - P \), where \( P \) is a projection. It is easy to verify that \( T \) is a projection operator because
\[
T^2 = (I - P)(I - P) = I - P - P + P^2 = I - P = T.
\]

Notice also that \( P(I - P)v = 0 \) implies that \( \mathcal{R}(T) \subseteq \mathcal{N}(P) \) and \( T v = v \) for \( v \in \mathcal{N}(P) \) implies \( \mathcal{N}(P) \subseteq \mathcal{R}(T) \). Therefore, \( \mathcal{R}(T) = \mathcal{N}(P) \) and \( I - P \) is a projection onto \( \mathcal{N}(P) \).

Definition 4.1.11. Let \( V \) be an inner-product space and \( P : V \to V \) be a projection operator. If \( \mathcal{R}(P) \perp \mathcal{N}(P) \), then \( P \) is called an orthogonal projection.

Example 4.1.12. Let \( V \) be an inner-product space and \( P : V \to V \) be an orthogonal projection. Then, \( v = P v + (I - P)v \) defines an orthogonal decomposition of \( v \) because \( P v \in \mathcal{R}(P) \), \((I - P)v \in \mathcal{N}(P) \) (e.g., \( P((I - P)v) = 0 \)), and \( \mathcal{R}(P) \perp \mathcal{N}(P) \). In addition, \( V = \mathcal{R}(P) \oplus \mathcal{N}(P) \) and hence \( \mathcal{N}(P) = \mathcal{R}(P) \perp \).

Theorem 4.1.13. For \( V = F^n \) with the standard inner product, an idempotent Hermitian matrix \( P \) defines an orthogonal projection operator.

Proof. We simply must verify that the range and null space are orthogonal. Since \( P u \in \mathcal{R}(P) \) and \((I - P)v \in \mathcal{N}(P) \) (e.g., \( P((I - P)v) = 0 \)), we observe that
\[
\langle P u, (I - P)v \rangle = v^H (I - P)^H P u = v^H (P - P^H P) u = v^H (P - P^2) u = 0.
\]

\( \square \)

Theorem 4.1.14. Suppose \( W \) is a closed subspace of a separable Hilbert space \( V \) and let \( E \) denote the orthogonal projection of \( V \) on \( W \). Then, \( E \) is an idempotent linear transformation of \( V \) onto \( W \), \( E w' = 0 \) iff \( w' \in W \perp \), and
\[
V = W \oplus W \perp.
\]

Proof. Let \( v \) be any vector in \( V \). Since \( E v \) is the best approximation of \( v \) by vectors in \( W \), it follows that \( v \in W \) implies \( E v = v \). Therefore, \( E (E v) = E v \) for any \( v \in V \) since \( E v \in W \). That is, \( E^2 = E \) and \( E \) is idempotent.

To show that \( E \) is a linear transformation, let \( w_1, w_2, \ldots \) be a countable orthonormal basis for \( W \) (whose existence follows from Theorem 3.7.17). Using part
CHAPTER 4. REPRESENTATION AND APPROXIMATION

3 of Theorem 4.1.2, we find that

\[ E(s_1 v_1 + v_2) = \sum_{i=1}^{\dim(W)} \langle s_1 v_1 + v_2, w_i \rangle w_i = \sum_{i=1}^{\dim(W)} \langle v_1, w_i \rangle w_i + \sum_{i=1}^{\dim(W)} \langle v_2, w_i \rangle w_i = s_1 E v_1 + E v_2. \]

Therefore, \( E \) is a linear transformation. It also follows that \( E w' = 0 \) iff \( w' \in W^\perp \) because \( W^\perp \) can be defined by the fact that \( \langle w', w_i \rangle = 0 \) for \( i \in \mathbb{N} \).

Again, let \( v \in V \) and recall that (by Theorem 4.1.2) \( E v \) is the unique vector in \( W \) such that \( v - E v \) is in \( W^\perp \). Therefore, the equation \( v = E v + (v - E v) \) gives a unique decomposition of \( v \) into \( E v \in W \) and \( v - E v \in W^\perp \). This unique decomposition implies that \( V \) is the direct sum of \( W \) and \( W^\perp \). Lastly, one finds from the definition of \( W^\perp \) that

\[ W \cap W^\perp = \{ u \in W | \langle u, w \rangle = 0 \ \forall \ w \in W \} \subseteq \{ u \in W | \langle u, u \rangle = 0 \} = \{ 0 \}. \]

**Corollary 4.1.15.** Let \( W \) be a closed subspace of a separable Hilbert space \( V \) and \( E \) be the orthogonal projection of \( V \) on \( W \). Then \( I - E \) is the orthogonal projection of \( V \) on \( W^\perp \).

**Proof.** This follows directly from the orthogonal decomposition in Theorem 4.1.14. One can also verify that \( I - E \) is an idempotent linear transformation of \( V \) with range \( W^\perp \) and nullspace \( W \). From Definition 4.1.11, we see that \( I - E \) is an orthogonal projection. \( \square \)

**Example 4.1.16.** Let \( V = \mathbb{C}^n \) be the standard \( n \)-dimensional complex Hilbert space. Let \( U \in \mathbb{C}^{n \times m} \) be a matrix whose columns \( u_1, \ldots, u_m \) form an orthonormal set in \( V \). Then, the best approximation of \( v \in V \) by vectors in \( \mathcal{R}(U) \) (as defined by (4.1)) can also be written as

\[ w = U U^H v = \sum_{i=1}^{m} u_i (u_i^H v). \]
4.2 Computing Approximations in Hilbert Spaces

4.2.1 Normal Equations

Suppose $V$ is a Hilbert space the subspace $W$ is spanned by $w_1, \ldots, w_n \in V$. Consider the situation where the sequence $w_1, \ldots, w_n$ is linearly independent, but not orthogonal. In this case, it is not possible to apply (4.1) directly. It is nevertheless possible to obtain a similar expression for the best approximation of $v$ by vectors in $W$. Theorem 4.1.2 asserts that $\hat{v} \in W$ is a best approximation of $v \in V$ by vectors in $W$ if and only if $v - \hat{v}$ is orthogonal to every vector in $W$. This implies that

$$\langle v - \hat{v}, w_j \rangle = \langle v - \sum_{i=1}^n s_i w_i, w_j \rangle = 0$$

or, equivalently,

$$\sum_{i=1}^n s_i \langle w_i, w_j \rangle = \langle v, w_j \rangle$$

for $j = 1, \ldots, n$. These conditions yield a system of $n$ linear equations in $n$ unknowns, which can be written in the matrix form

$$\begin{bmatrix}
\langle w_1, w_1 \rangle & \langle w_2, w_1 \rangle & \cdots & \langle w_n, w_1 \rangle \\
\langle w_1, w_2 \rangle & \langle w_2, w_2 \rangle & \cdots & \langle w_n, w_2 \rangle \\
\vdots & \vdots & \ddots & \vdots \\
\langle w_1, w_n \rangle & \langle w_2, w_n \rangle & \cdots & \langle w_n, w_n \rangle
\end{bmatrix}
\begin{bmatrix}
s_1 \\
s_2 \\
\vdots \\
s_n
\end{bmatrix} =
\begin{bmatrix}
\langle v, w_1 \rangle \\
\langle v, w_2 \rangle \\
\vdots \\
\langle v, w_n \rangle
\end{bmatrix}.$$

We can rewrite this matrix equation as

$$G \hat{s} = t$$

where

$$t^T = (\langle v, w_1 \rangle, \langle v, w_2 \rangle, \ldots, \langle v, w_n \rangle)$$

is the cross-correlation vector, and

$$\hat{s}^T = (s_1, s_2, \ldots, s_n)$$

is the vector of coefficients. Equations of this form are collectively known as the normal equations.
Definition 4.2.1. The \( n \times n \) matrix
\[
G = \begin{bmatrix}
\langle w_1, w_1 \rangle & \langle w_2, w_1 \rangle & \cdots & \langle w_n, w_1 \rangle \\
\langle w_1, w_2 \rangle & \langle w_2, w_2 \rangle & \cdots & \langle w_n, w_2 \rangle \\
\vdots & \vdots & \ddots & \vdots \\
\langle w_1, w_n \rangle & \langle w_2, w_n \rangle & \cdots & \langle w_n, w_n \rangle \\
\end{bmatrix}
\] (4.3)
is called the Gramian matrix. Since \( g_{ij} = \langle w_j, w_i \rangle \), it follows that the Gramian is a Hermitian symmetric matrix, i.e., \( G^H = G \).

Definition 4.2.2. A matrix \( M \in F^{n \times n} \) is positive-semidefinite if \( M^H = M \) and \( v^H M v \geq 0 \) for all \( v \in F^n - \{0\} \). If the inequality is strict, \( M \) is positive-definite.

An important aspect of positive-definite matrices is that they are always invertible. This follows from noting that \( Mv = 0 \) for \( v \neq 0 \) implies that \( v^H M v = 0 \) and contradicts the definition of positive definite.

Theorem 4.2.3. A Gramian matrix \( G \) is always positive-semidefinite. It is positive-definite if and only if the vectors \( w_1, \ldots, w_n \) are linearly independent.

Proof. Since \( g_{ij} = \langle w_j, w_i \rangle \), the conjugation property of the inner product implies \( G^H = G \). Using \( v = (v_1, \ldots, v_n)^T \in F^n \), we can write

\[
v^H G v = \sum_{i=1}^n \sum_{j=1}^n \bar{v}_i g_{ij} v_j = \sum_{i=1}^n \sum_{j=1}^n \bar{v}_i \langle w_j, w_i \rangle v_j \\
= \sum_{i=1}^n \sum_{j=1}^n \langle v_j w_j, v_i w_i \rangle = \left\langle \sum_{j=1}^n v_j w_j, \sum_{i=1}^n v_i w_i \right\rangle \\
= \left\| \sum_{i=1}^n v_i w_i \right\|^2 \geq 0.
\] (4.4)

That is, \( v^H G v \geq 0 \) for all \( v \in F^n \).

Suppose that \( G \) is not positive-definite. Then, there exists \( v \in F^n - \{0\} \) such that \( v^H G v = 0 \). By (4.4), this implies that

\[
\sum_{i=1}^n v_i w_i = 0
\]
and hence the sequence of vectors \( w_1, \ldots, w_n \) is not linearly independent.
Conversely, if \( G \) is positive-definite then \( v^H G v > 0 \) and

\[
\left\| \sum_{i=1}^{n} v_i w_i \right\| > 0
\]

for all \( v \in F^n - \{0\} \). Thus, the vectors \( w_1, \ldots, w_n \) are linearly independent. \( \square \)

### 4.2.2 Orthogonality Principle

**Theorem 4.2.4.** Let \( w_1, \ldots, w_n \) be vectors in an inner-product space \( V \) and denote the span of \( w_1, \ldots, w_n \) by \( W \). For any vector \( v \in V \), the norm of the error vector

\[
e = v - \sum_{i=1}^{n} s_i w_i
\]

is minimized when the error vector \( e \) is orthogonal to every vector in \( W \). If \( \hat{v} \) denotes the least-squares approximation of \( v \) then

\[
\langle v - \hat{v}, w_j \rangle = 0
\]

for \( j = 1, \ldots, n \).

**Proof.** Minimizing \( \|e\|^2 \) over \( s \), where \( e \) is given by (4.5) requires minimizing

\[
J(s) = \langle v - \sum_{i=1}^{n} s_i w_i, v - \sum_{j=1}^{n} s_j w_j \rangle
\]

\[
= \langle v, v \rangle - \sum_{i=1}^{n} \langle s_i w_i, v \rangle - \sum_{j=1}^{n} \langle v, s_j w_j \rangle + \sum_{i=1}^{n} \sum_{j=1}^{n} \langle s_i w_i, s_j w_j \rangle
\]

\[
= \langle v, v \rangle - \sum_{i=1}^{n} s_i \langle w_i, v \rangle - \sum_{j=1}^{n} \bar{s}_j \langle v, w_j \rangle + \sum_{i=1}^{n} \sum_{j=1}^{n} s_i \bar{s}_j \langle w_i, w_j \rangle.
\]

To take the derivative with respect to \( s \in \mathbb{C}^n \), we use the decomposition \( s = a + jb \), with \( a, b \in \mathbb{R}^n \), and define the differential operators

\[
\frac{\partial}{\partial s} \triangleq \frac{1}{2} \left( \frac{\partial}{\partial a} - j \frac{\partial}{\partial b} \right), \quad \frac{\partial}{\partial \bar{s}} \triangleq \frac{1}{2} \left( \frac{\partial}{\partial a} + j \frac{\partial}{\partial b} \right)
\]

where \( \partial/\partial a = (\partial/\partial a_1, \ldots, \partial/\partial a_n)^T \). Since \( J(s) \) is real function of \( s \), a stationary...
point of $J$ can be found by setting either derivative to 0. Choosing $\bar{s}$, gives

$$\frac{\partial}{\partial \bar{s}} J(\bar{s}) = -\begin{bmatrix} \langle v, w_1 \rangle \\ \langle v, w_2 \rangle \\ \vdots \\ \langle v, w_n \rangle \end{bmatrix} + \begin{bmatrix} \langle w_1, w_1 \rangle & \langle w_2, w_1 \rangle & \cdots & \langle w_n, w_1 \rangle \\ \langle w_1, w_2 \rangle & \langle w_2, w_2 \rangle & \cdots & \langle w_n, w_2 \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle w_1, w_n \rangle & \langle w_2, w_n \rangle & \cdots & \langle w_n, w_n \rangle \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix} = 0.$$ 

In matrix form, this yields the familiar equation

$$G \bar{s} = \bar{t}.$$ 

To ensure that this extremum is in fact a minimum, one can compute the 2nd derivative to show that the Hessian is $G$. Since $G$ is a positive-semidefinite matrix, the extremum is indeed a minimum.

This implies that $\|e\|^2$ is minimized if and only if $G \bar{s} = \bar{t}$. That is, $\|e\|^2$ is minimized if and only if $v - \hat{v}$ is orthogonal to every vector in $W$. □

Note that it is also possible to prove this theorem using the Cauchy-Schwarz inequality or the projection theorem.

### 4.3 Approximation for Systems of Linear Equations

#### 4.3.1 Matrix Representation

For finite-dimensional vector spaces, least-squares (i.e., best approximation) problems have natural matrix representations. Suppose $V = F^m$ and $w_1, w_2, \ldots, w_n \in V$ are column vectors. Then, the approximation vector is given by

$$\hat{v} = \sum_{i=1}^{n} s_i w_i$$

In matrix form, we have

$$\hat{v} = As,$$

where $A = [w_1 \cdots w_n]$. The optimization problem can then be reformulated as follows. Determine $\bar{s} \in F^n$ such that

$$\|e\|^2 = \|v - \hat{v}\|^2 = \|v - As\|^2$$
is minimized. Note that this occurs when the error vector is orthogonal to every vector in $W$, i.e.,

$$
\langle e, w_j \rangle = \langle v - \hat{v}, w_j \rangle = \langle v - As, w_j \rangle = 0
$$

for $j = 1, \ldots, n$.

### 4.3.2 Standard Inner Products

When $\| \cdot \|$ is the norm induced by the standard inner product, these conditions can be expressed as

$$
\begin{bmatrix}
  w_1^H \\
  \vdots \\
  w_n^H
\end{bmatrix}
(v - As) = 0.
$$

Using the definition of $A$, we obtain

$$
A^H As = A^H v.
$$

The matrix $A^H A$ is the Gramian $G$ defined in (4.3). The vector $A^H v$ is the cross correlation vector $t$.

When the vectors $w_1, \ldots, w_n$ are linearly independent, the Gramian matrix is positive definite and hence invertible. The optimal solution for the least-squares problem is therefore given by

$$
\hat{s} = (A^H A)^{-1} A^H v = G^{-1} t.
$$

The matrix $(A^H A)^{-1} A^H$ is often called the **pseudoinverse**.

The best approximation of $v \in V$ by vectors in $W$ is equal to

$$
\hat{v} = As = A (A^H A)^{-1} A^H v.
$$

The matrix $P = A (A^H A)^{-1} A^H$ is called the **projection matrix** for the range of $A$. It defines an orthogonal projection onto the range of $A$ (i.e., the subspace spanned by the columns of $A$).
4.3.3 Generalized Inner Products

We can also consider the case of a general inner product. Recall that an inner product on \( V \) is completely determined by the values

\[
h_{ji} = \langle e_i, e_j \rangle
\]

and that it can be expressed in terms of the matrix \( H \) (where \([H]_{j,i} = h_{j,i}\)) as

\[
\langle v, w \rangle = w^H H v.
\]

Minimizing \( \|e\|^2 = \|v - A\hat{s}\|^2 \) and using the orthogonality principle lead to the matrix equation

\[
A^H H A \hat{s} = A^H H v.
\]

When the vectors \( w_1, \ldots, w_n \) are linearly independent, the optimal solution is given by

\[
\hat{s} = (A^H H A)^{-1} A^H H v.
\]

4.3.4 Minimum Error

Let \( \hat{v} \in W \) be the best approximation of \( v \) by vectors in \( W \). Again, we can write

\[
v = \hat{v} + e,
\]

where \( e \in W^\perp \) is the minimum achievable error. The squared norm of the minimum error is given implicitly by

\[
\|v\|^2 = \|\hat{v} + e\|^2 = \langle \hat{v} + e, \hat{v} + e \rangle = \langle \hat{v}, \hat{v} \rangle + \langle e, e \rangle = \|\hat{v}\|^2 + \|e\|^2.
\]

We can then find an explicit expression for the approximation error,

\[
\|e\|^2 = \|v\|^2 - \|\hat{v}\|^2 = v^H H v - \hat{v}^H H \hat{v} = v^H H v - \hat{v}^H A^H H A \hat{v} = v^H H v - \hat{v}^H HA (A^H HA)^{-1} A^H H v = v^H \left( H - HA (A^H HA)^{-1} A^H H \right) v.
\]
4.4 Applications and Examples in Signal Processing

4.4.1 Linear Regression

Let \((x_1, y_1), \ldots, (x_n, y_n)\) be a collection of points in \(\mathbb{R}^2\). A linear regression problem consists in finding scalars \(a\) and \(b\) such that

\[ y_i \approx ax_i + b \]

for \(i = 1, \ldots, n\). Define the error component \(e_i\) by \(e_i = y_i - ax_i - b\), then

\[
\begin{bmatrix}
  y_1 \\
  \vdots \\
  y_n \\
\end{bmatrix}
= \begin{bmatrix}
  x_1 \\
  \vdots \\
  x_n \\
\end{bmatrix}
+ \begin{bmatrix}
  1 \\
  \vdots \\
  1 \\
\end{bmatrix}
+ \begin{bmatrix}
  e_1 \\
  \vdots \\
  e_n \\
\end{bmatrix}
= \begin{bmatrix}
  x_1 & 1 \\
  \vdots & \vdots \\
  x_n & 1 \\
\end{bmatrix}
\begin{bmatrix}
  a \\
  b \\
\end{bmatrix}
+ \begin{bmatrix}
  e_1 \\
  \vdots \\
  e_n \\
\end{bmatrix}
\]

In vector form, we can rewrite this equation as

\[ y = A\hat{s} + e, \]

where \(y = (y_1, \ldots, y_n)^T\), \(\hat{s} = (a, b)^T\), \(e = (e_1, \ldots, e_n)^T\), and

\[
A = \begin{bmatrix}
  x_1 & 1 \\
  \vdots & \vdots \\
  x_n & 1 \\
\end{bmatrix}
\]

This equation has a form analogous to the matrix representation of a least-squares problems. Consider the goal of minimizing \(\|e\|^2\). The line that minimizes the sums of the squares of the \emph{vertical} distances between the data abscissas and the line is then given by

\[ \hat{s} = (A^H A)^{-1} A^H y. \]

4.4.2 Linear Minimum Mean-Squared Error Estimation

Let \(Y, X_1, \ldots, X_n\) be a set of zero-mean random variables. The goal of the linear minimum mean-squared error (LMMSE) estimation problem is to find coefficients \(s_1, \ldots, s_n\) such that

\[ \hat{Y} = s_1X_1 + \cdots + s_nX_n \]
minimizes the MSE $E[|Y - \hat{Y}|^2]$. Using the inner product defined by

$$\langle X, Y \rangle = E[X \overline{Y}], \quad (4.6)$$

we can compute the linear minimum mean-squared estimate $\hat{Y}$ using

$$G_S = t,$$

where

$$G = \begin{bmatrix}
E[X_1X_1] & E[X_2X_1] & \cdots & E[X_nX_1] \\
E[X_1X_2] & E[X_2X_2] & \cdots & E[X_nX_2] \\
\vdots & \vdots & \ddots & \vdots \\
E[X_1X_n] & E[X_2X_n] & \cdots & E[X_nX_n]
\end{bmatrix}$$

and

$$t = \begin{bmatrix}
E[YX_1] \\
E[YX_2] \\
\vdots \\
E[YX_n]
\end{bmatrix}.$$ 

If the matrix $G$ is invertible, the minimum mean-squared error is given by

$$\|Y - \hat{Y}\|^2 = E[YY] - t^H G^{-1} t.$$

### 4.4.3 The Wiener Filter

Suppose that the sequence of zero-mean random variables $\{X[t]\}$ is wide-sense stationary, and consider the FIR filter

$$Y[t] = \sum_{k=0}^{K-1} h[k] X[t - k]$$

$$= \begin{bmatrix} X[t] & \cdots & X[t - K + 1] \end{bmatrix} \begin{bmatrix} h[0] \\ \vdots \\ h[K - 1] \end{bmatrix} = (X[t])^T h.$$ 

The goal is to design this filter in such a way that its output is as close as possible to a desired sequence $\{Z[t]\}$. In particular, we want to minimize the mean-squared error

By the orthogonality principle, the mean-squared error is minimized when the error is orthogonal to the data; that is, for $j = 0, 1, \ldots, K - 1$, we have

$$
\left\langle Z[t] - \sum_{k=0}^{K-1} h[k] X[t - k], X[t - j] \right\rangle = 0,
$$

or, equivalently, we can write

$$
\langle Z[t], X[t - j] \rangle = \sum_{k=0}^{K-1} h[k] \langle X[t - k], X[t - j] \rangle.
$$

Using (4.6), we obtain

$$
E[Z[t]X[t - j]] = \sum_{k=0}^{K-1} h[k] E[X[t - k]X[t - j]].
$$

(4.7)

where $j = 1, \ldots, K - 1$.

For this specific case where the normal equations are defined in terms of the expectation operator, these equations are called the **Wiener-Hopf** equations. The Gramian of the Wiener-Hopf equations can be expressed in a more familiar form using the autocorrelation matrix. Recall that $\{X[t]\}$ is a wide-sense stationary process. As such, we have

$$
R_{xx}(j - k) = R_{xx}(j, k) = E[X[t - k]X[t - j]] = \langle X[t - k], X[t - j] \rangle.
$$

Also define

$$
R_{zx}(j) = E[Z[t]X[t - j]] = \langle Z[t], X[t - j] \rangle.
$$

Using this notation, we can rewrite (4.7) as

$$
R_{zx} = \begin{bmatrix}
  R_{zx}(0) \\
  R_{zx}(1) \\
  \vdots \\
  R_{zx}(K - 1)
\end{bmatrix} = R_{xx} \begin{bmatrix}
  h[0] \\
  h[1] \\
  \vdots \\
  h[K - 1]
\end{bmatrix}
$$

where the $K \times K$ autocorrelation matrix is given by

$$
R_{xx} = \begin{bmatrix}
  R_{xx}[0] & \overline{R}_{xx}[1] & \cdots & \overline{R}_{xx}[K - 1] \\
  R_{xx}[1] & R_{xx}[0] & \cdots & \overline{R}_{xx}[K - 2] \\
  \vdots & \vdots & \ddots & \vdots \\
  R_{xx}[K - 1] & R_{xx}[K - 2] & \cdots & R_{xx}[0]
\end{bmatrix}.
$$
Note that the matrix $R_{xx}$ is Toeplitz, i.e., all the elements on a diagonal are equal. Assuming that $R_{xx}$ is invertible, the optimal filter taps are then given by

$$h = R_{xx}^{-1} R_{zx}.$$  

The minimum mean-squared error is given by

$$\|Z - Y\|^2 = \|Z\|^2 - \|Y\|^2 = E[ZZ] - E[h^H XX^T h] = E[ZZ] - h^H R_{xx} h = E[ZZ] - R_{xx}^H h,$$

where $t$ can be ignored because the processes are WSS.

### 4.4.4 LMMSE Filtering in Practice

While theoretical treatments of optimal filtering often assume one has well-defined random variables with known statistics, this is rarely the case in practice. Yet, there is a very close connection between Wiener filtering and natural data driven approaches. Consider the problem from the previous section and let $x[1], x[2], \ldots, x[N]$ and $z[1], z[2], \ldots, z[N]$ be realizations of the random processes.

As an application, one can think of the $x[t]$ sequence as the received samples in a wireless communication system and the $z[t]$ sequence as a pilot sequence (i.e., known to both the transmitter and receiver). It is assumed the transmitted sequence has been convolved with an unknown LTI system. This type of degradation is known as intersymbol interference (ISI) and the goal is to find a linear filter $h[0], h[1], \ldots, h[K - 1]$ that removes as much ISI as possible. A suitable cost function for this goal is

$$J(h) = \sum_{t=K}^{N} \lambda^{N-t} \left| z[t] - \sum_{k=0}^{K-1} h[k] x[t - k] \right|^2,$$

where the exponential weighting factor $\lambda$ emphasizes the most recently received symbols because, in reality, the channel conditions are changing with time.
Using the vector $z = \begin{bmatrix} z[K] & z[K + 1] & \cdots & z[N] \end{bmatrix}$ and the matrix

$$A = \begin{bmatrix}
  x[K] & x[K - 1] & \cdots & x[1] \\
  \vdots & \vdots & \ddots & \vdots \\
  x[N] & x[N - 1] & \cdots & x[N - K + 1]
\end{bmatrix},$$

we can rewrite this cost function as

$$J(h) = (Ah - z)^H \Lambda (Ah - z),$$

where $\Lambda$ is a diagonal matrix with diagonal entries $[\lambda^{N-K} \lambda^{N-K+1} \cdots \lambda^0]$. Using the orthogonality principle, one finds that the optimal solution is given by the normal equation

$$A^H \Lambda Ah = A^H \Lambda z.$$

To see the connection with Wiener filtering, the key observation is that the matrix $A^H \Lambda A$ and the vector $A^H \Lambda z$ are sample-average estimates of the correlation matrix and cross-correlation vector. This is because, for large $N$ and $\lambda$ close to 1, we have

$$[A^H \Lambda A]_{ij} = \sum_{t=K}^{N} \lambda^{N-t} x[t-j+1] \overline{x}[t-i+1] \approx \frac{R_{xx}(i-j)}{1-\lambda}$$

and

$$[A^H \Lambda z]_i = \sum_{t=K}^{N} \lambda^{N-t} z[t] \overline{x}[t-i+1] \approx \frac{R_{zx}(i)}{1-\lambda}.$$

Another benefit of this approach is that, as each new sample arrives, the solution $h$ can be updated with low complexity. Consider the matrix $G_N = A^H \Lambda A$ and vector $b_N = A^H \Lambda z$ as a function of $N$. Then, $G_{N+1} = \lambda G_N + u^H u$ and $b_{N+1} = \lambda b_N + z[N+1] u^H$, where

$$u = \begin{bmatrix} x[N+1] & x[N] & \cdots & x[N-K+2] \end{bmatrix}.$$ (4.8)

The updated solution vector $h_{N+1} = G_{N+1}^{-1} b_{N+1}$ can be computed efficiently using the Sherman-Morrison matrix inversion formula.
4.5 Dual Approximation

4.5.1 Minimum-Norm Solutions

In many cases, one is interested in finding the minimum-norm vector that satisfies some feasibility constraints. For example, an underdetermined system of linear equations has an infinite number of solutions. But, in practice, it often makes sense to prefer the minimum-norm solution over other solutions. Finding this solution is very similar to finding the best approximation.

Let $V$ be a Hilbert space and $w_1, w_2, \ldots, w_n$ be a set of linearly independent vectors in $V$. For any $v \in V$, consider finding the scalars $s_1, s_2, \ldots, s_n$ that minimize

$$
\left\| v - \sum_{i=1}^{n} s_i w_i \right\|.
$$

The answer is clearly given by the best approximation of $v$ by vectors in the span of $w_1, w_2, \ldots, w_n$. The orthogonality principle tells us that $s_1, s_2, \ldots, s_n$ must satisfy

$$
\begin{bmatrix}
\langle w_1, w_1 \rangle & \langle w_2, w_1 \rangle & \cdots & \langle w_n, w_1 \rangle \\
\langle w_1, w_2 \rangle & \langle w_2, w_2 \rangle & \cdots & \langle w_n, w_2 \rangle \\
\vdots & \vdots & \ddots & \vdots \\
\langle w_1, w_n \rangle & \langle w_2, w_n \rangle & \cdots & \langle w_n, w_n \rangle 
\end{bmatrix}
\begin{bmatrix}
s_1 \\
s_2 \\
\vdots \\
s_n
\end{bmatrix}
=
\begin{bmatrix}
\langle v, w_1 \rangle \\
\langle v, w_2 \rangle \\
\vdots \\
\langle v, w_n \rangle
\end{bmatrix}.
$$

(4.9)

The same problem can also be posed in a different manner.

**Theorem 4.5.1.** Let $V$ be a Hilbert space and $w_1, w_2, \ldots, w_n$ be a set of linearly independent vectors in $V$. The dual approximation problem is to find the vector $w \in V$ of minimum-norm that satisfies $\langle w, w_i \rangle = c_i$ for $i = 1, \ldots, n$. This vector is given by

$$
w = \sum_{i=1}^{n} s_i w_i,
$$

(4.10)

where the coefficients $s_1, s_2, \ldots, s_n$ can be found by solving (4.9) with $\langle v, w_i \rangle = c_i$.

**Proof.** Let $W = \text{span}(w_1, w_2, \ldots, w_n)$ and notice that the subset

$$A = \{ u \in V \mid \langle u, w_i \rangle = c_i \ \forall \ i = 1, \ldots, n \}$$

is simply the orthogonal complement $W^\perp$ translated by some fixed vector $v \in A$. This is because, for all $x \in W^\perp$, we have $\langle x, w_i \rangle = 0$ and $\langle v - x, w_i \rangle = c_i$. 
Thus, there is a one-to-one correspondence between \( u \in A \) and \( x \in W^\perp \) given by 
\[
u = v - x \]
and this implies
\[
\min_{u \in A} \|u\| = \min_{x \in W^\perp} \|v - x\|.
\]
Since the optimizer \( x^* \) of the RHS expression is the orthogonal projection of \( v \) onto \( W^\perp \), the resulting error vector \( v - x^* \) must be contained in \((W^\perp)^\perp = W\). With this knowledge, we let \( w = v - x^* \) and use (4.9) to solve for \( s_1, \ldots, s_n \) because we know the RHS satisfies \( \langle v, w_i \rangle = c_i \). Since \( w_1, \ldots, w_n \) are linearly independent, the Gramian is full rank and this linear system has a unique solution. \( \square \)

### 4.5.2 Underdetermined Linear Systems

Let \( A \in \mathbb{C}^{m \times n} \) with \( m < n \) be the matrix representation of an underdetermined system of linearly independent equations and \( v \in \mathbb{C}^m \) be any column vector. Then, the dual approximation theorem can be applied to solve the problem
\[
\min_{\hat{s} : A\hat{s} = v} \|\hat{s}\|.
\]
To see this as a dual approximation, we can rewrite the constraint as \((A^H)^H \hat{s} = v\) so that the columns of \( A^H \) define the vectors \( w_1, \ldots, w_n \) in Theorem 4.5.1. Then, the theorem concludes that the minimum norm solution lies in \( \mathcal{R}(A^H) \) (i.e., the column space of \( A^H \)). Using (4.10), one gathers that \( \hat{s} = A^H t \) for some \( t \) with \( A(A^H t) = v \). If the rows of \( A \) are linearly independent, then the columns of \( A^H \) are linearly independent and \((AA^H)^{-1}\) exists. In this case, the solution \( \hat{s} \) can be obtained in closed form and is given by
\[
\hat{s} = A^H (AA^H)^{-1} v.
\]

### 4.6 Projection onto Convex Sets

So far, we have focused on the projection of vectors onto subspaces. In this section, similar results are obtained for the projection of vectors onto convex sets.

**Definition 4.6.1.** Let \( V \) be a vector space. The subset \( A \subseteq V \) is called a convex set if, for all \( a_1, a_2 \in A \) and \( \lambda \in (0, 1) \), we have \( \lambda a_1 + (1 - \lambda) a_2 \in A \). The set is strictly convex if, for all \( a_1, a_2 \in A \) and \( \lambda \in (0, 1) \), we have \( \lambda a_1 + (1 - \lambda) a_2 \in A^\circ \).
CHAPTER 4. REPRESENTATION AND APPROXIMATION

Problem 4.6.2. Show that the intersection of convex sets is convex.

Definition 4.6.3. Let $V$ be a Hilbert space and $A \subseteq V$ be a closed convex set. The orthogonal projection of $v \in V$ onto $A$ is the mapping $P_A : V \to A$ defined by

$$P_A(v) \triangleq \arg \min_{u \in A} \|u - v\|.$$ 

Remark 4.6.4. If $A$ is compact, then the existence of the minimum (for any norm) is given by topology because $\|v - u\|$ is continuous in $u$. Uniqueness follows from geometric considerations. If both $u$ and $u'$ achieve the minimum distance $d$, then the convexity of the norm implies that the line segment between them also achieves the minimum distance. But, this implies that the closed ball of radius $d$ in $V$ contains a line segment on its boundary and one can use the Cauchy-Schwarz inequality to show this is impossible.

The following theorem instead uses vector space methods to establish the same result for all closed convex $A$.

Theorem 4.6.5. For Hilbert space $V$, the orthogonal projection of $v \in V$ onto a closed convex set $A \subseteq V$ exists and is unique.

Proof. Let $d = \inf_{u \in A} \|u - v\|$ be the infimal distance between $v$ and the set $A$. Next, consider any sequence $\{u_1, u_2, \ldots \} \subseteq A$ that achieves the infimum so that

$$\lim_{n \to \infty} \|u_n - v\| = d.$$ 

Since $A$ is complete, the next step is showing that this sequence is Cauchy. The parallelogram law states that $\|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2 - \|x + y\|^2$ and applying
4.6. PROJECTION ONTO CONVEX SETS

this to \( x = v - u_n \) and \( y = v - u_m \) gives

\[
\|u_m - u_n\|^2 = \|(v - u_n) - (v - u_m)\|^2 \\
= 2\|v - u_n\|^2 + 2\|v - u_m\|^2 - \|(v - u_n) + (v - u_m)\|^2 \\
= 2\|v - u_n\|^2 + 2\|v - u_m\|^2 - 4\|v - \frac{u_n + u_m}{2}\|^2 \\
\leq 2\|v - u_n\|^2 + 2\|v - u_m\|^2 - 4d^2
\]

because the convexity of \( A \) implies \( \frac{u_n + u_m}{2} \in A \) and therefore \( \|v - \frac{u_n + u_m}{2}\|^2 \geq d^2 \).

Since the limit of the RHS (as \( m, n \to \infty \)) equals 0, we find that the sequence \( u_n \) is Cauchy and therefore the limit \( u^* \) must exist. Since \( u_n \in A \) and \( A \) is closed, we also see that \( u^* \in A \). Therefore, the infimum is achieved as a minimum.

Uniqueness can be seen by assuming instead that \( u_m, u_n \) are two elements in \( A \) which are both at a distance \( d \) from \( v \). Then, the above derivation shows that \( \|u_m - u_n\|^2 \leq 0 \). Therefore, they are the same point.

Remark 4.6.6. The same result holds for norm projections in many other Banach spaces including \( L^p \) and \( \ell^p \) for \( 1 < p < \infty \). In general, it is required that the Banach space be strictly convex (for uniqueness) and reflexive (for existence).

Earlier in this chapter, we studied the equivalence between the orthogonality and Hilbert-space projections onto subspaces. The following result can be seen as a generalization of that result to Hilbert-space projections onto convex sets.

Theorem 4.6.7. For any \( v \notin A \), a necessary and sufficient condition for \( u^* = P_A(v) \) is that \( \text{Re} \langle v - u^*, u - u^* \rangle \leq 0 \) for all \( u \in A \).

Proof. Let \( u^* = P_A(v) \) be the unique projection of \( v \) onto \( A \). For all \( u \in A \) and any \( \alpha \in (0, 1) \), observe that \( u' = (1 - \alpha)u^* + \alpha u = u^* + \alpha(u - u^*) \in A \) due to convexity. The optimality of \( u^* \) implies that

\[
\|v - u^*\|^2 \leq \|v - u'\|^2 \\
\leq \|v - u^* - \alpha(u - u^*)\|^2 \\
= \|v - u^*\|^2 + \alpha^2\|u - u^*\|^2 - 2\alpha\text{Re} \langle v - u^*, u - u^* \rangle.
\]

Thus, \( \text{Re} \langle v - u^*, u - u^* \rangle \leq \frac{\alpha}{2}\|u - u^*\|^2 \). One can establish necessity by taking the limit as \( \alpha \to 0 \). For sufficiency, we assume \( \text{Re} \langle v - u^*, u - u^* \rangle \leq 0 \) and we
write
\[
\|v - u\|^2 - \|v - u^*\|^2 = \|(v - u^*) - (u - u^*)\|^2 - \|v - u^*\|^2 \\
= \|v - u^*\|^2 + \|u - u^*\|^2 - 2\text{Re}(v - u^*, u - u^*) - \|v - u^*\|^2 \\
\geq 0.
\]
Thus, \(\|v - u\|^2 \geq \|v - u^*\|^2\) for all \(u \in A\) and \(u^* = P_A(v)\). \(\square\)

4.6.1 Projection Properties and Examples

Let \(A\) be a closed convex subset of a Hilbert space \(V\) over \(\mathbb{R}\). By drawing a simple picture (e.g., see Figure 4.1), one can see that projecting \(v\) onto \(A\) is an operation that is translation invariant. Specifically, this means that translating the set \(A\) and the vector \(v\) by the same vector \(v_0\) results in an output that is also translated by \(v_0\). Mathematically, this means that, for all \(v, v_0 \in V\), the projection onto \(V\) satisfies
\[
P_{A + v_0}(v + v_0) = \arg \min_{u \in A + v_0} \|u - v - v_0\| \\
= v_0 + \arg \min_{u' \in A} \|(u' + v_0) - v - v_0\| \\
= v_0 + \arg \min_{u' \in A} \|u' - v\| \\
= v_0 + P_A(v).
\]

This also leads to the following trick. If a projection is easy when the set is centered, then one can: (i) translate the problem so that the set is centered, (ii) project onto the centered set, and (iii) translate back.

Using the best approximation theorem, it is easy to verify that the orthogonal projection of \(v \in V\) onto a one-dimensional subspace \(W = \text{span}(w)\) is given by
\[
P_W(v) = \frac{\langle v, w \rangle}{\|w\|^2} w.
\]

A hyperplane is a closed subspace of \(U \subset V\) that satisfies a single linear equality of the form \(\langle v, w \rangle = 0\) for all \(v \in U\). Such a subspace is said to have co-dimension one (e.g., if \(\dim(V) = n\), then \(\dim(U) = n - 1\)). Equivalently, \(U\) can be seen as the orthogonal complement of a one-dimensional subspace (e.g., \(U = W^\perp\)). Thus, we can write
\[
P_U(v) = P_{W^\perp}(v) = v - \frac{\langle v, w \rangle}{\|w\|^2} w.
\]
4.6. PROJECTION ONTO CONVEX SETS

Similarly, a linear equality such as $\langle v, w \rangle = c$, where $v_0$ is any vector in $V$ satisfying $\langle v_0, w \rangle = c$, defines an affine hyperplane. This is the shifted subspace $U + v_0$ of co-dimension one because

$$\langle v, w \rangle = \langle u + v_0, w \rangle = \langle u, w \rangle + \langle v_0, w \rangle = 0 + c = c.$$ 

Thus, we can project onto $U + v_0$ by translating, projecting, and then translating back. This gives

$$P_{U+v_0}(v) = (v - v_0) - \frac{\langle v - v_0, w \rangle}{\|w\|^2} w + v_0 = v - \frac{\langle v, w \rangle - c}{\|w\|^2} w,$$

which does not depend on the choice of $v_0$.

Next, let $H$ be the subset of $v \in V$ satisfying the linear inequality $\langle v, w \rangle \geq c$. Then, $H$ is a closed convex set known as a half space. For any $v \in H$, we have $P_H(v) = v$ and, for any $v \notin H$, we have $P_H(v) = P_{U+v_0}(v)$ because the closest point must lie on the separating hyperplane and achieve the inequality with equality.

For any $v \in H$, one can put these together to see that

$$P_H(v) = \begin{cases} v & \text{if } \langle v, w \rangle \geq c \\ v - \frac{\langle v, w \rangle - c}{\|w\|^2} w & \text{if } \langle v, w \rangle < c. \end{cases} \quad (4.11)$$

**Theorem 4.6.8.** Let $V$ be a Hilbert space over $\mathbb{R}$ and $A \subset V$ be a closed convex set. For any $v \notin A$, there is an affine hyperplane $U' = \{ u \in V | \langle u, w \rangle = c \}$ (defined by $w \in V$ and $c \in \mathbb{R}$) such that $\langle v, w \rangle < c$ and $\langle u, w \rangle \geq c$ for all $u \in A$.

**Proof.** Let $u^* = P_A(v)$ be the orthogonal projection of $v$ onto $A$ and define $w = u^* - v$ and $c = \langle u^*, w \rangle$. From Theorem 4.6.7, we see that $\langle u - u^*, u - u^* \rangle \leq 0$ for all $u \in A$. Thus, for all $u \in A$, we have

$$\langle u, w \rangle = \langle w, u \rangle = \langle u^* - v, u \rangle = -\langle u - u^*, u \rangle$$

$$\quad \geq -\langle u - u^*, u^* \rangle = \langle u^* - v, u^* \rangle$$

$$\quad = \langle w, u^* \rangle = \langle u^*, w \rangle = c,$$

where $(a)$ follows from $\langle u - u^*, u - u^* \rangle \leq 0$ for all $u \in A$. For $\langle v, w \rangle$, we observe that together, $u^* \in A$ and $v \notin A$, imply that

$$0 < \|u^* - v\|^2 = \langle u^* - v, u^* - v \rangle$$

$$\quad = \langle u^*, u^* - v \rangle - \langle v, u^* - v \rangle = c - \langle v, u^* - v \rangle,$$

which shows that $\langle v, w \rangle < c$ and completes the proof. \qed
**Corollary 4.6.9 (Farkas’ Lemma).** Let \( B \in \mathbb{R}^{m \times n} \) be a matrix and \( v \in \mathbb{R}^m \) be a vector. Then, exactly one of the following two conditions hold:

1. There exists \( s \in \mathbb{R}^n \) such that \( Bs = v \) and \( s \geq 0 \).

2. There exists \( w \in \mathbb{R}^m \) such that \( w^T B \geq 0 \) and \( w^T v < 0 \).

**Proof.** Consider the closed convex set \( A = \{ Bs | s \geq 0 \} \), where \( s \geq 0 \) denotes \( s_i \geq 0 \) for \( i = 1, \ldots, n \). If \( v \in A \), then we see that the first condition holds.

If \( v \notin A \), then we apply Theorem 4.6.8 using the standard Hilbert space \( \mathbb{R}^m \) to see that there exists \( w \in \mathbb{R}^m \) and \( c \in \mathbb{R} \) such that \( w^T v < c \) and \( w^T u \geq c \) for all \( u \in A \). Next, we observe that \( A \) is a cone (i.e., for all \( \alpha \geq 0 \) and \( u \in A \), we have \( \alpha u \in A \)). Thus, if there is any \( u \in A \) such that \( w^T u < 0 \), then \( w^T u \) can take any non-positive value for some \( u \in A \). This gives a contradiction and shows that \( w^T u \geq 0 \) for all \( u \in A \). Since \( 0 \in A \), \( c > 0 \) would also give a contradiction and it follows that \( c \leq 0 \) and \( w^T v < 0 \).

This establishes that either the first or second condition must hold. But, if they both hold, then we get the contradiction

\[
0 > w^T v = w^T (Bs) = (w^T B)s \geq 0,
\]

where the last step holds because \( w^T B \geq 0 \) and \( s \geq 0 \). Thus, exactly one holds. \( \square \)

**Theorem 4.6.10.** Let \( V \) be Hilbert space over \( \mathbb{R} \) and \( A \subset V \) be a closed convex set. Then, \( A \) equals the intersection of a set of half spaces.

**Proof.** Let \( \mathcal{H} \) be the set of all half spaces in \( V \) and let \( \mathcal{G} = \{ H \in \mathcal{H} | A \subseteq H \} \) be the subset of half spaces containing \( A \). For example, consider the half spaces defined by tangent planes passing through points on the boundary of \( A \). Let \( B = \cap_{H \in \mathcal{G}} H \) be the intersection of all the half spaces in \( \mathcal{G} \). Since each half space contains \( A \), it is clear that \( A \subseteq B \). To show that \( A = B \), we will show that \( (x \notin A) \rightarrow (x \notin B) \). If \( x \notin A \), then Theorem 4.6.8 shows that there is an affine hyperplane that separates \( x \) from \( A \) and an associated half space \( G \) that contains \( A \) but not \( x \). Since \( G \) contains \( A \), it follows that \( G \in \mathcal{G} \). But, \( x \notin G \) implies \( x \notin B \) because \( B \) is the intersection of the half spaces in \( \mathcal{G} \). This completes the proof. \( \square \)
4.6. PROJECTION ONTO CONVEX SETS

4.6.2 Minimum Distance Between Two Convex Sets

Now, consider the smallest distance between two disjoint closed convex sets \( A, B \subseteq V \). In this case, a unique solution may exist but a some things can go wrong. If the two sets are not strictly convex (e.g., consider two squares), then it is clearly possible for their to multiple pairs of points that achieve the minimum distance. Even if the two sets are strictly convex, one may find that the infimum is achieved as the points wander off to infinity. For example, consider the strictly convex hyperbolic sets

\[
A = \{(x, y) | x^2 - y^2 \geq 1, x > 0\} \quad \text{and} \quad B = \{(x, y) | y^2 - x^2 \geq 1, y \geq 0\}.
\]

These two sets share the line \( x = y > 0 \) as an asymptote, so their infimal distance is 0.

To understand this behavior, we first note that the distance \( f(u, v) = \|u - v\| \) is a convex function on the convex product set \( A \times B \). It follows that any local minimum value is a global minimum value distance.

**Theorem 4.6.11.** Let \( V \) be a Hilbert space and consider the infimal distance

\[
d = \inf_{u \in A, v \in B} \|u - v\|
\]

between two disjoint closed convex sets \( A, B \subseteq V \). If either set is compact, then the infimum is achieved. If the infimum is achieved and either set is strictly convex, then the minimizing points \( u^*, v^* \) are unique.

**Proof.** Consider any sequence \((u_1, v_1), (u_2, v_2), \ldots \in A \times B \) that satisfies

\[
\lim_{n \to \infty} \|u_n - v_n\| = d.
\]

If \( B \) is compact, then there is a subsequence \( v_{n_j} \) that converges to some \( v^* \in B \). Since \( \|P_A(v_{n_j}) - v_{n_j}\| \leq \|u_{n_j} - v_{n_j}\| \), we can replace \( u_{n_j} \) by \( P_A(v_{n_j}) \) and still achieve the infimum. The continuity of \( P_A \) also shows that \( u_{n_j} \to u^* = P_A(v^*) \) and this implies \( \|u^* - v^*\| = d \). Also, \( P_B(u^*) = v^* \) because \( v^* \) is the unique closest point in \( B \) to \( u^* \). Notice that \( v^* \) may not be unique (due to the subsequence construction) and, thus, the pair \((u^*, v^*)\) is not unique in general.

Since \( \|u - v\| \) is a convex function on the convex product set \( A \times B \), there is a (possibly empty) convex set of minimizers

\[
M = \{(u, v) \in A \times B \mid \|u - v\| = d\}.
\]
Also, each component of the \((u, v)\) points in \(M\) must lie on the boundary of its set because otherwise one could reduce the smallest distance by moving one point along the minimum distance line towards the boundary. Now, suppose that (i) \(A\) is strictly convex and (ii) \(M\) contains more than one pair of minimizers. Then, condition (ii) implies that there must be two boundary points \(u_1, u_2 \in \partial A\) such that \(\alpha u_1 + (1 - \alpha) u_2 \in \partial A\) for \(\alpha \in [0, 1]\). But this contradicts condition (i) and shows that, if \(A\) is strictly convex, then there is at most one pair \((u^*, v^*) \in M\) of minimizing points.

**Remark 4.6.12.** Finding the minimum distance between two disjoint closed convex sets \(A, B \subseteq V\) is a classic problem that is solved nicely by the idea of alternating minimization. Let \(v_0 \in B\) be an arbitrary initial point and define

\[
\begin{align*}
\overline{u}_{n+1} &= \arg \min_{u \in A} \|u - v_n\| \\
\overline{v}_{n+1} &= \arg \min_{v \in B} \|u_{n+1} - v\|
\end{align*}
\]

Notice that the sequence \(d_n = \|u_n - v_n\|\) is non-increasing and must therefore have a limit. By adapting the previous proof, one can show that, if either set is compact, then the sequence \((u_n, v_n)\) converges to a pair of vectors that minimize the distance.

**Theorem 4.6.13.** Let \(V\) be a Hilbert space over \(\mathbb{R}\) and \(A, B\) be disjoint closed convex subsets of \(V\). If either set is compact, then there is an affine hyperplane \(\{a \in V \mid \langle a, w \rangle = c\}\) (defined by \(w \in V\) and \(c \in \mathbb{R}\)) such that \(\langle u, w \rangle > c\) for all \(u \in A\) and \(\langle u, w \rangle < c\) for all \(u \in B\).

**Proof.** Applying Theorem [4.6.11] gives a pair of points \((u^*, v^*) \in A \times B\) that minimize the distance and satisfy \(u^* = P_A(v^*)\) and \(v^* = P_B(u^*)\). Applying Theorem [4.6.8] to \(P_A(v^*)\) shows that \(\langle u, u^* - v^* \rangle \geq \langle u^*, u^* - v^* \rangle\) for all \(u \in A\). Similarly, applying Theorem [4.6.8] to \(P_B(u^*)\) shows that \(\langle v, v^* - u^* \rangle \geq \langle v^*, v^* - u^* \rangle\) for all \(v \in B\). Negating this gives \(\langle v, u^* - v^* \rangle \leq \langle v^*, u^* - v^* \rangle\). Now, we observe that \(\langle u^*, u^* - v^* \rangle - \langle v^*, u^* - v^* \rangle = \|u^* - v^*\|^2 > 0\) because \(u^* \neq v^*\). Thus, we can choose \(w = u^* - v^*\) and \(c = \frac{1}{2}(\langle u^*, u^* - v^* \rangle + \langle v^*, u^* - v^* \rangle)\) to guarantee that \(\langle u, w \rangle > c\) for all \(u \in A\) and \(\langle u, w \rangle < c\) for all \(u \in B\).
Chapter 5

Optimization

The foundation of engineering is the ability to use math and physics to design and optimize complex systems. The advent of computers has made this possible on an unprecedented scale. This chapter provides a brief introduction to mathematical optimization theory.

5.1 Derivatives in Banach Spaces

In this chapter, we assume that readers are familiar with derivatives as defined in undergraduate multivariable calculus. To gain insight, we first recall the standard interpretation of the derivative as a local linear approximation of a function. For a function \( f : \mathbb{R}^n \to \mathbb{R}^m \), this interpretation gives

\[
    f(x + h) = f(x) + J(x) \; h + \text{higher order terms},
\]

where \( J(x) \in \mathbb{R}^{m \times n} \) is the Jacobian matrix of \( f \) at \( x \).

Instead of interpreting a multivariate derivative as a matrix, we will view the derivative \( f'(x) \) as a linear transform \( T \) from the domain to codomain. This transform maps the input perturbation \( h \) to a local approximation of the output perturbation. Since both are finite dimensional in our example, the linear transform \( T \) is represented by the Jacobian matrix and we have

\[
    f'(x)(h) = Th = J(x) \; h.
\]

Mathematically, such definitions require the structure of a Banach space because
one needs the linear structure to compute differences, and the norm topology to define limits. Completeness guarantees that limits exist under mild conditions.

**Definition 5.1.1.** Let $f : X \to Y$ be a mapping from a vector space $X$ over $\mathbb{R}$ to a Banach space $(Y, \| \cdot \|)$. Then, if it exists, the \textit{Gâteaux differential} (or directional derivative) of $f$ at $x$ in direction $h$ is given by

$$
\delta f(x; h) \triangleq \lim_{t \to 0} \frac{f(x + th) - f(x)}{t},
$$

where the limit is with respect to the implied mapping from $t \in \mathbb{R}$ to $Y$.

When this directional derivative exits, we can write the approximation

$$
f(x + th) \approx f(x) + t \delta f(x; h).
$$

In fact, we can get a tighter characterization that is especially meaningful in the context of optimization.

**Lemma 5.1.2.** Let $Y = (\mathbb{R}, | \cdot |)$ and suppose that $\delta f(x; h)$ exists and is negative for some $f$, $x$, and $h$. Then, there exists $t_0 > 0$ such that $f(x + th) < f(x)$ for all $t \in (0, t_0)$.

**Proof.** The $\delta f(x; h)$ limit implies that, for any $\epsilon > 0$, there is a $t_0 > 0$ such that

$$
f(x + th) - f(x) \leq (\delta f(x; h) + \epsilon) t
$$

for all $t \in (0, t_0)$. If $\delta f(x; h) < 0$, then one can choose $\epsilon = -\frac{1}{2} \delta f(x; h)$ to see that the RHS is negative for all $t \in (0, t_0)$. The stated result follows.

**Example 5.1.3.** For the standard Banach space $X = Y = \mathbb{R}^2$, let $f(x) = (x_1 x_2, x_1 + x_2^2)$. Then, for $x = (1, 1)$, $h = (1, 2)$, we have

$$
\delta f(x, h) = \frac{d}{dt}((1 + t)(1 + 2t), (1 + t) + (1 + 2t)^2) \bigg|_{t=0} = (3, 5).
$$

**Problem 5.1.4.** Suppose $X = Y = L^1([0, 1])$ is the Banach space of Lebesgue absolutely integrable functions mapping $[0, 1]$ to $\mathbb{R}$ and $f(x) = \|x\| = \int_0^1 |x(s)|ds$ is the norm of $x$. Assuming the set $\{ s \in [0, 1] | x(s) = 0 \}$ has measure 0, show that

$$
\delta f(x; h) \triangleq \lim_{t \to 0} \int_0^1 \frac{1}{t}(|x(s) + th(s)| - |x(s)|)ds = \int_0^1 \text{sgn}(x(s))h(s)ds.
$$
5.1. DERIVATIVES IN BANACH SPACES

Definition 5.1.5. Let \( f : X \rightarrow Y \) be a mapping from a vector space \( X \) over \( \mathbb{R} \) to a Banach space \((Y, \| \cdot \|)\). Then, \( f \) is Gâteaux differentiable at \( x \) if the Gâteaux differential \( \delta f(x; h) \) exists for all \( h \in X \) and is a linear function of \( h \). If, in addition, \( X \) is a Banach space, then \( \delta f(x; h) \) must be a continuous linear function of \( h \).

Remark 5.1.6. For simplicity, our treatment of Gâteaux derivatives assumes \( X \) is a vector space over \( \mathbb{R} \) but similar results are possible over \( \mathbb{C} \) as well.

Definition 5.1.7. Let \( f : X \rightarrow Y \) be a mapping from a Banach space \((X, \| \cdot \|_X)\) to a Banach space \((Y, \| \cdot \|_Y)\). Then, \( f \) is Fréchet differentiable at \( x \) if there is a linear transformation \( T : X \rightarrow Y \) with \( \| T \| < \infty \) that satisfies

\[
\lim_{h \to 0} \frac{\| f(x + h) - f(x) - T(h) \|_Y}{\| h \|_X} = 0,
\]

(5.1)

where the limit is with respect to the implied Banach space mapping \( X \rightarrow \mathbb{R} \). In this case, the Fréchet derivative at \( x \) equals \( T \) and is denoted by \( f'(x) \) in general.

Example 5.1.8. A function \( f : \mathbb{R}^n \rightarrow \mathbb{R}^m \) with \( f = (f_1, f_2, \ldots, f_m)^T \) is (Fréchet) differentiable at \( x_0 \) if the mapping \( J \) from \( \mathbb{R}^n \) to the Jacobian matrix

\[
J(x) = f'(x) = \begin{bmatrix}
\frac{\partial f_1}{\partial x_1}(x) & \frac{\partial f_1}{\partial x_2}(x) & \cdots & \frac{\partial f_1}{\partial x_n}(x) \\
\frac{\partial f_2}{\partial x_1}(x) & \frac{\partial f_2}{\partial x_2}(x) & \cdots & \frac{\partial f_2}{\partial x_n}(x) \\
\vdots & \vdots & \ddots & \vdots \\
\frac{\partial f_m}{\partial x_1}(x) & \frac{\partial f_m}{\partial x_2}(x) & \cdots & \frac{\partial f_m}{\partial x_n}(x)
\end{bmatrix},
\]

exists and is continuous in \( x \) at \( x = x_0 \). A necessary and sufficient condition for this is that each partial derivative is continuous in \( x \) at \( x = x_0 \).

If \( m = 1 \), then the Jacobian is closely related to the gradient of the function

\[
\nabla f(x) \triangleq f'(x)^H = \left[ \frac{\partial f}{\partial x_1}(x) \frac{\partial f}{\partial x_2}(x) \cdots \frac{\partial f}{\partial x_n}(x) \right]^H.
\]

It is worth noting that the orientation of the gradient vector (i.e., row versus column vector) is sometimes defined differently. This is because derivatives can be understood as linear transforms and either orientation can be used to define the correct linear transform.

Example 5.1.9. Let \( X \) be a Hilbert space over \( \mathbb{R} \) and \( f : X \rightarrow \mathbb{R} \) be a real functional. If the Fréchet derivative \( f'(x) \) exists, then it is a continuous linear functional.
Thus, the Riesz representation theorem guarantees that there is a vector \( u \in X \) such that \( f'(x)(h) = \langle h, u \rangle \) for all \( h \in X \). This vector is called the gradient \( \nabla f(x) \) and it follows that
\[
f'(x)(h) = \langle h, \nabla f(x) \rangle \quad \text{for all } h \in X.
\]

**Problem 5.1.10.** In the setting of the previous example, show that, if \( \nabla f(x) \neq 0 \), then \( f(x - \delta \nabla f(x)) < f(x) \) for some \( \delta > 0 \).

**Theorem 5.1.11.** Let \( f : X \to Y \) be a mapping from a Banach space \( (X, \| \cdot \|_X) \) to a Banach space \( (Y, \| \cdot \|_Y) \). If \( f \) is Fréchet differentiable at \( x \) with derivative \( f' \), then \( f \) is Gâteaux differentiable at \( x \) with Gâteaux differential \( \delta f(x; h) = f'(x)(h) \).

**Proof.** For \( h = 0 \), the statement is trivial. For \( h \neq 0 \), we first observe that \( th \to 0 \) as \( t \to 0 \). Letting \( T = f'(x) \), we can combine this with (5.1) to see that
\[
0 = \lim_{t \to 0} \frac{\|f(x + th) - f(x) - T(th)\|_Y}{\|th\|_X} = \lim_{t \to 0} \frac{\|f(x + th) - f(x) - tT(h)\|}{t\|h\|_X} = \frac{1}{\|h\|_X} \lim_{t \to 0} \frac{\|f(x + th) - f(x) - tT(h)\|}{t\|h\|_X}.
\]
Thus, the Gâteaux differential exists and satisfies \( \delta f(x; h) = T(h) = f'(x)(h) \).

**Theorem 5.1.12.** Let \( X, Y, Z \) be Banach spaces and let \( f : X \to Y \) and \( g : Y \to Z \) be functions. If \( f \) is Fréchet differentiable at \( x \) and \( g \) is Fréchet differentiable at \( y = f(x) \), then \( (g \circ f)(x) = g(f(x)) \) is Fréchet differentiable at \( x \) with derivative \( g'(f(x)) \circ f'(x) \).

**Proof.** For the stated derivatives, the errors in the implied linear approximations are
\[
\phi(v) = f(x + v) - f(x) - f'(x)(v), \quad \psi(u) = g(y + u) - g(y) - g'(y)(u), \quad \rho(h) = g(f(x + h)) - g(f(x)) - (g'(y) \circ f'(x))(h).
\]
From the assumptions of differentiability, we know that the first two approximations become tight for small perturbations. In other words,
\[
\lim_{v \to 0} \frac{\|\phi(v)\|_Y}{\|v\|_X} = 0, \quad \lim_{u \to 0} \frac{\|\psi(u)\|_Z}{\|u\|_Y} = 0.
\]
Next, we observe that the definition of $\phi$ implies

$$g(f(x + h)) - g(f(x)) = g(f(x) + f'(x)(h) + \phi(h)) - g(y).$$

Combining this with the definition of $\rho$ shows that

$$\rho(h) = g(f(x) + f'(x)(h) + \phi(h)) - g(y) - (g'(y) \circ f'(x))(h)$$

$$= \psi(f'(x)(h) + \phi(h)) + g'(y)(f'(x)(h) + \phi(h)) - (g'(y) \circ f'(x))(h)$$

$$= \psi(f'(x)(h) + \phi(h)) + g'(y)(\phi(h)).$$

We take this opportunity to note that $\|g'(f(x)) \circ f'(x)\| \leq \|g'(f(x))\| \cdot \|f'(x)\| \leq \infty$ because $\|f'(x)\| \leq \infty$ and $\|g'(f(x))\| < \infty$. Since $\lim_{h \to 0} \|\phi(h)\| Y / \|h\| X = 0$, there is a $t > 0$ such that $\|\phi(h)\| Y \leq \|f'(x)\| \cdot \|h\| X$ if $\|h\| X < t$. Under the same condition, it follows that $2\|f'(x)\| \cdot \|h\| X \geq \|f'(x)\| \cdot \|h\| X + \|\phi(h)\| Y$. Using this, we can write

$$\frac{\|\rho(h)\| Z}{\|h\| X} = \frac{\|\psi(f'(x)(h) + \phi(h)) + g'(y)(\phi(h))\| Z}{\|h\| X}$$

$$\leq 2\|f'(x)\| \cdot \frac{\|\psi(f'(x)(h) + \phi(h))\| Z}{2\|f'(x)\| \cdot \|h\| X} + \frac{\|g'(y)(\phi(h))\| Z}{\|h\| X}$$

$$\leq 2\|f'(x)\| \cdot \frac{\|\psi(f'(x)(h) + \phi(h))\| Z}{\|f'(x)\| \cdot \|h\| X + \|\phi(h)\| Y} + \frac{\|g'(y)(\phi(h))\| Y}{\|h\| X}$$

$$\leq 2\|f'(x)\| \cdot \frac{\|\psi(f'(x)(h) + \phi(h))\| Z}{\|f'(x)(h) + \phi(h)\| Y} + \frac{\|g'(y)(\phi(h))\| Y}{\|h\| X}.$$

Since $(f'(x)(h) + \phi(h)) \to 0$ as $h \to 0$, it follows that the limit of the RHS, as $h \to 0$, also exists and equals 0. Thus, $\lim_{h \to 0} \|\rho(h)\| Z / \|h\| X = 0$ and the Fréchet derivative of $g(f(x))$ exists and satisfies the chain rule. \qed

**Theorem 5.1.13.** Let $X, Y$ be Banach spaces and $f : X \to Y$ be a function. For $x_1, x_2 \in X$, let $h = x_2 - x_1$ and assume the Gâteaux differential $\delta f((1 - s)x_1 + sx_2; h)$ exists for all $s \in [0, 1]$. Then, $\|f(x_2) - f(x_1)\| \leq M\|x_2 - x_1\|$, where

$$M = \sup_{s \in [0, 1]} \frac{\|\delta f((1 - s)x_1 + sx_2; h)\|}{\|x_2 - x_1\|}.$$
Proof. For \( w_1 = \frac{1}{2}(x_1 + x_2) \), observe that
\[
\frac{\|f(x_2) - f(x_1)\|}{\|x_2 - x_1\|} = \frac{\|f(x_2) - f(w_1) + f(w_1) - f(x_1)\|}{\|x_2 - x_1\|} \\
\leq \frac{\|f(x_2) - f(w_1)\| + \|f(w_1) - f(x_1)\|}{\|x_2 - x_1\|} \\
= \frac{\|f(x_2) - f(w_1)\|}{2\|x_2 - w_1\|} + \frac{\|f(w_1) - f(x_1)\|}{2\|w_1 - x_1\|}.
\]
Suppose that \( \|f(x_2) - f(x_1)\| > M\|x_2 - x_1\| \). Then, there is an \( \epsilon > 0 \) such that one or both of the following conditions must hold:
\[
\frac{\|f(x_2) - f(w_1)\|}{\|x_2 - w_1\|} \geq M + \epsilon \quad \text{and} \quad \frac{\|f(w_1) - f(x_1)\|}{\|w_1 - x_1\|} \geq M + \epsilon.
\]
Repeating indefinitely and choosing a satisfying subinterval at each step, one gets a sequence \( w_n \) of midpoints that converges to \( x = (1 - s)x_1 + sx_2 \) for some \( s \in [0, 1] \).

Since the Gâteaux differential \( \delta f(x; h) \) exists by assumption, it follows that
\[
M + \epsilon \leq \frac{\|f(w_n) - f(x)\|}{\|w_n - x\|} = \frac{\|f(x + 2^{-n}h) - f(x)\|}{2^n\|x_2 - x_1\|} \to \frac{\|\delta f(x; h)\|}{\|x_2 - x_1\|}.
\]
This contradicts the definition of \( M \) and, thus, \( \|f(x_2) - f(x_1)\| \leq M\|x_2 - x_1\| \). \( \square \)

Lemma 5.1.14. Let \( X, Y \) be Banach spaces and \( f : X \to Y \) be a function. If the Fréchet derivative \( f'(x) \) exists and satisfies \( \|f'(x)\| \leq L \) for all \( x \) in a convex set \( A \subseteq X \), then \( f \) is Lipschitz continuous on \( A \) with Lipschitz constant \( L \).

Proof. Assume \( \|f'(x)\| \leq L \) for all \( x \) in a convex set \( A \subseteq X \). Then, for any \( x_1, x_2 \in A \), let \( h = x_2 - x_1 \) and notice that Theorem [5.1.11] implies that
\[
\|\delta f(x_1 + sh; h)\| = \|f'(x_1 + sh)(h)\| \leq \|f'(x_1 + sh)\|\|h\|,
\]
for all \( s \in [0, 1] \). Applying Theorem [5.1.13], we see that \( \|f(x_2) - f(x_1)\| \leq M\|x_2 - x_1\| \) with \( M \leq \|f'(x)\| \leq L \). This completes the proof. \( \square \)

Lemma 5.1.15. Let \( f : X \to \mathbb{R} \) map the Hilbert space \( X \) to the real numbers. If \( \nabla f(x) \) exists and satisfies \( \|\nabla f(y) - \nabla f(x)\| \leq L\|y-x\| \), then
\[
|f(y) - f(x) - \langle y-x, \nabla f(x) \rangle| \leq \frac{1}{2}L\|y-x\|^2.
\]
5.2. UNCONSTRAINED OPTIMIZATION

Proof. Let \( h = y - x \) and \( \phi(t) = f(x + th) \). Then, \( \phi'(t) = \langle h, \nabla f(x + th) \rangle \) and

\[
\begin{align*}
|f(y) - f(x) - \langle h, \nabla f(x) \rangle| &= \int_0^1 (\phi'(t) - \phi'(0)) \, dt \\
&= \int_0^1 \langle h, \nabla f(x + th) - \nabla f(x) \rangle \, dt \\
&\leq \int_0^1 \|h\| \|\nabla f(x + th) - \nabla f(x)\| \, dt \\
&\leq \int_0^1 \|h\| L \|h\| \, dt \\
&= \frac{1}{2} L \|h\|^2.
\end{align*}
\]

\( \square \)

5.2 Unconstrained Optimization

Functions mapping elements of a vector space (over \( F \)) down to the scalar field \( F \) play a very special role in the analysis of vector spaces.

Definition 5.2.1. Let \( V \) be a vector space over \( F \). Then, a functional on \( V \) is a function \( f : V \to F \) that maps \( V \) to \( F \).

Linear functionals (i.e., functionals that are linear) are used to define many important concepts in abstract vector spaces. For unconstrained optimization, however, linear functionals are not interesting because they are either zero or they achieve all values in \( F \).

Definition 5.2.2. Let \( (X, \| \cdot \|) \) be a normed vector space. Then, a real functional \( f : X \to \mathbb{R} \) achieves a local minimum value at \( x_0 \in X \) if there is an \( \epsilon > 0 \) such that, for all \( x \in X \) satisfying \( \|x - x_0\| < \epsilon \), we have \( f(x) \geq f(x_0) \). If the bound holds for all \( x \in X \), then the local minimum is also a global minimum value.

Theorem 5.2.3. Let \( (X, \| \cdot \|) \) be a normed vector space and \( f : X \to \mathbb{R} \) be a real functional. If \( \delta f(x_0, h) \) exists and is negative for any \( h \in X \), then \( x_0 \) is not a local minimum value.

Proof. First, we apply Lemma 5.1.2 with the \( x \) and \( h \) for which \( \delta f(x_0, h) < 0 \). This gives a \( t_0 > 0 \) such that \( f(x_0 + th) < f(x_0) \) for all \( t \in (0, t_0) \). Thus, there can be no \( \epsilon > 0 \) satisfying the definition of a local minimum value in Definition 5.2.2. \( \square \)
5.3 Convex Functionals

Convexity is a particularly nice property of spaces and functionals that leads to well-defined minimum values.

Definition 5.3.1. Let \( V \) be a vector space, \( A \subseteq V \) be a convex set, and \( f : V \to \mathbb{R} \) be a functional. Then, a functional \( f \) is called convex on \( A \) if, for all \( a_1, a_2 \in A \) and \( \lambda \in (0, 1) \), we have

\[
f(\lambda a_1 + (1 - \lambda) a_2) \leq \lambda f(a_1) + (1 - \lambda) f(a_2).
\]

The functional is strictly convex if equality occurs only when \( a_1 = a_2 \). A functional is called (strictly) concave if \(-f\) is (strictly) convex.

Definition 5.3.2. A Banach space \( X \) is called strictly convex if the unit ball, given by \( \{ x \in X | \|x\| \leq 1 \} \), is a strictly convex set. An equivalent condition is that equality in the triangle inequality (i.e., \( \|x + y\| = \|x\| + \|y\| \)) for non-zero vectors implies that \( x = sy \) for some \( s \in F \).

Example 5.3.3. Let \((X, \| \cdot \|)\) be a normed vector space. Then, the norm \( \| \cdot \| : X \to \mathbb{R} \) is a convex functional on \( X \). Proving this is a good introductory exercise.

Example 5.3.4. Let \( X \) be an an inner-product space. For \( x, y \in X \) and \( \lambda \in (0, 1) \),

\[
\| \lambda x + (1 - \lambda)y \|^2 = \lambda^2 \|x\|^2 + 2\lambda(1 - \lambda)\text{Re}(x, y) + (1 - \lambda)^2 \|y\|^2 \\
= \lambda \|x\|^2 + (1 - \lambda) \|y\|^2 - \lambda(1 - \lambda) \|x - y\|^2 \\
\leq \lambda \|x\|^2 + (1 - \lambda) \|y\|^2,
\]

with equality iff \( x = y \). Thus, the square of the induced norm \( \| \cdot \|^2 \) is a strictly convex functional on \( X \).

Theorem 5.3.5. Let \((X, \| \cdot \|)\) be a normed vector space, \( A \subseteq X \) be a convex set, and \( f : X \to \mathbb{R} \) be a convex functional on \( A \). Then, any local minimum value of \( f \) on \( A \) is a global minimum value on \( A \). If the functional is strictly convex on \( A \) and achieves a local minimum value on \( A \), then there is a unique point \( x_0 \in A \) that achieves the global minimum value on \( A \).
5.3. CONVEX FUNCTIONALS

Proof. Let $x_0 \in A$ a point where the functional achieves a local minimum value. Proving by contradiction, we suppose that there is another point $x_1 \in A$ such that $f(x_1) < f(x_0)$. From the definition of a local minimum value, we find an $\epsilon > 0$ such that $f(x) \geq f(x_0)$ for all $x \in A$ satisfying $\|x - x_0\| < \epsilon$. Choosing $\lambda < \frac{\epsilon}{\|x_0 - x_1\|}$ in $(0,1)$ and $x = (1 - \lambda)x_0 + \lambda x_1$ implies that $\|x - x_0\| < \epsilon$ while the convexity of $f$ implies that

$$f(x) = f((1 - \lambda)x_0 + \lambda x_1) \leq (1 - \lambda)f(x_0) + \lambda f(x_1) < f(x_0).$$

This contradicts the definition of a local minimum value and implies that $f(x_0)$ is a global minimum value on $A$. If $f$ is strictly convex and $f(x_1) = f(x_0)$, then we suppose that $x_0 \neq x_1$. In this case, strict convexity implies that

$$f((1 - \lambda)x_0 + \lambda x_1) < (1 - \lambda)f(x_0) + \lambda f(x_1) = f(x_0).$$

This contradicts the fact that $f(x_0)$ is a global minimum value on $A$ and implies that $x_0 = x_1$ is unique. \qed

Theorem 5.3.6. Let $(X, \|\cdot\|)$ be a normed vector space and $f: X \to \mathbb{R}$ be a convex functional on a convex set $A \subseteq X$. If $f$ is Gâteaux differentiable at $x_0 \in A$, then

$$f(x) \geq f(x_0) + \delta f(x_0; x - x_0)$$

for all $x \in A$. If $f$ is strictly convex then the inequality is strict for $x \neq x_0$.

Proof. By the convexity of $A$ and $f$, we have $x_0 + \lambda(x - x_0) \in A$ and

$$f(x_0 + \lambda(x - x_0)) \leq f(x_0) + \lambda(f(x) - f(x_0)) \tag{5.2}$$

for all $\lambda \in (0,1)$. Also, if $f$ is strictly convex, then (5.2) strict for $x \neq x_0$. Thus,

$$f(x) \geq f(x_0) + \frac{f(x + \lambda(x - x_0)) - f(x_0)}{\lambda}$$

and taking the limit at $\lambda \downarrow 0$ completes the proof for a convex functional.

For the case where $f$ is strictly convex, we first apply the convex result to see

$$f(x_0 + \lambda(x - x_0)) \geq f(x_0) + \delta f(x_0; \lambda(x - x_0)) = f(x_0) + \lambda\delta f(x_0; x - x_0),$$

where the second step holds because $\delta f(x; h)$ is linear in $h$. This gives

$$\delta f(x_0; x - x_0) \leq \frac{f(x_0 + \lambda(x - x_0)) - f(x_0)}{\lambda} < f(x) - f(x_0),$$

where the second inequality holds because (5.2) is a strict inequality for $x \neq x_0$. \qed
Corollary 5.3.7. Let \((X, \| \cdot \|)\) be a normed vector space and \(f : X \to \mathbb{R}\) be a convex functional on a convex set \(A \subseteq X\). If \(f\) is Gâteaux differentiable at \(x_0 \in A\) and \(\delta f(x_0; x - x_0) = 0\) for all \(x \in A\), then
\[
f(x_0) = \min_{x \in A} f(x).
\]
If \(f\) is strictly convex, \(x_0\) is the unique minimizer over \(A\).

5.4 Constrained Optimization

Lagrangian optimization is an indispensable tool in engineering and physics that allows one to solve constrained non-linear optimization problems. For convex problems, there are now efficient algorithms that can handle thousands of variables and constraints. In some cases, there are also analytical techniques that allow one to derive tight bounds on optimum value. These approaches have become so common that convex Lagrangian optimization problems are now taught as a fundamental part of the graduate engineering curriculum. For simplicity, we focus on the case where the domain \(D\) is a subset of the finite-dimensional real space \(\mathbb{R}^n\).

Constrained non-linear optimization problems over \(D \subseteq \mathbb{R}^n\) can be put into the following standard form. Let \(f_i : D \to \mathbb{R}\) and \(h_j : D \to \mathbb{R}\) be a real functionals on \(D\) for \(i = 0, 1, \ldots, m\) and \(j = 1, 2, \ldots, p\). Then, the standard form is

\[
\begin{align*}
\text{minimize} & \quad f_0(x) \\
\text{subject to} & \quad f_i(x) \leq 0, \quad i = 1, 2, \ldots, m \\
& \quad h_j(x) = 0, \quad j = 1, 2, \ldots, p \\
& \quad x \in D.
\end{align*}
\]

The function \(f_0\) is called the objective function while the functions \(f_1, \ldots, f_m\) are called inequality constraints and the functions \(h_1, \ldots, h_p\) are called equality constraints.

Definition 5.4.1. A vector \(x \in D\) is feasible if it satisfies the constraints. Let \(\mathcal{F} = \{x \in D \mid f_i(x) \leq 0, i = 1, 2, \ldots, m, h_j(x) = 0, j = 1, \ldots, p\}\) be the set of feasible vectors. Then, the problem is feasible if \(\mathcal{F} \neq \emptyset\).
5.4. CONSTRAINED OPTIMIZATION

Definition 5.4.2. The optimal value is

\[ p^* = \inf_{x \in \mathcal{F}} f_0(x). \]

By convention, \( p^* \) is allowed to take infinite values and \( p^* = \infty \) if the problem is not feasible.

Evaluating the function at any feasible point automatically an upper bound because

\[ p^* \leq f_0(x) \forall x \in \mathcal{F}. \]

The optimization of a linear function with arbitrary affine equality and inequality constraints is called a linear program. Linear programs (LPs) have many equivalent forms and any linear program can be transformed into any standard form.

Definition 5.4.3. Two standard minimization forms of an LP are given by:

\[
\begin{align*}
\text{minimize} & \quad c^T x \\
\text{subject to} & \quad Ax = b \\
& \quad x \succeq 0
\end{align*}
\]

\[
\begin{align*}
\text{minimize} & \quad c^T x \\
\text{subject to} & \quad Ax \succeq b \\
& \quad x \succeq 0
\end{align*}
\]

5.4.1 The Lagrangian

The Lagrangian is used to transform constrained optimization problems into unconstrained optimization problems. One can think of it as introducing a cost \( \lambda_i \geq 0 \) associated with violating the \( i \)-th inequality constraint and a variable \( \nu_j \) used to enforce the \( j \)-th equality constraint.

Definition 5.4.4. The Lagrangian \( L: \mathcal{D} \times \mathbb{R}^m \times \mathbb{R}^p \rightarrow \mathbb{R} \) associated with optimization problem is

\[ L(x, \Lambda, \nu) = f_0(x) + \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{j=1}^{p} \nu_j h_j(x), \]

where \( \lambda_i \) is the Lagrange multiplier associated with the \( i \)-th inequality constraint and \( \nu_j \) is the Lagrange multiplier associated with the \( j \)-th equality constraint.

Definition 5.4.5. A point \( x^* \) is called locally optimal if there is an \( \epsilon_0 > 0 \) such that, for all \( \epsilon < \epsilon_0 \), it holds that \( f_0(x) \geq f_0(x^*) \) for all \( x \in \mathcal{F} \) satisfying \( \| x - x^* \| < \epsilon \).

The \( i \)-th inequality constraint is active at \( x^* \) if \( f_i(x^*) = 0 \). Otherwise, it is inactive.

Let \( A = \{ i \in \{1, \ldots, m\} \mid f_i(x^*) = 0 \} \) be the set of active constraints at \( x^* \).
Definition 5.4.6 (Mangasarian-Fromovitz). A standard constrained optimization problem satisfies the MF constraint qualification at $x^*$ if the functions $f_i$ and $h_j$ are all continuously differentiable at $x^*$ and there exists a vector $w \in \mathbb{R}^n$ satisfying $\nabla f_i(x^*)^T w < 0$ for $i \in A$ and $\nabla h_j(x^*)^T w = 0$ for $j = 1, \ldots, p$. If the constraints $h_j$ are not all affine, then one additionally needs that the vectors $\nabla h_1(x^*), \ldots, \nabla h_p(x^*) \in \mathbb{R}^n$ form a linearly independent set.

Theorem 5.4.7 (Karush-Kuhn-Tucker). If $x^*$ is a constrained local optimum that satisfies the MF constraint qualification, then there exist $\lambda^* \geq 0$ and $\nu^*$ such that

$$\nabla f_0(x^*) + \sum_{i \in A} \lambda_i^* \nabla f_i(x^*) + \sum_{j=1}^p \nu_j^* \nabla h_j(x^*) = 0. \tag{5.3}$$

This theorem provides a necessary condition for a point $x^*$ to be locally optimal for a constrained optimization problem. Before considering its proof, it is useful to discuss the geometric picture underlying its contrapositive statement: if (5.3) does not hold for all $\lambda^* \geq 0$ and $\nu^* \in \mathbb{R}^p$, then $x^*$ is not locally optimal.

Now, consider what happens if we evaluate the function at $x(t) = x^* + ty$ for some direction $y$ and a sufficiently small $t > 0$. For any continuously differentiable function $f$, the definition of the derivative implies that

$$f(x(t)) = f(x^*) + t \nabla f(x^*)^T y + o(t),$$

where $o(t) \to 0$ as $t \to 0$. If the problem is unconstrained (e.g., $m = p = 0$), then $\nabla f_0(x^*)$ must be 0. This is because the negative gradient $-\nabla f_0(x^*)$ gives the direction of steepest descent for the objective function and one is guaranteed to reduce the function by choosing $y = -\nabla f_0(x^*)$ (e.g., see Lemma 5.1.2). If there are constraints, however, then $x(t)$ may be infeasible. For the $j$-th equality constraint, the definition of the derivative implies that, for sufficiently small $t$, $x(t)$ will be infeasible if $|\nabla h_j(x^*)^T y| > 0$. Thus, we certainly need $\nabla h_j(x^*)^T y = 0$ for all $j$.

If the $i$-th inequality constraint is active (i.e., $f_i(x^*) = 0$), then the definition of the derivative implies that, for sufficiently small $t$, $x(t)$ will be infeasible if $\nabla f_i(x^*)^T y > 0$. Thus, we certainly need $\nabla f_i(x^*)^T y \leq 0$ for all $i \in A$. If the constraint is inactive (i.e., $f_i(x^*) < 0$), then due to continuity it will remain satisfied for sufficiently small $t$. 
5.4. CONSTRAINED OPTIMIZATION

Figure 5.1: A contour plot of the function \( f_0(x_1, x_2) = (x_1 - 1)^2 + (x_2 - 1)^2 - x_1x_2 / 2 \) whose minimum occurs at \((4/3, 4/3)\) (i.e., the center of the blue ellipse). The red line indicates the inequality constraint \( f_1(x_1, x_2) = 1.85 + (x_1 - 2.25)^2 / 2 - x_2 \leq 0 \). The picture shows that the constrained minimum occurs where the objective contour line is tangent to the active constraint line.

The geometric picture implied by Theorem 5.4.7 is that of a game where one would like to decrease the objective \( f_0(x^*) \) by choosing \( y \) such that \( \nabla f_0(x^*)^T y < 0 \) but there are constraints on the set of allowable \( y \)'s. Let \( H = \text{span}\{\nabla h_j(x^*)\} \) be the subspace of directions that violate the equality constraints at \( x^* \). Similarly, let the cone of directions that violate the active inequality constraints is given by

\[
F = \left\{ \sum_{i \in A} \lambda_i \nabla f_i(x^*) \mid \lambda_i \geq 0, i \in A \right\}.
\]

Thus, one can only pick directions \( y \) that are orthogonal to all vectors in \( H \) and also have a non-positive inner product with all vectors in \( F \).

Let the matrix \( P \) define the orthogonal projection of \( \mathbb{R}^n \) onto \( H^\perp \). Using this,
we can translate the equation (5.3) into the statement

\[-P \nabla f_0(x^*) \in PF\]

or “the projection, onto \(H^\perp\), of the descent direction lies in the projection, onto \(H^\perp\), of the cone of directions that violate the inequality constraints”. The reason for this is that we can absorb the \(\nabla h_j\) terms into the \(\nabla f_i\) terms by defining

\[f^{(i)} = \nabla f_i(x^*) + \sum_{j=1}^{p} \nu_{j,i} \nabla h_j(x^*) = P \nabla f_i(x^*)\]

so that \(f^{(i)} \in H^\perp\) for \(i = 0, 1, \ldots, m\). Then, the cone \(PF\) is defined by

\[PF = \left\{ \sum_{i \in A} \lambda_i f^{(i)} \middle| \lambda_i \geq 0, i \in A \right\}.

If \(-P \nabla f_0(x^*) \notin PF\), then we project \(-P \nabla f_0(x^*)\) onto \(PF\) to get a non-zero residual \(\underline{y}\). The resulting vector gives a direction where the objective function decreases linearly in \(t\) and the constraint violations are \(o(t)\). The challenge in making this proof precise is that, unless the equality constraints are affine, they may not be exactly satisfied for \(t > 0\). In standard proofs of this result, this difficulty is overcome by using the implicit function theorem to construct an \(x(t)\) that starts in the direction of \(y\) but is perturbed slightly to remain feasible.

**Proof.** For simplicity, we prove only the case where \(h_j(x) = a_j^T x - b\) is affine.

First, we define

\[\underline{y}(\lambda, \nu) = -\nabla f_0(x^*) - \sum_{i=1}^{m} \lambda_i \nabla f_i(x^*) - \sum_{j=1}^{p} \nu_j \nabla h_j(x^*) \].

The vector \(\underline{y}(\lambda, \nu)\) can be seen as the residual of the descent direction for the objective function after the constraint gradients have been used to cancel some parts.

Next, we let \(\nu^*(\lambda) = \arg \min_{\nu \in \mathbb{R}^p} \|\underline{y}(\lambda, \nu)\|\) and apply the best approximation theorem (for the standard inner product space) to see that

\[\underline{y}(\lambda, \nu^*(\lambda)) = P \underline{y}(\lambda, 0),\]

where the matrix \(P\) defines an orthogonal projection onto \(H^\perp\) and \(H = \text{span}(\{a_j\})\).

This ensures that each \(h_j(x^* + t \underline{y}(\lambda, \nu^*(\lambda))) = 0\) for all \(\lambda \in \mathbb{R}^m\) and \(t \in \mathbb{R}\).
Continuing, we let \( S = \{ \lambda \in \mathbb{R}^m \mid \lambda \geq 0, \lambda_i = 0, i \notin A \} \) and compute
\[
y^* = \arg \min_{\lambda \in S} \| y(\lambda, \nu^*(\lambda)) \|.
\]
This optimization uses the gradients of the active constraints to cancel as much of the residual descent direction as possible. Thus, \( y^* \neq 0 \) implies there is a descent direction that does not violate the constraints. Looking at the formulas for \( y(\lambda, \nu) \) and \( y(\lambda, \nu^*(\lambda)) \), we can also interpret \( y^* \) as the error vector for the projection of \( v = -P \nabla f_0(\bar{x}^*) \) onto the convex set \( PF \), which is the closed convex cone of perturbations that preserve the equality constraints but locally violate the inequality constraints. Then, \( u^* = v - y^* \) equals the projection itself and we observe that Theorem 4.6.7 implies \((u - u^*)^T(v - u^*) \leq 0\) for all \( u \in PF \). Since \( 0 \in PF \), we can choose \( u = 0 \) to see that \((u^*)^T(v - u^*) \geq 0\). Using this, we can write
\[
-(P \nabla f_0(\bar{x}^*))^T y^* = v^T(v - u^*) = (v - u^*)^T(v - u^*) + (u^*)^T(v - u^*) 
\geq \|y^*\|^2.
\]
If (5.3) cannot be satisfied by some \( \lambda \in S \) and \( \nu \in \mathbb{R}^p \), then \( y^* \neq 0 \) and \( \|y^*\| > 0 \). Thus, a perturbation in the \( y^* \) direction will decrease the value of the objective function while essentially preserving feasibility.

But, the \( y^* \) direction is only guaranteed to preserve feasibility to first order (i.e., \( (P \nabla f_i(\bar{x}^*))^T y^* \leq 0 \) for \( i = 1, \ldots, m \)). To fix this, first one needs to augment \( y^* \) with a small amount of some vector \( w \) satisfying \( (P \nabla f_i(\bar{x}^*))^T w < 0 \) for all \( i = 1, \ldots, m \). Such a vector is guaranteed by the constraint qualification. Then, we can choose some \( \delta > 0 \) such that \((P \nabla f_0(\bar{x}^*))^T(y^* + \delta w) \leq -\frac{1}{2}\|y^*\|\). With this modification, the definition of the derivative implies that, for sufficiently small \( t \), \( \bar{x}(t) = \bar{x}^* + t(y^* + \delta w) \) will be a feasible vector satisfying \( f_0(\bar{x}(t)) < f_0(\bar{x}^*) \). \( \square \)

### 5.4.2 Lagrangian Duality

**Definition 5.4.8.** The Lagrangian dual function is defined to be
\[
g(\lambda, \nu) \triangleq \inf_{x \in D} L(x, \lambda, \nu).
\]
Lemma 5.4.9. The Lagrangian dual problem

\[
\text{maximize} \quad g(\lambda, \nu) \\
\text{subject to} \quad \lambda \geq 0
\]

has a unique maximum value \( d^* \leq p^* \). This property is known as weak duality.

Proof. The Lagrangian dual function is concave because it is the pointwise infimum of affine functions

\[
g(\alpha \lambda + (1 - \alpha) \lambda', \alpha \nu + (1 - \alpha) \nu') = \inf_{x \in D} L(x, \alpha \lambda + (1 - \alpha) \lambda', \alpha \nu + (1 - \alpha) \nu') \\
= \inf_{x \in D} \left( \alpha L(x, \lambda, \nu) + (1 - \alpha) L(x, \lambda', \nu') \right) \\
\geq \inf_{x \in D} \alpha L(x, \lambda, \nu) + \inf_{x' \in D} (1 - \alpha) L(x', \lambda', \nu') \\
= \alpha g(\lambda, \nu) + (1 - \alpha) g(\lambda', \nu').
\]

Thus, it follows from Theorem 5.3.5 that \( g \) has a unique maximum value \( d^* \) which can be upper bounded by

\[
g(\lambda, \nu) = \inf_{x \in D} L(x, \lambda, \nu) \overset{(a)}{=} \inf_{x \in F} L(x, \lambda, \nu) \\
\overset{(b)}{=} p^* + \sum_{i=1}^{m} \lambda_i f_i(x) \overset{(c)}{\leq} p^*,
\]

where \((a)\) is implied by \( F \subseteq D \), \((b)\) follows from \( h_j(x) = 0 \) for \( x \in F \), and \((c)\) holds by combining \( f_i(x) \leq 0 \) for \( x \in F \) and \( \lambda_i \geq 0 \).

The Lagrangian dual function can be \(-\infty\) for a wide range of \((\lambda, \nu)\). In this case, it makes sense to eliminate these points by defining the implicit constraint set

\[
C \triangleq \{(\lambda, \nu) \in \mathbb{R}^m \times \mathbb{R}^p | \lambda \succeq 0, g(\lambda, \nu) > -\infty \}.
\]

The points \((\lambda, \nu) \in C\) are called dual feasible and it follows that

\[
d^* = \sup_{(\lambda, \nu) \in C} g(\lambda, \nu).
\]

By convention, \( d^* = -\infty \) if the dual problem is not feasible (i.e., \( C = \emptyset \)).
5.4. CONSTRAINED OPTIMIZATION

**Definition 5.4.10.** If \( d^* = p^* \), then one says **strong duality** holds for the problem.

**Theorem 5.4.11.** Let \( \bar{x}^* \) be a primal optimal point and \( (\lambda^*, \nu^*) \) be a dual optimal point. If strong duality holds, \( \bar{x}^* \in D^o \), and all \( f_i \) and \( h_j \) functions are differentiable at \( \bar{x}^* \), then we get the KKT conditions of complementary slackness, \( \lambda^*_i f_i(\bar{x}^*) = 0 \) for \( i = 1, \ldots, m \), and stationarity (5.3).

**Proof.** By weak duality, we have
\[
d^* = g(\lambda^*, \nu^*) \leq f_0(\bar{x}^*) = p^*.
\]
Since \( \bar{x}^* \) is feasible, combining \( d^* = p^* \) with the proof of weak duality shows that
\[
\inf_{x \in D} L(x, \lambda^*, \nu^*) = L(x^*, \lambda^*, \nu^*)
\]
and \( \lambda^*_i = 0 \) if the \( i \)-th inequality constraint is inactive (i.e., \( f_i(\bar{x}^*) < 0 \)). Thus, we also observe that complementary slackness condition \( \lambda^*_i f_i(\bar{x}^*) = 0 \) holds for \( i = 1, \ldots, m \). Since \( \bar{x}^* \in D^o \), it follows that \( \bar{x}^* \) is a locally optimal point of \( L(x, \lambda^*, \nu^*) \). Thus, \( \bar{x}^* \) must be a stationary point of \( L(x, \lambda^*, \nu^*) \) and taking the \( x \)-derivative gives (5.3). \[\square\]

**Example 5.4.12.** For the first LP in Definition 5.4.3 the Lagrangian is given by
\[
L(x, \lambda, \nu) = c^T x + \nu^T (b - Ax) - \lambda^T x,
\]
where the \( \lambda \) term is negative because the constraint is \( x \succeq 0 \). Thus, the Lagrangian dual function is given by
\[
g(\lambda, \nu) = \inf_{x \in D} L(x, \lambda, \nu) = \begin{cases} b^T \nu & \text{if } c - A^T \nu - \lambda = 0 \\ \infty & \text{otherwise.} \end{cases}
\]
Solving the implicit constraint and using the fact that \( \lambda \succeq 0 \), one gets the dual LP problem
\[
\begin{align*}
\text{maximize} & \quad b^T \nu \\
\text{subject to} & \quad A^T \nu \preceq c.
\end{align*}
\]
Strong duality for linear programs says that, if the original LP has an optimal solution (i.e., it is neither unbounded nor infeasible), then the dual LP has an optimal solution of the same value.
5.4.3 Convex Optimization

**Definition 5.4.13.** An optimization problem in standard form is called convex if all \( f_i \) functions are convex, all the \( h_j \) functions are affine (i.e., \( h_j(x) = a_j^T x - b_j \)), and \( D = \mathbb{R}^n \).

**Problem 5.4.14.** For a convex standard-form optimization problem (i.e., satisfying Definition 5.4.13), show that the feasible set is a convex set.

Applying Theorem 5.3.5 to this setup shows that a convex standard-form optimization problem has a unique minimum value. Also, if the function \( f_0 \) is strictly convex, then the minimum value achieved uniquely. There are a number of stronger conditions that also imply strong duality for convex optimization problems. **Slater’s condition** is stated below as a theorem and its proof can be found in [BV04, Sec. 5.3.2].

**Theorem 5.4.15 (Slater’s Condition).** If a convex optimization problem has a point \( x_0 \) where \( f_i(x_0) < 0 \) for \( i = 1, \ldots, m \) and \( h_j(x_0) = 0 \) for \( j = 1, \ldots, p \), then the MF constraint qualification and strong duality both hold for the problem. In addition, if all \( f_i \) functions are differentiable, then the KKT conditions are necessary and sufficient for optimality.

**Example 5.4.16.** For a channel with colored noise, the input distribution that maximizes the achievable information rate can be found by solving the convex optimization problem, known as water-filling, given by

\[
\begin{align*}
\text{minimize} \quad & - \sum_{i=1}^{n} \log (x_i + \alpha_i) \\
\text{subject to} \quad & \sum_{i=1}^{n} x_i = P \\
& x \succeq 0.
\end{align*}
\]

Choosing \( x_i = \frac{P}{n} \) for \( i = 1, \ldots, n \) gives a point that satisfies Slater’s condition, so strong duality holds for this problem.

**Example 5.4.17.** For the water-filling problem, the Lagrangian can be written as

\[
L(x, \lambda, \nu) = - \sum_{i=1}^{n} \log(x_i + \alpha_i) - \sum_{i=1}^{m} \lambda_i x_i + \nu \left( -P + \sum_{i=1}^{n} x_i \right)
\]
and the Lagrangian dual is given by \( g(\lambda, \nu) = \inf_{x \in \mathbb{R}^n} L(x, \lambda, \nu) \).

If \( \lambda_i < 0 \), then the Lagrangian tends to \(-\infty\) as \( x_i \to -\infty \). Thus, the system is implicitly constrained to have \( \lambda_i \geq 0 \). The first-order optimality conditions, for \( i = 1, 2, \ldots, n \), are given by

\[
-\frac{1}{x_i + \alpha_i} - \lambda_i + \nu = 0.
\]

Solving this for \( x_i \) shows that \( x_i \) is increasing in \( \lambda_i \) (for \( \lambda_i \geq 0 \)) and this implies that \( g(\lambda, \nu) \) is decreasing in \( \lambda_i \) (for \( \lambda_i \geq 0 \) and \( x_i \geq 0 \)).

Thus, the expression \( \max_{\lambda \geq 0} g(\lambda, \nu) \) is given by choosing the smallest non-negative \( \lambda_i \)'s for which \( x_i \geq 0 \). This implies that

\[
(x_i, \lambda_i) = \begin{cases} 
(\frac{1}{\nu} - \alpha_i, 0) & \text{if } \nu < \frac{1}{\alpha_i} \\
(0, \nu - \frac{1}{\alpha_i}) & \text{if } \nu \geq \frac{1}{\alpha_i}.
\end{cases}
\]

From this, the value of \( \nu \) can be determined by solving

\[
\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} \max \left\{ 0, \frac{1}{\nu} - \alpha_i \right\} = P.
\]

By strong duality, the optimal value of the dual problem equals the optimal value of the original problem. Finally, the problem can be easily solved for a range of \( P \) values by sweeping through a range of \( \nu \) values and computing \( P \) in terms of \( \nu \).
Chapter 6

Linear Transformations and Operators

6.1 The Algebra of Linear Transformations

**Theorem 6.1.1.** Let $V$ and $W$ be vector spaces over the field $F$. Let $T$ and $U$ be two linear transformations from $V$ into $W$. The function $(T + U)$ defined pointwise by

$$(T + U)(v) = Tv + Uv$$

is a linear transformation from $V$ into $W$. Furthermore, if $s \in F$, the function $(sT)$ defined by

$$(sT)(v) = s(Tv)$$

is also a linear transformation from $V$ into $W$. The set of all linear transformation from $V$ into $W$, together with the addition and scalar multiplication defined above, is a vector space over the field $F$.

**Proof.** Suppose that $T$ and $U$ are linear transformation from $V$ into $W$. For $(T + U)$ defined above, we have

$$(T + U)(sv + w) = T(sv + w) + U(sv + w)$$

$$= s(Tv) + Tw + s(Uv) + Uw$$

$$= s(Tv + Uv) + (Tv + Tw)$$

$$= s((T + U)v) + (T + U)w,$$
which shows that \((T + U)\) is a linear transformation. Similarly, we have

\[
(rT) (sv + w) = r (T (sv + w)) \\
= r (s (Tv) + (Tw)) \\
= rs (Tv) + r (Tw) \\
= s (r (Tv)) + rT (w) \\
= s ((rT) v) + (rT) w
\]

which shows that \((rT)\) is a linear transformation.

To verify that the set of linear transformations from \(V\) into \(W\) together with the operations defined above is a vector space, one must directly check the conditions of Definition 3.3.1. These are straightforward to verify, and we leave this exercise to the reader.

We denote the space of linear transformations from \(V\) into \(W\) by \(L(V, W)\). Note that \(L(V, W)\) is defined only when \(V\) and \(W\) are vector spaces over the same field.

**Fact 6.1.2.** Let \(V\) be an \(n\)-dimensional vector space over the field \(F\), and let \(W\) be an \(m\)-dimensional vector space over \(F\). Then the space \(L(V, W)\) is finite-dimensional and has dimension \(mn\).

**Theorem 6.1.3.** Let \(V\), \(W\), and \(Z\) be vector spaces over a field \(F\). Let \(T \in L(V, W)\) and \(U \in L(W, Z)\). Then the composed function \(UT\) defined by \((UT) (v) = U (T (v))\) is a linear transformation from \(V\) into \(Z\).

**Proof.** Let \(v_1, v_2 \in V\) and \(s \in F\). Then, we have

\[
(UT) (sv_1 + v_2) = U (T (sv_1 + v_2)) \\
= U (sTv_1 + Tv_2) \\
= sU (Tv_1) + U (Tv_2) \\
= s(UT) (v_1) + (UT) (v_2),
\]

as desired.

**Definition 6.1.4.** If \(V\) is a vector space over the field \(F\), a **linear operator** on \(V\) is a linear transformation from \(V\) into \(V\).
Definition 6.1.5. An **algebra** over a field \( F \) is a vector space \( V \) over \( F \) that has a bilinear vector product \( \cdot : V \times V \to V \) satisfying \((su) \cdot (tv) = (st)(u \cdot v)\) and 
\[
(su + v) \cdot (tw + x) = st(u \cdot w) + s(u \cdot x) + t(v \cdot w) + (v \cdot x),
\]
for all \( s, t \in F \) and \( u, v, w, x \in V \). If \( V \) is a Banach space and the norm of the vector product satisfies \( \|u \cdot v\| \leq \|u\|\|v\| \), then it is called a **Banach algebra**.

Example 6.1.6. The set \( L(V, V) \) of linear operators on \( V \) forms an algebra when the vector product is defined by functional composition \( UT(v) = U(T(v)) \). If \( V \) is a Banach space and \( L(V, V) \) is equipped with the induced operator norm, then it forms a Banach algebra.

Definition 6.1.7. A linear transformation \( T \) from \( V \) into \( W \) is called **invertible** if there exists a function \( U \) from \( W \) to \( V \) such that \( UT \) is the identity function on \( V \) and \( TU \) is the identity function on \( W \). If \( T \) is invertible, the function \( U \) is unique and is denoted by \( T^{-1} \). Furthermore, \( T \) is invertible if and only if

1. \( T \) is one-to-one: \( T v_1 = T v_2 \implies v_1 = v_2 \)
2. \( T \) is onto: the range of \( T \) is \( W \).

Example 6.1.8. Consider the vector space \( V \) of semi-infinite real sequences \( \mathbb{R}^\omega \) where \( \underline{v} = (v_1, v_2, v_3, \ldots) \in V \) with \( v_n \in \mathbb{R} \) for \( n \in \mathbb{N} \). Let \( L : V \to V \) be the left-shift linear transformation defined by
\[
L \underline{v} = (v_2, v_3, v_4, \ldots)
\]
and \( R : V \to V \) be the right-shift linear transformation defined by
\[
R \underline{v} = (0, v_1, v_2, \ldots).
\]
Notice that \( L \) is onto but not one-to-one and \( R \) is one-to-one but not onto. Therefore, neither transformation is invertible.

Example 6.1.9. Consider the normed vector space \( V \) of semi-infinite real sequences \( \mathbb{R}^\omega \) with the standard Schauder basis \( \{e_1, e_2, \ldots\} \). Let \( T : V \to V \) be the linear transformation that satisfies \( T e_i = i^{-1}e_i \) for \( i = 1, 2, \ldots \). Let the linear transformation \( U : V \to V \) satisfy \( U e_i = i e_i \) for \( i = 1, 2, \ldots \). It is easy to verify that \( U = T^{-1} \) and \( UT = TU = I \).
This example should actually bother you somewhat. Since $T$ reduces vector components arbitrarily, its inverse must enlarge them arbitrarily. Clearly, this is not a desirable property. Later, we will introduce a norm for linear transforms which quantifies this problem.

**Theorem 6.1.10.** Let $V$ and $W$ be vector spaces over the field $F$ and let $T$ be a linear transformation from $V$ into $W$. If $T$ is invertible, then the inverse function $T^{-1}$ is a linear transformation from $W$ onto $V$.

**Proof.** Let $w_1$ and $w_2$ be vectors in $W$ and let $s \in F$. Define $v_j = T^{-1}w_j$, for $j = 1, 2$. Since $T$ is a linear transformation, we have

$$T(sv_1 + v_2) = sT(v_1) + T(v_2) = sw_1 + w_2.$$ 

That is, $sv_1 + v_2$ is the unique vector in $V$ that maps to $sw_1 + w_2$ under $T$. It follows that

$$T^{-1}(sw_1 + w_2) = sv_1 + v_2 = s(T^{-1}w_1) + T^{-1}w_2$$

and $T^{-1}$ is a linear transformation. 

A **homomorphism** is a mapping between algebraic structures which preserves all relevant structure. An **isomorphism** is a homomorphism which is also invertible. For vector spaces, the relevant structure is given by vector addition and scalar multiplication. Since a linear transformation preserves both of these operation, it is also a vector space homomorphism. Likewise, an invertible linear transformation is a vector space isomorphism.

## 6.2 The Dual Space

**Definition 6.2.1.** Let $V$ be a vector space. The collection of all linear functionals on $V$, denoted $L(V, F)$, forms a vector space. We also denote this space by $V^*$ and call it the **dual space** of $V$.

The following theorem shows that, if $V$ is finite dimensional, then

$$\dim V^* = \dim V.$$ 

In this case, one actually finds that $V$ is isomorphic to $V^*$. Therefore, the two spaces can be identified with each other so that $V = V^*$ for finite dimensional $V$. 
6.2. THE DUAL SPACE

Theorem 6.2.2. Let $V$ be a finite-dimensional vector space over the field $F$, and let $B = v_1, \ldots, v_n$ be a basis for $V$. There is a unique dual basis $B^* = f_1, \ldots, f_n$ for $V^*$ such that $f_j(v_i) = \delta_{ij}$. For each linear functional on $V$, we have

$$f = \sum_{i=1}^{n} f(v_i) f_i,$$

and for each vector $v$ in $V$, we have

$$v = \sum_{i=1}^{n} f_i(v) v_i.$$

Proof. Let $B = v_1, \ldots, v_n$ be a basis for $V$. According to Theorem 3.4.7, there is a unique linear functional $f_i$ on $V$ such that $f_i(v_j) = \delta_{ij}$.

Thus, we obtain from $B$ a set of $n$ distinct linear functionals $f_1, \ldots, f_n$ on $V$. These functionals are linearly independent; suppose that

$$f = \sum_{i=1}^{n} s_i f_i,$$

then

$$f(v_j) = \sum_{i=1}^{n} s_i f_i(v_j) = \sum_{i=1}^{n} s_i \delta_{ij} = s_j.$$

In particular, if $f$ is the zero functional, $f(v_j) = 0$ for $j = 1, \ldots, n$ and hence the scalars $\{s_j\}$ must all equal 0. It follows that the functionals $f_1, \ldots, f_n$ are linearly independent. Since $\dim V^* = n$, we conclude that $B^* = f_1, \ldots, f_n$ forms a basis for $V^*$, the dual basis of $B$.

Next, we want to show that there is a unique basis which is dual to $B$. If $f$ is a linear functional on $V$, then $f$ is some linear combination of $f_1, \ldots, f_n$ with

$$f = \sum_{i=1}^{n} s_i f_i.$$

Furthermore, by construction, we must have $s_j = f(v_j)$ for $j = 1, \ldots, n$. Similarly, if

$$v = \sum_{i=1}^{n} t_i v_i,$$

then $v_i$ is a basis for $V$. Therefore, $B = v_1, \ldots, v_n$ is a basis for $V$. Since $\dim V = n$, we conclude that $B$ is a basis for $V$. Thus, there is a unique linear functional $f_i$ on $V$ such that $f_i(v_j) = \delta_{ij}$. For each linear functional on $V$, we have

$$f = \sum_{i=1}^{n} f(v_i) f_i,$$

and for each vector $v$ in $V$, we have

$$v = \sum_{i=1}^{n} f_i(v) v_i.$$
is a vector in $V$, then

$$f_j (v) = \sum_{i=1}^{n} t_i f_j (v_i) = \sum_{i=1}^{n} t_i \delta_{ij} = t_j.$$ 

That is, the unique expression for $v$ as a linear combination of $v_1, \ldots, v_n$ is

$$v = \sum_{i=1}^{n} f_i (v) v_i.$$ 

One important use of the dual space is to define the transpose of a linear transform in a way that generalizes to infinite dimensional vector spaces. Let $V, W$ be vector spaces over $F$ and $T: V \to W$ be a linear transform. If $g \in W^*$ is a linear functional on $W$ (i.e., $g: W \to F$), then $g(Tv) \in V^*$ is a linear functional on $V$. The transpose of $T$ is the mapping $U: W^* \to V^*$ defined by $f(v) = g(Tv) \in V^*$ for all $g \in W^*$. If $V, W$ are finite-dimensional, then one can identify $V = V^*$ and $W = W^*$ via isomorphism and recover the standard transpose mapping $U: W \to V$ implied by the matrix transpose.

The details of this definition are not used in the remainder of these notes, but can be useful in understanding the subtleties of infinite dimensional spaces. For infinite dimensional Hilbert spaces, we will see later that the definition again simplifies because one identify $V = V^*$ via isomorphism. The interesting case that does not simplify is that of linear transforms between infinite dimensional Banach spaces.

### 6.3 Operator Norms

For any vector space of linear transforms, one can define a norm to get a normed vector space of linear transforms (e.g., consider the Frobenius norm of a matrix). In constrast, an operator norm is defined for linear transforms between normed spaces and it is induced by the vector norms of the underlying spaces. Intuitively, the induced operator norm is the largest factor by which a linear transform can increase the length of a vector. This defines a simple “worst-case” expansion for any linear transform.
Definition 6.3.1. Let $V$ and $W$ be two normed vector spaces and let $T : V \to W$ be a linear transformation. The induced operator norm of $T$ is defined to

$$\|T\| = \sup_{v \in V \setminus \{0\}} \frac{\|Tv\|}{\|v\|} = \sup_{v \in V, \|v\|=1} \|Tv\|.$$ 

A common question about the operator norm is, “How do I know the two expressions give the same result?” To see this, we can write

$$\sup_{v \in V \setminus \{0\}} \frac{\|Tv\|}{\|v\|} = \sup_{v \in V, \|v\|=1} T \frac{v}{\|v\|} = \sup_{u \in V, \|u\|=1} \|Tu\|.$$ 

Previously, we have seen that the set $L(V, W)$ of linear transformations from $V$ into $W$, with the standard addition and scalar multiplication, satisfies the conditions required to be a vector space. Now, we have a norm for that vector space. Interested readers should verify that the above definition satisfies the first two standard conditions required by a norm. To verify the triangle inequality, we can write

$$\|T + U\| = \sup_{v \in V, \|v\|=1} \| (T + U)v \| \leq \sup_{v \in V, \|v\|=1} (\|Tv\| + \|Uv\|) \leq \sup_{v \in V, \|v\|=1} \|Tv\| + \sup_{v \in V, \|v\|=1} \|Uv\| = \|T\| + \|U\|.$$ 

The induced operator norm also has another property that follows naturally from its definition. Notice that

$$\|T\| = \sup_{u \in V \setminus \{0\}} \frac{\|Tu\|}{\|u\|} \geq \frac{\|Tu\|}{\|u\|}$$

for all non-zero $u \in V$. Checking the special case of $u = 0$ separately, one can show the induced operator-norm inequality $\|Tu\| \leq \|T\|\|u\|$ for all $u \in V$.

For the space $L(V, V)$ of linear operators on $V$, a norm is called submultiplicative if $\|TU\| \leq \|T\|\|U\|$ for all $T, U \in L(V, V)$. The induced operator-norm inequality shows that all induced operator norms are submultiplicative because

$$\|UTv\| \leq \|U\| \|Tv\| \leq \|U\| \|T\| \|v\|.$$ 

This also defines a submultiplicative norm for the algebra of linear operators on $V$. 
6.3.1 Bounded Transformations

Definition 6.3.2. A linear transformation is called bounded if its induced operator norm is finite.

Theorem 6.3.3. A linear transformation $T : V \to W$ is bounded if and only if it is continuous.

Proof. Suppose that $T$ is bounded; that is, there exists $M$ such that $\|T\psi\| \leq M \|\psi\|$ for all $\psi \in V$. Let $\psi_1, \psi_2, \ldots$ be a convergent sequence in $V$, then

$$\|T\psi_i - T\psi_j\| = \|T(\psi_i - \psi_j)\| \leq M \|\psi_i - \psi_j\|.$$ 

This implies that $T\psi_1, T\psi_2, \ldots$ is a convergent sequence in $W$, and $T$ is continuous.

Conversely, assume $T$ is continuous and notice that $T0 = 0$. Therefore, for any $\epsilon > 0$, there is a $\delta > 0$ such that $\|T\psi\| < \epsilon$ for all $\|\psi\| < \delta$. Since the norm of $\psi = \frac{\delta \psi}{2\|\psi\|}$ is equal to $\frac{\delta}{2}$, we get

$$\|T\psi\| = \left\| T \frac{\delta \psi}{2\|\psi\|} \right\| \frac{2\|\psi\|}{\delta} < \frac{2\epsilon}{\delta} \|\psi\|.$$ 

The value $M = \frac{2\epsilon}{\delta}$ serves as an upper bound on $\|T\|$.

Then, by showing that linear transformations over finite-dimensional spaces are continuous, one concludes that they are also bounded. This is accomplished in the following theorem.

Theorem 6.3.4. Let $V$ and $W$ be normed vector spaces and let $T : V \to W$ be a linear transformation. If $V$ is finite dimensional, then $T$ is continuous and bounded.

Lemma 6.3.5. Let $V$ be a finite-dimensional normed vector space, and let

$$\mathcal{B} = \psi_1, \ldots, \psi_n$$

be a basis for $V$. Then, for $\psi \in V$, each coefficient $s_i$ in the expansion

$$\psi = s_1\psi_1 + \cdots + s_n\psi_n$$

is a continuous linear function of $\psi$. Being continuous, it is also bounded, so there exists a constant $M$ such that $|s_i| \leq M \|\psi\|$.
6.3. OPERATOR NORMS

Proof of Lemma. The linearity property is straightforward, its proof is omitted. It will suffice to show that there is an \( m > 0 \) such that

\[
m |s_i| \leq m (|s_1| + \cdots + |s_n|) \leq \|v\|,
\]

since (6.1) implies that \( |s_i| \leq m^{-1} \|v\| \). We first show that this holds for coefficients \( \{s_1, \ldots, s_n\} \) satisfying the condition \( |s_1| + \cdots + |s_n| = 1 \). Let

\[
S = \left\{ (s_1, \ldots, s_n) \middle| \sum_{i=1}^{n} |s_i| = 1 \right\}.
\]

This set is closed and bounded; it is therefore compact. Define the function \( f : S \to \mathbb{R} \) by

\[
f(s_1, \ldots, s_n) = \|s_1v_1 + \cdots + s_nv_n\|.
\]

It can be shown that \( f \) is continuous, and it is clear that \( f > 0 \) over \( S \). Let

\[
m = \min_{(s_1, \ldots, s_n) \in S} f(s_1, \ldots, s_n).
\]

Since \( f \) is continuous and \( S \) is compact, this minimum exists and is attained by some point \( (s'_1, \ldots, s'_n) \in S \). Note that \( m > 0 \) for otherwise \( v_1, \ldots, v_n \) are linearly dependent, contradicting the fact that \( B \) is a basis. Thus \( m \) so defined satisfies (6.1).

For general sets of coefficients \( \{s_i\} \), let \( c = |s_1| + \cdots + |s_n| \). If \( c = 0 \), the result is trivial. If \( c > 0 \), then write

\[
\|s_1v_1 + \cdots + s_nv_n\| = \frac{s_1}{c}v_1 + \cdots + \frac{s_n}{c}v_n\right\| \| = cf \left( \frac{s_1}{c}, \ldots, \frac{s_n}{c} \right) \geq cm = m (|s_1| + \cdots + |s_n|).
\]

This is the desired result. \( \Box \)

We are now ready to prove the theorem.

Proof of Theorem. Let \( B = v_1, \ldots, v_n \) be a basis for \( V \). Let \( v \in V \) be expressed in terms of this basis as

\[
v = s_1v_1 + \cdots + s_nv_n.
\]
Let $C = \max_{1 \leq i \leq n} \|T_{v_i}\|$. Then,
\[
\|T_v\| = \|T( s_1 v_1 + \cdots + s_n v_n)\|
\leq |s_1| \|T v_1\| + \cdots + |s_n| \|T v_n\|
\leq C (|s_1| + \cdots + |s_n|).
\]
By the previous lemma, this implies that there exists an $M$ such that $|s_1| + \cdots + |s_n| \leq M \|v\|$, so that
\[
\|T v\| \leq C M \|v\|.
\]

6.3.2 The Neumann Expansion

**Theorem 6.3.6.** Let $\| \cdot \|$ be a submultiplicative operator norm and $T : V \to V$ be a linear operator with $\|T\| < 1$. Then, $(I - T)^{-1}$ exists and
\[
(I - T)^{-1} = \sum_{i=0}^{\infty} T^i.
\]

**Proof.** First, we observe that the sequence
\[ A_n = \sum_{i=0}^{n-1} T^i. \]
is Cauchy. This follows from the fact that, for $m < n$, we have
\[
\|A_n - A_m\| = \left\|\sum_{i=m}^{n-1} T^i\right\| \leq \sum_{i=m}^{n-1} \|T\|^i = \frac{\|T\|^m - \|T\|^n}{1 - \|T\|} \leq \frac{\|T\|^m}{1 - \|T\|}.
\]
Since this goes to zero as $m \to \infty$, we see that the limit $\lim_{n \to \infty} A_n$ exists.

Next, we observe that
\[
(I - T) (I + T + T^2 + \cdots + T^{n-1}) = I - T^n.
\]
Since $\|T\| < 1$, we have $\lim_{k \to \infty} T^k = 0$ because $\|T^k\| \leq \|T\|^k \to 0$. Taking the limit $n \to \infty$ of both sides gives
\[
(I - T) \sum_{i=0}^{\infty} T^i = \lim_{n \to \infty} (I - T^n) = I.
\]

Likewise, reversing the order multiplication results in the same result. This shows that $\sum_{i=0}^{\infty} T^i$ must be the inverse of $I - T$. \qed
If one only needs to show that \( I - T \) is non-singular, then proof by contradiction is somewhat simpler. Suppose \( I - T \) is singular, then there exists a non-zero vector \( \mathbf{v} \) such that \( (I - T) \mathbf{v} = 0 \). But, this implies that \( \|\mathbf{v}\| = \|T \mathbf{v}\| \leq \|T\| \|\mathbf{v}\| \). Since \( \|\mathbf{v}\| \neq 0 \), this gives the contradiction \( \|T\| \geq 1 \) and implies that \( I - T \) is non-singular.

### 6.3.3 Matrix Norms

\[
\|A\|_\infty = \max_{\|\mathbf{v}\|_\infty = 1} \|Av\|_\infty = \max_i \sum_j |a_{ij}|
\]

\[
\|A\|_1 = \max_{\|\mathbf{v}\|_1 = 1} \|Av\|_1 = \max_j \sum_i |a_{ij}|
\]

The 2-norm of a matrix can be found by solving

\[
\max_{\|\mathbf{v}\|_2 = 1} \|Av\|_2^2 = \mathbf{v}^H A^H A \mathbf{v}.
\]

Using the Lagrange multiplier technique, one seeks to minimize

\[
J = \mathbf{v}^H A^H A \mathbf{v} - \lambda \mathbf{v}^H \mathbf{v}.
\]

Taking the gradient with respect to \( \mathbf{v} \) and equating the result to zero, we get

\[
A^H A \mathbf{v} = \lambda \mathbf{v}.
\]

The corresponding \( \mathbf{v} \) must be an eigenvector of the matrix \( A^H A \). Left multiplying this equation by \( \mathbf{v}^H \) and using the fact that \( \mathbf{v}^H \mathbf{v} = 1 \), we obtain

\[
\mathbf{v}^H A^H A \mathbf{v} = \lambda \mathbf{v}^H \mathbf{v} = \lambda.
\]

Since we are maximizing the left hand side of this equation, \( \lambda \) must be the largest eigenvalue of \( A^H A \). For an \( n \times n \) matrix \( B \) with eigenvalues \( \lambda_1, \ldots, \lambda_n \), the **spectral radius** \( \rho(B) \) is defined by

\[
\rho(B) = \max_i |\lambda_i|.
\]

The spectral radius of \( B \) is the smallest radius of a circle centered at the origin that contains all the eigenvalues of \( B \). It follows that

\[
\|A\|_2 = \sqrt{\rho(A^H A)}.
\]

When \( A \) is Hermitian, \( \|A\|_2 = \rho(A) \). The 2-norm is also called the **spectral norm**.
The Frobenius norm is given by
\[
\|A\|_F = \left( \sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}|^2 \right)^{\frac{1}{2}}.
\]
This norm is also called the Euclidean norm. Note that \(\|A\|^2_F = \text{tr}(A^HA)\).

### 6.4 Linear Functionals on Hilbert Spaces

Let \(V\) be an inner-product space, and let \(v\) be some fixed vector in \(V\). Define the function \(f_v\) from \(V\) into \(F\) by
\[
f_v(w) = \langle w, v \rangle.
\]
Clearly, \(f_v\) is a linear functional on \(V\). If \(V\) is a Hilbert space, then every continuous linear functional on \(V\) arises in this way from some vector \(v\). This result is known as the Riesz representation theorem.

**Lemma 6.4.1.** If \(\langle v, w \rangle = \langle u, w \rangle\) for all \(w \in V\), then \(v = u\).

**Proof.** Then, \(\langle v - u, w \rangle = 0\) for all \(w \in V\). Therefore, \(\langle v - u, v - u \rangle = 0\) and this implies \(v - u = 0\). \(\square\)

**Theorem 6.4.2 (Riesz).** Let \(V\) be a Hilbert space and \(f\) be a continuous linear functional on \(V\). Then, there exists a unique vector \(v \in V\) such that \(f(w) = \langle w, v \rangle\) for all \(w \in V\).

**Proof.** While the result holds in any Hilbert space, this proof assumes \(V\) is separable for simplicity. Therefore, we let \(v_1, v_2, \ldots\) be a countable orthonormal basis for \(V\). We wish to find a candidate vector \(v\) for the inner product.

First, we note that \(f\) is bounded because it is continuous and, as such, there exists \(M\) such that \(|f(x)| \leq M\|x\|\) for all \(x \in V\). Let \(x_n = \sum_{i=1}^{n} f(v_i)v_i\). For any \(n\), we have
\[
M\|x_n\| \geq |f(x_n)| = \left| \sum_{i=1}^{n} f(v_i)f(v_i) \right| = \sum_{i=1}^{n} |f(v_i)|^2 = \sum_{i=1}^{n} f(v_i)^2 = \sum_{i=1}^{n} f(v_i)^2.
\]

\[
= \sum_{i=1}^{n} \langle f(v_i)v_i, f(v_i)v_i \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \langle f(v_i)v_j, f(v_i)v_i \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \langle f(v_i)v_j, f(v_i)v_i \rangle = \langle x_n, x_n \rangle = \|x_n\|^2.
\]
This implies that $\|x_n\| \leq M$ for all $n$. Hence, $\lim_{n \to \infty} \sum_{i=1}^{n} |f(v_i)|^2$ is bounded and the vector

$$v = \sum_{i=1}^{\infty} f(v_i)v_i,$$

is in $V$ because it is the limit point of a Cauchy sequence. Let $f_v$ be the functional defined by

$$f_v(w) = \langle w, v \rangle.$$

By the Cauchy-Schwarz, we can verify that

$$\|f_v\| \triangleq \sup_{u \in V - \{0\}} \frac{f_v(u)}{\|u\|} = \|v\|.$$

Since $f$ is continuous, it follows that $\|f\| < \infty$ and $\|v\| < \infty$. Then,

$$f_v(v_j) = \left( v_j, \sum_{i=1}^{\infty} f(v_i)v_i \right) = f(v_j).$$

Since this is true for each $v_j$, it follows that $f = f_v$. Now, consider any $v' \in V$ such that $\langle w, v \rangle = \langle w, v' \rangle$ for all $w \in W$. Applying Lemma 6.4.1 shows that $v = v'$ and we conclude that $v$ is unique.

An important consequence of this theorem is that the continuous dual space $V^*$ of a Hilbert space $V$ is isometrically isomorphic to the original space $V$. Let $R: V^* \to V$ be the implied Riesz mapping from continuous linear functionals on $V$ (i.e., $V^*$) to elements of $V$. Then, $f(v) = \langle v, R(f) \rangle$ for all $f \in V^*$. The isomorphism can be shown by verifying that $R(sf_1 + f_2) = \overline{s}R(f_1) + R(f_2)$ and one finds that the mapping $R$ is conjugate linear. The mapping is isometric because $\|f\| = \|R(f)\|$. Based on this isomorphism, one can treat a Hilbert space as self-dual and assume without confusion that $V = V^*$.

**Theorem 6.4.3.** Let $V$ and $W$ be Hilbert spaces, and assume $T: V \to W$ is a continuous linear transformation. Then, the adjoint is the unique linear transformation $T^*$ on $W$ such that

$$\langle Tw, w \rangle = \langle v, T^*w \rangle$$

for all vectors $v \in V$, $w \in W$. 

Proof. Let \( w \) be any vector in \( W \). Then \( f(v) = \langle Tv, w \rangle \) is a continuous linear functional on \( V \). It follows from the Riesz representation theorem (Theorem 6.4.2) that there exists a unique vector \( v' \in V \) such that \( f(v) = \langle Tv, w \rangle = \langle v, v' \rangle \). Of course, the vector \( v' \) depends on the choice of \( w \). So, we define the adjoint mapping \( T^* : W \to V \) to give the required \( v' \) for each \( w \). In other words,

\[
v' = T^*w.
\]

Next, we must verify that \( T^* \) is a linear transformation. Let \( w_1, w_2 \) be in \( W \) and \( s \) be a scalar. For all \( v \in V \),

\[
\langle v, T^*(sw_1 + w_2) \rangle = \langle T_v, (sw_1 + w_2) \rangle
= \overline{s} \langle T_v, w_1 \rangle + \langle T_v, w_2 \rangle
= s \langle v, T^*w_1 \rangle + \langle v, T^*w_2 \rangle
= \langle v, sT^*w_1 \rangle + \langle v, T^*w_2 \rangle
= \langle v, sT^*w_1 + T^*w_2 \rangle.
\]

Since this holds for all \( v \in V \), we gather from Lemma 6.4.1 that \( T^*(sv_1 + v_2) = sT^*v_1 + T^*v_2 \). Therefore, \( T^* \) is linear. The uniqueness of \( T^* \) is inherited from Theorem 6.4.2 because, for each \( w \in W \), the vector \( T^*w \) is determined uniquely as the vector \( v' \) such that \( \langle Tv, w \rangle = \langle v, v' \rangle \) for all \( v \in V \).

**Theorem 6.4.4.** Let \( V \) be a finite-dimensional inner-product space and let

\[
B = \{v_1, \ldots, v_n\}
\]

be an orthonormal basis for \( V \). Let \( T \) be a linear operator on \( V \) and let \( A \) be the matrix representation of \( T \) in the ordered basis \( B \). Then \( A_{kj} = \langle Tv_j, v_k \rangle \).

Proof. Since \( B \) is an orthonormal basis, we have

\[
v = \sum_{k=1}^{n} \langle v, v_k \rangle v_k.
\]

The matrix \( A \) is defined by

\[
Tv_j = \sum_{k=1}^{n} A_{kj} v_k
\]

and since

\[
Tv_j = \sum_{k=1}^{n} \langle Tv_j, v_k \rangle v_k,
\]

we conclude that \( A_{kj} = \langle Tv_j, v_k \rangle \).
6.5. FUNDAMENTAL SUBSPACES

**Corollary 6.4.5.** Let $V$ be a finite-dimensional inner-product space, and let $T$ be a linear operator on $V$. In any orthonormal basis for $V$, the matrix for $T^*$ is the conjugate transpose of the matrix of $T$.

*Proof.* Let $\mathcal{B} = v_1, \ldots, v_n$ be an orthonormal basis for $V$, let $A = [T]_\mathcal{B}$ and $B = [T^*]_\mathcal{B}$. According to the previous theorem,

$$A_{kj} = \langle T v_j, v_k \rangle$$
$$B_{kj} = \langle T^* v_j, v_k \rangle$$

By the definition of $T^*$, we then have

$$B_{kj} = \langle T^* v_j, v_k \rangle = \langle v_k, T^* v_j \rangle = \langle T v_k, v_j \rangle = A_{jk}.$$

We note here that every linear operator on a finite-dimensional inner-product space $V$ has an adjoint on $V$. However, in the infinite-dimensional case this is not necessarily true. In any case, there exists at most one such operator $T^*$.

### 6.5 Fundamental Subspaces

There are four fundamental subspaces of a linear transformation $T : V \to W$ when $V$ and $W$ are Hilbert spaces. We have already encountered two such spaces: The range of $T$ and the nullspace of $T$. Recall that the range of a linear transformation $T$ is the set of all vectors $w \in W$ such that $w = T v$ for some $v \in V$. The nullspace of $T$ consists of all vectors $v \in V$ such that $T v = 0$.

The other two fundamental subspaces of $T$ are the **range of the adjoint** $T^*$, denoted $R_{T^*}$ and the **nullspace of the adjoint** $T^*$, denoted $N_{T^*}$. The various subspaces of the transformation $T : V \to W$ can be summarized as follows,

$$R_T \subseteq W$$
$$N_T \subseteq V$$
$$R_{T^*} \subseteq V$$
$$N_{T^*} \subseteq W.$$
Theorem 6.5.1. Let $V$ and $W$ be Hilbert spaces and $T : V \to W$ be a bounded linear transformation from $V$ to $W$ such that $R_T$ and $R_{T^*}$ are both closed. Then,

1. the range $R_T$ is the orthogonal complement of $N_{T^*}$, i.e., $[R_T]^\bot = N_{T^*}$;

2. the nullspace $N_T$ is the orthogonal complement of $R_{T^*}$, i.e., $[R_{T^*}]^\bot = N_T$.

Complementing these equalities, we get

\[
R_T = R_T = [N_T]^\bot \\
R_{T^*} = R_{T^*} = [N_T]^\bot.
\]

Proof. Let $w \in R_T$, then there exists $v \in V$ such that $Tv = w$. Assume that $n \in N_{T^*}$, then

\[
\langle w, n \rangle = \langle Tv, n \rangle = \langle v, T^*n \rangle = 0.
\]

That is, $w$ and $n$ are orthogonal vectors. It follows that $N_{T^*} \subseteq [R_T]^\bot$. Now, let $w \in [R_T]^\bot$. Then, for every $v \in V$, we have

\[
\langle Tv, w \rangle = 0.
\]

This implies that $\langle v, T^*w \rangle = 0$, by the definition of the adjoint. Since this is true for every $v \in V$, we get $T^*w = 0$, so $w \in N_{T^*}$. Then $[R_T]^\bot \subseteq N_{T^*}$, which combined with our previous result yields $[R_T]^\bot = N_{T^*}$. Using a similar argument, one can show that $[R_{T^*}]^\bot = N_T$.

\[\square\]

6.6 Pseudoinverses

Theorem 6.6.1. Let $V$ and $W$ be Hilbert spaces and $T$ be a bounded linear transformation from $V$ to $W$ where $R_T$ is closed. The equation $Tv = w$ has a solution if and only if $\langle w, u \rangle = 0$ for every vector $u \in N_{T^*}$, i.e.,

\[
w \in R_T \iff w \perp N_{T^*}.
\]

In matrix notation, $Av = w$ has a solution if and only if $u^Hw = 0$ for every vector $u$ such that $A^Hu = 0$. 

In matrix notation,
Proof. Assume that $Tv = w$, and let $u \in N_{T^*}$. Since $T$ is bounded, the adjoint $T^*$ exists and

$$\langle w, u \rangle = \langle Tv, u \rangle = \langle v, T^*u \rangle = \langle v, 0 \rangle = 0.$$ 

To prove the reverse implication, suppose that $\langle w, u \rangle = 0$ when $u \in N_{T^*}$ and $Tv = w$ has no solution. Since $w \notin R_T$ and $R_T$ is closed, it follows that

$$w_o = w - P_{R_T}w = w - w_r \neq 0.$$ 

But

$$\langle w, w_o \rangle = \langle w_r + w_o, w_o \rangle = \langle w_o, w_o \rangle > 0,$$

which contradicts the assumption that $\langle w, u \rangle = 0$ when $u \in N_{T^*}$. We must conclude that $Tv = w$ has a solution. \hfill \Box

**Fact 6.6.2.** The solution to $Tv = w$ (if it exists) is unique if and only if the only solution to $Tv = 0$ is $v = 0$. That is, if $N_T = \{0\}$.

### 6.6.1 Least Squares

Let $T: V \to W$ be a bounded linear transformation. If the equation $Tv = w$ has no solution, then we can find a vector $v$ that minimizes

$$\|Tv - w\|^2.$$ 

**Theorem 6.6.3.** The vector $v \in V$ minimizes $\|Tv - w\|$ if and only if

$$T^*Tv = T^*w.$$ 

**Proof.** Minimizing $\|w - T\hat{v}\|$ is equivalent to minimizing $\|w - \hat{w}\|$, where $\hat{w} = Tv \in R_T$. By the projection theorem, we must have

$$w - \hat{w} \in [R_T]^\perp.$$ 

But this is equivalent to

$$w - \hat{w} \in N_{T^*}.$$ 

That is, $T^*(w - \hat{w}) = 0$, or equivalently $T^*w = T^*\hat{w}$. Conversely, if $T^*Tv = T^*w$, then

$$T^*(Tv - w) = 0,$$

so that $Tv - w \in N_{T^*}$. Hence, the error is orthogonal to the subspace $R_T$ and has minimal length by the projection theorem. \hfill \Box
Corollary 6.6.4. If $A$ is a matrix such that $A^H A$ is invertible, then the least-squares solution to $Av = w$ is

$$v = (A^H A)^{-1} A^H w.$$  

The matrix $(A^H A)^{-1} A^H$ is the left inverse of $A$ and is an example of a Moore-Penrose pseudoinverse.

Theorem 6.6.5. Suppose the vector $\hat{\nu} \in V$ minimizes $\|v\|$ over all $v \in V$ satisfying $Tv = w$. Then, $\hat{\nu} \in [N_T]^\perp$ and, if $R_T^*$ is closed, $\hat{\nu} = T^* u$ for some $u \in W$.

Proof. Suppose $\hat{\nu} \notin [N_T]^\perp$, then the orthogonal decomposition $V = [N_T]^\perp + N_T$ shows that the projection of $\hat{\nu}$ onto $[N_T]^\perp$ has smaller norm but still satisfies $T\hat{\nu} = w$. This gives a contradiction and shows that $\hat{\nu} \in [N_T]^\perp$. If $R_T^*$ is closed, then $R_T^* = [N_T]^\perp$ and $\hat{\nu} = T^* u$ for some $u \in W$. \qed

Corollary 6.6.6. If $A$ is a matrix such that $AA^H$ is invertible, then the minimum-norm solution to $Av = w$ is

$$v = A^H (AA^H)^{-1} w.$$  

Proof. The theorem shows that $v = A^H u$ and $Av = AA^H u = w$. Since $AA^H$ is invertible, this gives $u = (AA^H)^{-1} w$ and computing $v$ gives the desired result. \qed

The matrix $A^H (AA^H)^{-1}$ is the right inverse of $A$ and is another example of a Moore-Penrose pseudoinverse.

Definition 6.6.7. Let $T: V \to W$ be a bounded linear transformation, where $V$ and $W$ are Hilbert spaces, and $R_T$ is closed. For each $w \in W$, there is a unique vector $\hat{v}$ of minimum norm in the set of vectors that minimize $\|Tv - w\|$. The pseudoinverse $T^*$ is the transformation mapping each $w \in W$ to its unique $\hat{v}$. 
Matrix Factorization and Analysis

Matrix factorizations are an important part of the practice and analysis of signal processing. They are at the heart of many signal-processing algorithms. Their applications include solving linear equations (LU), decorrelating random variables (LDLT, Cholesky), orthogonalizing sets of vectors (QR), and finding low-rank matrix approximations (SVD). Their usefulness is often two-fold: they allow efficient computation of important quantities and they are (often) designed to minimize round-off error due to finite-precision calculation. An algorithm is called numerically stable, for a particular set of inputs, if the error in the final solution is proportional to the round-off error in the elementary field operations.

7.1 Triangular Systems

A square matrix \( L \in F^{n \times n} \) is called lower triangular (or upper triangular) if all elements above (or below) the main diagonal are zero. Likewise, a triangular matrix (lower or upper) is a unit triangular if it has all ones on the main diagonal. A system of linear equations is called triangular if it can be represented by the matrix equation \( Ax = b \) where \( A \) is either upper or lower triangular.

7.1.1 Solution by Substitution

Let \( L \in F^{n \times n} \) be a lower triangular matrix with entries \( l_{ij} = [L]_{ij} \). The matrix equation \( Ly = b \) can be solved efficiently using forward substitution, which is
defined by the recursion
\[ y_j = \frac{1}{l_{jj}} \left( b_j - \sum_{i=1}^{j-1} l_{ji} y_i \right), \quad j = 1, 2, \ldots, n. \]

Example 7.1.1. Consider the system
\[
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
y_1 \\
y_2 \\
y_3
\end{bmatrix}
= \begin{bmatrix} 1 \\ 2 \\ 9 \end{bmatrix}.
\]

Applying the above recursion gives
\[
y_1 = \frac{1}{1} = 1 \\
y_2 = \frac{1}{1}(2 - 1 \cdot 1) = 1 \\
y_3 = \frac{1}{1}(9 - 1 \cdot 1 - 2 \cdot 1) = 6.
\]

Let \( U \in F^{n \times n} \) be an upper triangular matrix with entries \( u_{ij} = [U]_{ij} \). The matrix equation \( Ux = y \) can be solved efficiently using backward substitution, which is defined by the recursion
\[ x_j = \frac{1}{u_{jj}} \left( y_j - \sum_{i=j+1}^{n} u_{ji} x_i \right), \quad j = n, n - 1, \ldots, 1. \]

Example 7.1.2. Consider the system
\[
\begin{bmatrix}
1 & 1 & 1 \\
0 & 1 & 3 \\
0 & 0 & 2
\end{bmatrix}
\begin{bmatrix}
x_1 \\
x_2 \\
x_3
\end{bmatrix}
= \begin{bmatrix} 1 \\ 1 \\ 6 \end{bmatrix}.
\]

Applying the above recursion gives
\[
x_3 = \frac{6}{2} = 3 \\
x_2 = \frac{1}{1}(1 - 3 \cdot 3) = -8 \\
x_1 = \frac{1}{1}(1 - 1 \cdot 6 - 1 \cdot (-8)) = 3.
\]

The computational complexity of each substitution is roughly \( \frac{1}{2} n^2 \) operations.
Problem 7.1.3. Show that set of upper triangular matrices is a subalgebra of the set of all matrices. Since it is clearly a subspace, only two properties must be verified:

1. that the product of two upper triangular matrices is upper triangular
2. that the inverse of an upper triangular matrix is upper triangular

7.1.2 The Determinant

The determinant $\det(A)$ of a square matrix $A \in F^{n \times n}$ is a scalar which captures a number of important properties of that matrix. For example, $A$ is invertible iff $\det(A) \neq 0$ and the determinant satisfies $\det(AB) = \det(A) \det(B)$ for square matrices $A, B$. Mathematically, it is the unique function mapping matrices to scalars that is (i) linear in each column, (ii) negated by column transposition, and (iii) satisfies $\det(I) = 1$.

The determinant of a square matrix can be defined recursively using the fact that $\det([a]) = a$. Let $A \in F^{n \times n}$ be an arbitrary square matrix with entries $a_{ij} = [A]_{ij}$. The $(i, j)$-minor of $A$ is the determinant of the $(n-1) \times (n-1)$ matrix formed by deleting the $i$-th row and $j$-th column of $A$.

Fact 7.1.4 (Laplace’s Formula). The determinant of $A$ is given by

$$\det(A) = \sum_{j=1}^{n} a_{ij}(-1)^{i+j}M_{ij} = \sum_{i=1}^{n} a_{ij}(-1)^{i+j}M_{ij},$$

where $M_{ij}$ is the $(i, j)$-minor of $A$.

Theorem 7.1.5. The determinant of a triangular matrix is the product of its diagonal elements.

Proof. For upper (lower) triangular matrices, this can be shown by expanding the determinant along the first column (row) to compute each minor. \[\square\]

7.2 LU Decomposition

7.2.1 Introduction

LU decomposition is a generalization of Gaussian elimination which allows one to efficiently solve a system of linear equations $AX = b$ multiple times with different
right-hand sides. In its basic form, it is numerically stable only if the matrix is positive definite or diagonally dominant. A slight modification, known as partial pivoting, makes it stable for a very large class of matrices.

Any square matrix $A \in F^{n \times n}$ can be factored as $A = LU$, where $L$ is a unit lower-triangular matrix and $U$ is an upper-triangular matrix. The following example uses elementary row operations to cancel, in each column, all elements below the main diagonal. These elementary row operations are represented using left multiplication by a unit lower-triangular matrix.

$$
\begin{bmatrix}
1 & 1 & 1 \\
1 & 2 & 4 \\
1 & 3 & 9
\end{bmatrix}
= 
\begin{bmatrix}
1 & 1 & 1 \\
1 & 2 & 4 \\
1 & 3 & 9
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
-1 & 1 & 0 \\
-1 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 2 & 4 \\
1 & 3 & 9
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
-1 & 1 & 0 \\
-1 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
= 
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
$$

This allows one to write

$$
\begin{bmatrix}
1 & 1 & 1 \\
1 & 2 & 4 \\
1 & 3 & 9
\end{bmatrix}
= 
\begin{bmatrix}
1 & 0 & 0 \\
1 & 0 & 0 \\
1 & 0 & 0
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & 1 \\
1 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 2 & 1
\end{bmatrix}
$$

LU decomposition can also be used to efficiently compute the determinant of $A$. Since $\det(A) = \det(LU) = \det(L) \det(U)$, the problem is reduced to computing the determinant of triangular matrices. Using Theorem 7.1.5, it is easy to see that $\det(L) = 1$ and $\det(U) = \prod_{i=1}^{n} u_{ii}$.
7.2.2 Formal Approach

To describe LU decomposition formally, we first need to describe the individual operations that are used to zero out matrix elements.

**Definition 7.2.1.** Let $A \in F^{n \times n}$ be an arbitrary matrix, $\alpha \in F$ be a scalar, and $i, j \in \{1, 2, \ldots, n\}$. Then, adding $\alpha$ times the $j$-th row to the $i$-th row an elementary row-addition operation. Moreover, $I + \alpha E_{ij}$, where $E_{ij} \triangleq e_i e_j^T$ and $e_k$ is the $k$-th standard basis vector, is the elementary row-addition matrix which effects this operation via left multiplication.

**Example 7.2.2.** For example, elementary row operations are used to cancel the $(2, 1)$ matrix entry in

$$(I - E_{2,1})A = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 1 & 3 & 9 \end{bmatrix}.$$

**Lemma 7.2.3.** The following identities capture the important properties of elementary row-operation matrices:

1. $E_{ij}E_{kl} = \delta_{j,k}E_{il}$
2. $(I + \alpha E_{ij})(I + \beta E_{kl}) = I + \alpha E_{ij} + \beta E_{kl}$ if $j \neq k$
3. $(I + \alpha E_{ij})^{-1} = (I - \alpha E_{ij})$ if $i \neq j$.

**Proof.** This proof is left as an exercise. \hfill \square

Now, consider the process for computing the LU decomposition of $A$. To initialize the process, we let $A^{(1)} = A$. In each round, we let

$$L_j^{-1} = \prod_{i=j+1}^{n} \left( I - \frac{a_{ij}^{(j)}}{a_{jj}^{(j)}} E_{i,j} \right)$$

be the product of elementary row operation matrices which cancel the subdiagonal elements of the $j$-th column. The process proceeds by defining $A^{(j+1)} = L_j^{-1} A^{(j)}$ so that $A^{(j+1)}$ has all zeros below the diagonal in the first $j$ columns. After $n - 1$ rounds, the process terminates with

$$U = A^{(n)} = L_{n-1}^{-1} L_{n-2}^{-1} \cdots L_1^{-1} A$$

where $L = L_1 L_2 \cdots L_{n-1}$ is unit lower triangular.
Lemma 7.2.4. From the structure of elementary row operation matrices, we see
\[
\prod_{j=1}^{n-1} \prod_{i=j+1}^{n} (I + \alpha_{ij} E_{i,j}) = I + \sum_{j=1}^{n-1} \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j}.
\]

Proof. First, we notice that
\[
\prod_{i=j+1}^{n} (I + \alpha_{ij} E_{i,j}) = I + \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j}
\]
for \( j = 1, 2, \ldots, n - 1 \). Expanding the product shows that any term with two \( E \) matrices must contain a product \( E_{i,j} E_{l,j} \) with \( l > i > j \). By Lemma 7.2.3i, we see that this term must be zero because \( j \neq l \).

Now, we can prove the main result via induction. First, we assume that
\[
\prod_{j=1}^{k} \prod_{i=j+1}^{n} (I + \alpha_{ij} E_{i,j}) = I + \sum_{j=1}^{k} \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j}.
\]
Next, we find that if \( k \leq n - 2 \), then
\[
\prod_{j=1}^{k+1} \prod_{i=j+1}^{n} (I + \alpha_{ij} E_{i,j}) = \left( \prod_{j=1}^{k} \prod_{i=j+1}^{n} (I + \alpha_{ij} E_{i,j}) \right) \left( \prod_{l=k+2}^{n} (I + \alpha_{l,k+1} E_{l,k+1}) \right) = I + \sum_{j=1}^{k+1} \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j} + \sum_{j=1}^{k} \sum_{i=j+1}^{n} \sum_{l=k+2}^{n} \alpha_{ij} \alpha_{l,k+1} E_{i,j} E_{l,k+1} = I + \sum_{j=1}^{k+1} \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j} + \sum_{j=1}^{k} \sum_{i=j+1}^{n} \sum_{l=k+2}^{n} \alpha_{ij} \alpha_{l,k+1} E_{i,j} E_{l,k+1} = I + \sum_{j=1}^{k+1} \sum_{i=j+1}^{n} \alpha_{ij} E_{i,j}.
\]
Finally, we point out that the base case \( k = 1 \) is given by the initial observation. □

Theorem 7.2.5. This process generates one column of \( L \) per round because
\[
[L]_{ij} = \begin{cases} 
\frac{a_{i,j}^{(i)}}{a_{j,j}^{(i)}} & \text{if } 1 \leq i < j \\
1 & \text{if } i = j \\
0 & \text{otherwise.}
\end{cases}
\]
7.2. LU DECOMPOSITION

Proof. First, we note that

\[ L = L_1 L_2 \cdots L_{n-1} \]

\[ = \prod_{j=1}^{n-1} \left( \prod_{i=j+1}^{n} \left( I - \frac{a_{i,j}}{a_{j,j}} E_{i,j} \right) \right)^{-1} \]

\[ = \prod_{i=1}^{n-1} \prod_{i=j+1}^{n} \left( I - \frac{a_{i,j}}{a_{j,j}} E_{i,j} \right)^{\alpha} \]

\[ = \prod_{i=1}^{n-1} \prod_{i=j+1}^{n} \left( I + \frac{a_{i,j}}{a_{j,j}} E_{i,j} \right)^{\beta} \]

\[ = I + \sum_{i=1}^{n-1} \sum_{i=j+1}^{n} \frac{a_{i,j}}{a_{j,j}} E_{i,j}, \]

where (a) follows from Lemma 7.2.3 (i.e., all matrices in the inside product commute) and (b) follows from Lemma 7.2.3 (ii). Picking off the \((i, j)\) entry of \(L\) (e.g., with \(e_i^T L e_j\)) gives the stated result. \(\square\)

Finally, we note that the LU decomposition can be computed in roughly \(\frac{2}{3} n^3\) field operations.

7.2.3 Partial Pivoting

Sometimes the pivot element \(a_{j,j}^{(j)}\) can be very small or zero. In this case, the algorithm will either fail (e.g., divide by zero) or return a very unreliable result. The algorithm can be easily modified to avoid this problem by swapping rows of \(A^{(j)}\) to increase the magnitude of the pivot element before each cancellation phase. This results in a decomposition of the form \(PA = LU\), where \(P\) is a permutation matrix.

In this section, we will describe LU decomposition with partial pivoting using the notation from the previous section. The main difference is that, in each round, we will define \(A^{(j+1)} = M_j^{-1} P_j A^{(j)}\) where \(P_j\) is a permutation matrix. In particular, left multiplication by \(P_j\) swaps row \(j\) with row \(p_j\), where

\[ p_j = \arg \max_{i=j+1, \ldots, n} |a_{i,j}^{(j)}|. \]

The matrix \(M_j^{-1}\) is now chosen to cancel the subdiagonal elements in \(j\)-th column of \(P_j A^{(j)}\). After \(n-1\) rounds, the resulting decomposition has the form

\[ A^{(n)} = M_{n-1}^{-1} P_{n-1} M_{n-2}^{-1} P_{n-2} \cdots M_1^{-1} P_1 A = U. \]
To show this can also be written in the desired form, we need to understand some properties of the permutations. First, we point that swapping two rows is a transposition and therefore $P_j^2 = I$. Next, we will show that the permutations can be moved to the right.

**Lemma 7.2.6.** Let $M = I + \sum_{j=1}^{k} \sum_{i=j+1}^{n} \alpha_{ij} E_{ij}$ and $Q$ be a permutation matrix which swaps row $l \geq k + 1$ and row $m > l$. Then, $QM = \tilde{M}Q$ where

$$\tilde{M} = I + \sum_{j=1}^{k} \sum_{i=j+1}^{n} \alpha_{ij} Q E_{ij}.$$ 

Therefore, we can write

$$A^{(n)} = \underbrace{M_{n-1}^{-1} \cdots M_2^{-1} \cdots M_1^{-1} P_{n-1} \cdots P_2 P_1} L^{-1} A = U$$

and $PA = LU$.

**Proof.** The proof is left as an exercise.

### 7.3 LDLT and Cholesky Decomposition

If the matrix $A \in \mathbb{C}^{n \times n}$ is Hermitian, then the LU decomposition allows the factorization $A = LDL^H$, where $L$ is unit lower triangular and $D$ is diagonal. Since this factorization is typically applied to real matrices, it is referred to as **LDLT decomposition**. If $A$ is also positive definite, then the diagonal elements of $D$ are positive and we can write $A = (LD^{1/2})(LD^{1/2})^H$. The form $A = \tilde{L}\tilde{L}^H$, where $\tilde{L}$ is lower triangular, is known as **Cholesky factorization**.

To see this, we will describe the LDLT decomposition using the notation from LU decomposition starting from $A^{(1)} = A$. In the $j$-th round, define $L_j^{-1}$ to be the product of elementary row-operation matrices which cancel the subdiagonal elements of the $j$-th column $A^{(j)}$. Then, define $A^{(j+1)} = L_j^{-1} A^{(j)} L_j^{-H}$ and notice that $A^{(j+1)}$ is Hermitian because $A^{(j)}$ is Hermitian. Next, notice that $A^{(j+1)}$ has zeros below the diagonal in the first $j$ columns and zeros to the right of diagonal in the first $j$ rows. This follows from the fact that the first $j$ rows of $A^{(j)}$ are not affected by applying $L_j^{-1}$ on left. Therefore, applying $L_j^{-H}$ on the right also cancels
7.3. LDLT AND CHOLESKY DECOMPOSITION

the elements to the right of the diagonal in the \( j \)-th row. After \( n - 1 \) rounds, we find that \( D = A^{(n)} \) is a diagonal matrix.

There are a number of redundancies in the computation described above. First off, the \( L \) matrix computed by LU decomposition is identical to the \( L \) matrix computed by LDLT decomposition. Therefore, one can save operations by defining \( A^{(j+1)} = L_{j}^{-1} A^{(j)} \). Moreover, the elements to the right of the diagonal in \( A^{(j)} \) do not affect the computation at all. So, one can roughly half the number of additions and multiplies by only updating the lower triangular part of \( A^{(j)} \). The resulting computational complexity is roughly \( \frac{1}{3} n^3 \) field operations.

7.3.1 Cholesky Decomposition

For a positive-definite matrix \( A \), we can first apply the LDLT decomposition and then define \( \tilde{L} = LD^{1/2} \). This gives the Cholesky decomposition \( \tilde{L}\tilde{L}^H = LDL^H = A \).

The Cholesky decomposition is typically used to compute whitening filters for random variables. For example, one can apply it to the correlation matrix \( R = E[XX^H] \) of a random vector \( X \). Then, one can define \( Y = \tilde{L}^{-1} X \) and see that

\[
E[YY^H] = E[\tilde{L}^{-1} XX^H \tilde{L}^{-H}] = \tilde{L}^{-1} RR^{-H} = I.
\]

From this, one sees that \( Y \) is a vector of uncorrelated (or white) random variables.

7.3.2 QR decomposition

A complex matrix \( Q \in \mathbb{C}^{n \times n} \) is called unitary if \( Q^H Q = QQ^H = I \). If all elements of the matrix are real, then it is called orthogonal and \( Q^T Q = QQ^T = I \).

Theorem 7.3.1. Any matrix \( A \in \mathbb{C}^{m \times n} \) can be factored as

\[
A = QR,
\]

where \( Q \) is an \( m \times m \) unitary matrix, \( QQ^H = I \), and \( R \) is an \( m \times n \) upper-triangular matrix.

Proof. To show this decomposition, we start by applying Gram-Schmidt Orthogonalization to the columns \( a_1, \ldots, a_n \) of \( A \). This results in orthonormal vectors
\{q_1, \ldots, q_l\}, \text{ where } l = \min(m, n), \text{ such that }
\begin{align*}
a_j &= \sum_{i=1}^{\min(j, l)} r_{i,j} q_i \quad \text{for } j = 1, 2, \ldots, n.
\end{align*}

This gives an \(m \times l\) matrix \(Q = [q_1 \ldots q_l]\) and an \(l \times n\) upper-triangular matrix \(R\), with entries \([R]_{i,j} = r_{i,j}\), such that \(A = QR\). If \(m \leq n\), then \(l = m\), \(Q\) is unitary, and the decomposition is complete. Otherwise, we must extend the orthonormal set \(\{q_1, \ldots, q_l\}\) to an orthonormal basis \(\{q_1, \ldots, q_m\}\) of \(\mathbb{C}^m\). This gives an \(m \times m\) unitary matrix \(Q' = [q_1 \ldots q_m]\). Adding \(m - n\) rows of zeros to the previous \(R\) matrix gives an \(m \times n\) matrix \(R'\) such that \(A = Q'R'\).

7.4 Hermitian Matrices and Complex Numbers

**Definition 7.4.1.** A square matrix \(Q \in \mathbb{R}^{n \times n}\) is **orthogonal** if \(Q^T Q = QQ^T = I\).

**Definition 7.4.2.** A square matrix \(U \in \mathbb{C}^{n \times n}\) is **unitary** if \(U^* U = UU^* = I\).

It is worth noting that, for unitary (resp. orthogonal) matrices, it suffices to check only that \(U^* U = I\) (resp. \(Q^T Q = I\)) because \(U\) is invertible (e.g., it has linearly independent columns) and

\[
U^* U = I \implies I = UU^{-1} = U(U^* U)U^{-1} = UU^*.
\]

A useful analogy between matrices and complex numbers is as follows.

- **Hermitian matrices** satisfying \(A^H = A\) are analogous to real numbers, whose complex conjugates are equal to themselves.

- **Unitary matrices** satisfying \(U^* U = I\) are analogous to complex numbers on the unit circle, satisfying \(\bar{z}z = 1\).

- **Orthogonal matrices** satisfying \(Q^T Q = I\) are analogous to the real numbers \(z = \pm 1\), such that \(z^2 = 1\).

The transformation

\[
z = \frac{1 + jr}{1 - jr}
\]

maps real number \(r\) into the unit circle \(|z| = 1\). Analogously, by Cayley’s formula,

\[
U = (I + jR)(I - jR)^{-1},
\]

a Hermitian matrix \(R\) is mapped to a unitary matrix.
Chapter 8

Canonical Forms

8.1 Eigenvalues and Eigenvectors

Definition 8.1.1. Let $V$ be a vector space over the field $F$ and let $T$ be a linear operator on $V$. An eigenvalue of $T$ is a scalar $\lambda \in F$ such that there exists a non-zero vector $v \in V$ with $Tv = \lambda v$. Any vector $v$ such that $Tv = \lambda v$ is called an eigenvector of $T$ associated with the eigenvalue value $\lambda$.

Definition 8.1.2. The spectrum $\sigma(T)$ of a linear operator $T : V \to V$ is the set of all scalars such that the operator $(T - \lambda I)$ is not invertible.

Example 8.1.3. Let $V = \ell_2$ be the Hilbert space of infinite square-summable sequences and $T : V \to V$ be the right-shift operator defined by

$$T(v_1, v_2, \ldots) = (0, v_1, v_2, \ldots).$$

Since $T$ is not invertible, it follows that the scalar 0 is in the spectrum of $T$. But, it is not an eigenvalue because $T v = 0$ implies $v = 0$ and an eigenvector must be a non-zero vector. In fact, this operator does not have any eigenvalues.

For finite-dimensional spaces, things are quite a bit simpler.

Theorem 8.1.4. Let $A$ be the matrix representation of a linear operator on a finite-dimensional vector space $V$, and let $\lambda$ be a scalar. The following are equivalent:

1. $\lambda$ is an eigenvalue of $A$

2. the operator $(A - \lambda I)$ is singular
3. \( \det(A - \lambda I) = 0. \)

**Proof.** First, we show the first and second are equivalent. If \( \lambda \) is an eigenvalue of \( A \), then there exists a non-zero vector \( v \in V \) such that \( Av = \lambda v \). Therefore, \( (A - \lambda I)v = 0 \) and \( (A - \lambda I) \) is singular. Likewise, if \( (A - \lambda I)v = 0 \) for some non-zero \( v \in V \) and \( \lambda \in F \), then \( Av = \lambda v \). To show the second and third are equivalent, we note that the determinant of a matrix is zero iff it is singular.

The last criterion is important. It implies that every eigenvalue \( \lambda \) is a root of the polynomial

\[
\chi_A(\lambda) \triangleq \det(\lambda I - A)
\]

called the **characteristic polynomial** of \( A \). The equation \( \det(A - \lambda I) = 0 \) is called the characteristic equation of \( A \). The spectrum \( \sigma(A) \) is given by the roots of the characteristic polynomial \( \chi_A(\lambda) \).

Let \( A \) be a matrix over the field of real or complex numbers. A nonzero vector \( v \) is called a **right eigenvector** for the eigenvalue \( \lambda \) if \( Av = \lambda v \). It is called a **left eigenvector** if \( v^H A = \lambda v^H \).

**Definition 8.1.5.** Let \( \lambda \) be an eigenvalue of the matrix \( A \). The **eigenspace** associated with \( \lambda \) is the set \( E_\lambda = \{ v \in V | Av = \lambda v \} \). The **algebraic multiplicity** of \( \lambda \) is the multiplicity of the zero at \( t = \lambda \) in the characteristic polynomial \( \chi_A(t) \). The **geometric multiplicity** of an eigenvalue \( \lambda \) is equal to dimension of the eigenspace \( E_\lambda \) or \( \text{nullity}(A - tI) \).

**Theorem 8.1.6.** If the eigenvalues of an \( n \times n \) matrix are all distinct, then the eigenvectors of \( A \) are linearly independent.

**Proof.** We will prove the slightly stronger statement: if \( \lambda_1, \lambda_2, \ldots, \lambda_k \) are distinct eigenvalues with eigenvectors \( v_1, v_2, \ldots, v_k \), then the eigenvectors are linearly independent. Suppose that

\[
\sum_{i=1}^{k} c_i v_i = 0
\]

for scalars \( c_1, c_2, \ldots, c_k \). Notice that one can annihilate \( v_j \) from this equation by multiplying both sides by \( (A - \lambda_j I) \). So, multiplying both sides by a product of
8.1. EIGENVALUES AND EIGENVECTORS

these matrices gives

\[
\prod_{j=1, j \neq m}^{k} (A - \lambda_j I) \sum_{i=1}^{k} c_j v_i = \left( \prod_{j=1, j \neq m}^{k} (A - \lambda_j I) \right) c_m v_m = c_m v_m \prod_{j=1, j \neq m}^{k} (\lambda_m - \lambda_j) = 0.
\]

Since all eigenvalues are distinct, we must conclude that \( c_m = 0 \). Since the choice of \( m \) was arbitrary, it follows that \( c_1, c_2, \ldots, c_k \) are all zero. Therefore, the vectors \( v_1, v_2, \ldots, v_k \) are linearly independent. \( \square \)

**Definition 8.1.7.** Let \( T \) be a linear operator on a finite-dimensional vector space \( V \). The operator \( T \) is **diagonalizable** if there exists a basis \( B \) for \( V \) such that each basis vector is an eigenvector of \( T \).

\[
[T]_B = \begin{bmatrix}
\lambda_1 & 0 & \cdots & 0 \\
0 & \lambda_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \lambda_n
\end{bmatrix}
\]

Similarly, a matrix \( A \) is diagonalizable if there exists an invertible matrix \( S \) such that

\[ A = SAS^{-1} \]

where \( \Lambda \) is a diagonal matrix.

**Theorem 8.1.8.** If an \( n \times n \) matrix has \( n \) linearly independent eigenvectors, then it is diagonalizable.

**Proof.** Suppose that the \( n \times n \) matrix \( A \) has \( n \) linearly independent eigenvectors, which we denote by \( v_1, \ldots, v_n \). Let the eigenvalue of \( v_i \) be denoted by \( \lambda_i \) so that

\[ Av_j = \lambda_j v_j, \quad j = 1, \ldots, n. \]

In matrix form, we have

\[
A \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} = \begin{bmatrix} Av_1 & \cdots & Av_n \end{bmatrix} = \begin{bmatrix} \lambda_1 v_1 & \cdots & \lambda_n v_n \end{bmatrix}.
\]
We can rewrite the last matrix on the right as
\[
\begin{bmatrix}
\lambda_1 v_1 & \cdots & \lambda_n v_n
\end{bmatrix} =
\begin{bmatrix}
\lambda_1 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & \lambda_n
\end{bmatrix} = S \Lambda.
\]

where
\[
S = \begin{bmatrix}
v_1 & \cdots & v_n
\end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix}
\lambda_1 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & \lambda_n
\end{bmatrix},
\]

Combining these two equations, we obtain the equality
\[
AS = S \Lambda.
\]

Since the eigenvectors are linearly independent, the matrix \( S \) is full rank and hence invertible. We can therefore write
\[
A = S \Lambda S^{-1}
\]
\[
\Lambda = S^{-1} AS.
\]

That is, the matrix \( A \) is diagonalizable. \(\square\)

The type of the transformation from \( A \) to \( \Lambda \) arises in a variety of contexts.

**Definition 8.1.9.** If there exists an invertible matrix \( T \) such that
\[
A = T B T^{-1},
\]
then matrices \( A \) and \( B \) are said to be **similar**.

If \( A \) and \( B \) are similar, then they have the same eigenvalues. Similar matrices can be considered representations of the same linear operator using different bases.

**Lemma 8.1.10.** Let \( A \) be an \( n \times n \) Hermitian matrix (i.e., \( A^H = A \)). Then, the eigenvalues of \( A \) are real and the eigenvectors associated with distinct eigenvalues are orthogonal.

**Proof.** First, we notice that \( A = A^H \) implies \( v^H A v \) is real because
\[
\bar{s} = (v^H A v)^H = v^H A^H v = v^H A v = s.
\]
If $Av = \lambda_1 v$, left multiplication by $v^H$ shows that

$$v^H Av = \lambda_1 v^H v = \lambda_1 \|v\|^2.$$

Therefore, $\lambda_1$ is real. Next, assume that $Aw = \lambda_2 w$ and $\lambda_2 \neq \lambda_1$. Then, we have

$$\lambda_1 \lambda_2 w^H v = w^H A^H Av = w^H A^2 v = \lambda_1^2 w^H v.$$

We also assume, without loss of generality, that $\lambda_1 \neq 0$. Therefore, if $\lambda_2 \neq \lambda_1$, then $w^H v = 0$ and the eigenvectors are orthogonal.

8.2 Applications of Eigenvalues

8.2.1 Differential Equations

It is well known that the solution of the 1st-order linear differential equation

$$\frac{d}{dt} x(t) = ax(t)$$

is given by

$$x(t) = e^{at} x(0).$$

It turns out that this formula can be extended to coupled differential equations. Let $A$ be a diagonalizable matrix and consider the set of 1st order linear differential equations defined by

$$\frac{d}{dt} x(t) = Ax(t).$$

Using the decomposition $A = S \Lambda S^{-1}$ and the substitution $x(t) = Sy(t)$, we find that

$$\frac{d}{dt} \overline{x}(t) = \frac{d}{dt} Sy(t) = S \frac{d}{dt} y(t).$$

and

$$\frac{d}{dt} \overline{x}(t) = A \overline{x}(t) = ASy(t).$$
This implies that
\[ \frac{d}{dt}y(t) = S^{-1}ASy(t) = \Lambda y(t). \]

Solving each individual equation gives
\[ y_j(t) = e^{\lambda_j t} y_j(0) \]
and we can group them together in matrix form with
\[ y(t) = e^{\Lambda t} y(0). \]

In terms of \( x(t) \), this gives
\[ x(t) = S e^{\Lambda t} S^{-1} x(0). \]

In the next section, we will see this is equal to
\[ x(t) = e^{At} x(0). \]

### 8.2.2 Functions of a Matrix

The diagonal form of a diagonalizable matrix can be used in a number of applications. One such application is the computation of matrix exponentials. If \( A = SAS^{-1} \) then
\[ A^2 = SAS^{-1}SAS^{-1} = S\Lambda^2S^{-1} \]
and, more generally,
\[ A^n = SAS^{-1}. \]

Note that \( \Lambda^n \) is obtained in a straightforward manner as
\[ \Lambda^n = \begin{bmatrix} \lambda_1^n & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n^n \end{bmatrix}. \]

This observation drastically simplifies the computation of the matrix exponential \( e^A \),
\[ e^A = \sum_{i=0}^{\infty} \frac{A^i}{i!} = S \left( \sum_{i=0}^{\infty} \frac{\Lambda^i}{i!} \right) S^{-1} = Se^{\Lambda}S^{-1}, \]

where
\[ e^A = \begin{bmatrix} e^{\lambda_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{\lambda_n} \end{bmatrix}. \]
Theorem 8.2.1. Let \( p(\cdot) \) be a given polynomial. If \( \lambda \) is an eigenvalue of \( A \), while \( v \) is an associated eigenvector, then \( p(\lambda) \) is an eigenvalue of the matrix \( p(A) \) and \( v \) is an eigenvector of \( p(A) \) associated with \( p(\lambda) \).

Proof. Consider \( p(A)v \). Then,

\[
p(A)v = \sum_{k=0}^{t} p_k A^k v = \sum_{k=0}^{t} p_k \lambda^k v = p(\lambda)v.
\]

That is \( p(A)v = p(\lambda)v \). \( \Box \)

A matrix \( A \) is singular if and only if 0 is an eigenvalue of \( A \).

8.3 The Jordan Form

Not all matrices are diagonalizable. In particular, if \( A \) has an eigenvalue whose algebraic multiplicity is larger than its geometric multiplicity, then that eigenvalue is called defective. A matrix with a defective eigenvalue is not diagonalizable.

Theorem 8.3.1. Let \( A \) be an \( n \times n \) matrix. Then \( A \) is diagonalizable if and only if there is a set of \( n \) linearly independent vectors, each of which is an eigenvector of \( A \).

Proof. If \( A \) has \( n \) linearly independent eigenvectors \( v_1, \ldots, v_n \), then let \( S \) be an invertible matrix whose columns are there \( n \) vectors. Consider

\[
S^{-1}AS = S^{-1} \begin{bmatrix} A v_1 & \cdots & A v_n \end{bmatrix} = S^{-1} \begin{bmatrix} \lambda_1 v_1 & \cdots & \lambda_n v_n \end{bmatrix} = S^{-1}SA = \Lambda.
\]

Conversely, suppose that there is a similarity matrix \( S \) such that \( S^{-1}AS = \Lambda \) is a diagonal matrix. Then \( AS = SA \). This implies that \( A \) times the \( i \)th column of \( S \) is the \( i \)th diagonal entry of \( \Lambda \) times the \( i \)th column of \( S \). That is, the \( i \)th column of \( S \) is an eigenvector of \( A \) associated with the \( i \)th diagonal entry of \( \Lambda \). Since \( S \) is nonsingular, there are exactly \( n \) linearly independent eigenvectors. \( \Box \)
Definition 8.3.2. The **Jordan normal form** of any matrix $A \in \mathbb{C}^{n \times n}$ with $l \leq n$ linearly independent eigenvectors can be written as

$$A = TJT^{-1},$$

where $T$ is an invertible matrix and $J$ is the block-diagonal matrix

$$J = \begin{bmatrix} J_{m_1}(\lambda_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_{m_l}(\lambda_l) \end{bmatrix}.$$ 

The $J_m(\lambda)$ are $m \times m$ matrices called Jordan blocks, and they have the form

$$J_m(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{bmatrix}.$$ 

It is important to note that the eigenvalues $\lambda_1, \ldots, \lambda_l$ are not necessarily distinct (i.e., multiple Jordan blocks may have the same eigenvalue). The Jordan matrix $J$ associated with any matrix $A$ is unique up to the order of the Jordan blocks. Moreover, two matrices are similar iff they are both similar to the same Jordan matrix $J$.

Since every matrix is similar to a Jordan block matrix, one can gain some insight by studying Jordan blocks. In fact, Jordan blocks exemplify the way that matrices can be degenerate. For example, $J_m(\lambda)$ has the single eigenvector $e_1$ (i.e., the standard basis vector) and satisfies

$$J_m(0) e_{j+1} = e_j \quad \text{for} \quad j = 1, 2, \ldots, m - 1.$$ 

So, the reason this matrix has only one eigenvector is that left-multiplication by this matrix shifts all elements in a vector up element.

Computing the Jordan normal form of a matrix can be broken into two parts. First, one can identify, for each distinct eigenvalue $\lambda$, the **generalized eigenspace**

$$G_\lambda = \{ \nu \in \mathbb{C}^n \mid (A - \lambda I)^n \nu = 0 \}.$$ 

Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of $A$ ordered by decreasing magnitude. Let $d_j$ be the dimension of $G_{\lambda_j}$, which is equal to the sum of the sizes of the Jordan blocks associated with $\lambda_j$. The Jordan matrix $J$ is then constructed by placing the Jordan blocks corresponding to each distinct eigenvalue in the order of decreasing magnitude. The invertible matrix $T$ is constructed by using a basis of eigenvectors and generalized eigenvectors as its columns.
blocks associated with $\lambda$, then $\sum_{j=1}^{k} d_j = n$. Let $T$ be a matrix whose first $d_1$ columns for a basis for $G_{\lambda_1}$, next $d_2$ columns form a basis for $G_{\lambda_2}$, and so on. In this case, the matrix $T^{-1}AT$ is block diagonal and the $j$-th block $B_j$ is associated with the eigenvalue $\lambda_j$.

To put $A$ in Jordan normal form, we now need to transform each block matrix $B$ into Jordan normal form. One can do this by identifying the subspace $V_j$ that is not mapped to 0 by $(B - \lambda I)^{j-1}$ (i.e., $\mathcal{N}((B - \lambda I)^{j-1})^\perp$). This gives the sequence $V_1, \ldots, V_J$ of non-empty subspaces (e.g., $V_j$ is empty for $j > J$). Now, we can form a sequence of bases $W_J, W_{J-1}, \ldots, W_1$ recursively starting from $W_J$ with

$$W_j = W_{j+1} \cup \{(B - \lambda I)w | w \in W_{j+1}\} \cup \text{basis}(V_j - V_{j-1}),$$

where $\text{basis}(V_j - V_{j-1})$ is some set basis vectors that extends $V_{j-1}$ to $V_j$. Each vector in $W_j$ gives rise to a length $j$ Jordan chain of vectors $v_{i-1} = (B - \lambda I)v_i \in W_{i-1}$ starting from any $v_j \in W_j$. Each vector $v_j$ defined in this way is called a generalized eigenvector of order $j$. By correctly ordering the basis $W_1$ as columns of $T$, one finds that $T^{-1}BT$ is a Jordan matrix.

**Example 8.3.3.** Consider the matrix

$$\begin{bmatrix} 4 & 0 & 1 & 0 \\ 2 & 2 & 3 & 0 \\ -1 & 0 & 2 & 0 \\ 4 & 0 & 1 & 2 \end{bmatrix}.$$

First, we find the characteristic polynomial

$$\chi_A(t) = \det(tI - A) = t^4 - 10t^3 + 37t^2 - 60t + 36 = (t - 2)^2(t - 3)^2.$$

Next, we find the eigenvectors associated with the eigenvalues $\lambda_1 = 3$ and $\lambda_2 = 2$. This is done by finding a basis $v_1^{(1)}, v_2^{(1)}, \ldots$ for the nullspace of $A - \lambda I$ and gives

$$v_1^{(1)} = [1 \ -1 \ -1 \ 3]^T, \quad v_2^{(1)} = [0 \ 1 \ 0 \ 0]^T, \quad v_2^{(2)} = [0 \ 0 \ 0 \ 1]^T.$$

Since the eigenvalue $\lambda_1$ has algebraic multiplicity 2 and geometric multiplicity 1, we still need to find another generalized eigenvector associated with this eigenspace.
In particular, we need a vector \( \underline{w} \) which satisfies \((A - \lambda_1 I)\underline{w} = \underline{v}_1^{(1)} \). This gives

\[
\begin{bmatrix}
1 & 0 & 1 & 0 \\
2 & -1 & 3 & 0 \\
-1 & 0 & -1 & 0 \\
4 & 0 & 1 & -1
\end{bmatrix}
\begin{bmatrix}
w_1 \\
w_2 \\
w_3 \\
w_4
\end{bmatrix} =
\begin{bmatrix}
1 \\
-1 \\
-1 \\
3
\end{bmatrix}.
\]

Using the pseudoinverse of \((A - \lambda_1 I)\), one finds that \( \underline{w} = \left[ \frac{11}{12} \frac{37}{12} \frac{1}{12} \frac{9}{12} \right] \). Using this, we construct the Jordan normal form by noting that

\[
\begin{bmatrix}
4 & 0 & 1 & 0 \\
2 & 2 & 3 & 0 \\
-1 & 0 & 2 & 0 \\
4 & 0 & 1 & 2
\end{bmatrix}
\begin{bmatrix}
\underline{v}_1^{(1)} \\
\underline{w} \\
\underline{v}_1^{(2)} \\
\underline{v}_2^{(2)}
\end{bmatrix} =
\begin{bmatrix}
3 & 1 & 0 & 0 \\
0 & 3 & 0 & 0 \\
0 & 0 & 2 & 0 \\
0 & 0 & 0 & 2
\end{bmatrix}
\begin{bmatrix}
\underline{v}_1^{(1)} \\
\underline{w} \\
\underline{v}_1^{(2)} \\
\underline{v}_2^{(2)}
\end{bmatrix}.
\]

This implies that \( A = TJT^{-1} \) with

\[
T = \begin{bmatrix}
\underline{v}_1^{(1)} & \underline{w} & \underline{v}_1^{(2)} & \underline{v}_2^{(2)}
\end{bmatrix} =
\begin{bmatrix}
1 & \frac{11}{12} & 0 & 0 \\
-1 & \frac{37}{12} & 1 & 0 \\
-1 & \frac{1}{12} & 0 & 0 \\
3 & \frac{9}{12} & 0 & 1
\end{bmatrix}.
\]

### 8.4 Applications of Jordan Normal Form

Jordan normal form often allows one to extend to all matrices results that are easy to prove for diagonalizable matrices.

#### 8.4.1 Convergent Matrices

**Definition 8.4.1.** An \( n \times n \) matrix \( A \) is **convergent** if \( \| A^k \| \to 0 \) for any norm.

Of course, this is equivalent to the statement “\( A^k \) converges to the all zero matrix”. Since all finite-dimensional vector norms are equivalent, it also follows that this condition does not depend on the norm chosen.
Recall that the spectral radius $\rho(A)$ of a matrix $A$ is the magnitude of the largest eigenvalue. If $A$ is diagonalizable, then $A^k = T \Lambda^k T^{-1}$ and it is easy to see that

$$\|A^k\| \leq \|T\| \|\Lambda^k\| \|T^{-1}\|.$$ 

Since all finite-dimensional vector norms are equivalent, we know that $\|\Lambda^k\| \leq M \|\Lambda^k\|_1 = M \rho(A)^k$. Therefore, $A$ is convergent if $\rho(A) < 1$. If $\rho(A) \geq 1$, then it is easy to show that $\|\Lambda^k\| > 0$ and therefore that $\|A^k\| > 0$. For general matrices, we can instead use the Jordan normal form and the following lemma.

**Lemma 8.4.2.** The Jordan block $J_m(\lambda)$ is convergent iff $|\lambda| < 1$.

**Proof.** This follows from the fact that $J_m(\lambda) = \lambda I + N$, where $[N]_{i,j} = \delta_{i+1,j}$. Using the Binomial formula, we write

$$\|(\lambda I + N)^k\| = \left\| \sum_{i=0}^{k} \binom{k}{i} N^i \lambda^{k-i} \right\|$$

$$\leq \sum_{i=0}^{m-1} \binom{k}{i} |\lambda|^{k-i},$$

where the second step follows from the fact that $\|N^i\|$ is 1 for $i = 1, \ldots, m - 1$ and zero for $i \geq m$. Notice that $\binom{k}{i} |\lambda|^{k-i} \leq k^{m-1} |\lambda|^{k-m+1}$ for $0 \leq i \leq m - 1$. Since $k^{m-1} |\lambda|^{k-m+1} \to 0$ as $k \to \infty$ iff $|\lambda| < 1$, we see that each term in the sum converges to zero under the same condition. On the other hand, if $|\lambda| \geq 1$, then $|\binom{k}{i} |\lambda|^{k-i}| \geq 1$ for all $k \geq 0$.

**Theorem 8.4.3.** A matrix $A \in \mathbb{C}^{n \times n}$ is convergent iff $\rho(A) < 1$.

**Proof.** Using the Jordan normal form, we can write $A = T J T^{-1}$, where $J$ is a block diagonal with $k$ Jordan blocks $J_1, \ldots, J_k$. Since $J$ is block diagonal, we also have that $\|J^k\| \leq \sum_{i=1}^{k} \|J_i^k\|$. If $\rho(A) < 1$, then the eigenvalue $\lambda$ associated with each Jordan block satisfies $\|\lambda\| < 1$. In this case, the lemma shows that $\|J_i^k\| \to 0$ which implies that $\|J^k\| \to 0$. Therefore, $\|A^k\| \to 0$ and $A$ is convergent. On the other hand, if $\rho(A) \geq 1$, then there is a Jordan block $J_i$ with $|\lambda| \geq 1$ and $|[J_i^k]_{1,1}| \geq 1$ for all $k \geq 0$. 

In some cases, one can make stronger statements about large powers of a matrix.
Definition 8.4.4. A matrix $A$ has a unique eigenvalue of maximum modulus if the Jordan block associated with that eigenvalue is $1 \times 1$ and all other Jordan blocks are associated with eigenvalues of smaller magnitude.

The following theorem shows that a properly normalized matrix of this type converges to a non-zero limit.

Theorem 8.4.5. If $A$ has a unique eigenvalue $\lambda_1$ of maximum modulus, then

$$\lim_{k \to \infty} \frac{1}{\lambda_1^k} A^k = uu^H,$$

where $Au = \lambda_1 u$, $u^HA = \lambda_1 v^H$, and $v^Hu = 1$.

Proof. Let $B = \frac{1}{\lambda_1} A$ so that maximum modulus eigenvalue is now 1. Next, choose the Jordan normal form $B = TJT^{-1}$ so that the Jordan block associated with the eigenvalue 1 is in the top left corner of $J$. In this case, it follows from the lemma that $J^n$ converges to $e_1e_1^H$ as $n \to \infty$. This implies that $B^n = TJ^nT^{-1}$ converges to $T e_1e_1^HT^{-1} = uu^H$ where $u$ is the first column of $T$ and $v^H$ is the first row of $T^{-1}$.

By construction, the first column of $T$ is the right eigenvector $u$ and satisfies $Au = \lambda_1 u$. Likewise, the first row of $T^{-1}$ is the left eigenvector $v^H$ associated with the eigenvalue 1 because $B^H = T^{-H}J^HT^H$ and the first column of $T^{-H}$ (i.e., Hermitian conjugate of first row of $T^{-1}$) is the right eigenvector of $A^H$ associated with $\lambda_1$. Therefore, $v^HA = \lambda_1 v^H$. Finally, the fact that $u = B^n u \to uu^Hu$ implies that $v^Hu = 1$.  \qed
Chapter 9

Singular Value Decomposition

9.1 Diagonalization of Hermitian Matrices

Lemma 9.1.1 (Schur Decomposition). For any square matrix $A$, there exists a unitary matrix $U$ such that

$$U^H A U = T$$

where $T$ is upper triangular. That is, every square matrix is similar to an upper-triangular matrix.

Proof. We prove this lemma by induction on the size $n$ of the matrix. Since it is clearly true for scalars (i.e., matrices of size $n = 1$), the base case is trivial. Now, suppose that the result holds for all $k = 1, 2, \ldots, n - 1$ and let $A \in \mathbb{C}^{n \times n}$. Since every matrix has at least one eigenvector, we let $u$ be an eigenvector of $A$ normalized so that $\|u\|_2 = 1$. Using the Gram-Schmidt procedure, it is possible to construct an orthonormal basis $B = \mathbf{x}_1, \ldots, \mathbf{x}_n$ for $\mathbb{C}^n$, with $\mathbf{x}_1 = u$. Define the matrix $U_n$ by

$$U_n = \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_n \end{bmatrix}.$$

Since $B$ is a basis for $\mathbb{C}^n$, every column of the matrix $AU_n$ can be expressed as a linear combination of vectors in $B$, say,

$$A\mathbf{x}_i = \sum_{j=1}^{n} s_{j,i} \mathbf{x}_j \quad i = 1, \ldots, n.$$

Note that $A\mathbf{x}_1 = \lambda_1 \mathbf{x}_1$ for some $\lambda_1$ since $\mathbf{x}_1 = u$, an eigenvector of $A$. We can then
CHAPTER 9. SINGULAR VALUE DECOMPOSITION

write

\[ A U_n = \begin{bmatrix} A_{x_1} & \cdots & A_{x_n} \end{bmatrix} = U_n \begin{bmatrix} \lambda_1 & s_{1,2} & \cdots & s_{1,n} \\ 0 & s_{2,2} & \cdots & s_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & s_{n,2} & \cdots & s_{n,n} \end{bmatrix} = U_n \begin{bmatrix} \lambda_1 & s^T \\ 0 & A_{n-1} \end{bmatrix}, \]

where we have used the convenient notation

\[ A_{n-1} = \begin{bmatrix} s_{2,2} & \cdots & s_{2,n} \\ \vdots & \ddots & \vdots \\ s_{n,2} & \cdots & s_{n,n} \end{bmatrix} \]

and \( s^T = (s_{1,2}, \ldots, s_{1,n}) \). By the inductive hypothesis, we can write \( A_{n-1} = U_{n-1} T_{n-1} U_{n-1}^H \) where \( T_{n-1} \) is upper triangular and \( U_{n-1} \) is unitary. It follows that

\[
AU_n = U_n \begin{bmatrix} \lambda_1 & s^T \\ 0 & A_{n-1} \end{bmatrix} = U_n \begin{bmatrix} \lambda_1 & s^T \\ 0 & U_{n-1} T_{n-1} U_{n-1}^H \end{bmatrix} \\
= U_n \begin{bmatrix} 1 & 0^T \\ 0 & U_{n-1} \end{bmatrix} \begin{bmatrix} \lambda_1 & s^T U_{n-1} \\ 0 & T_{n-1} \end{bmatrix} \begin{bmatrix} 1 & 0^T \\ 0 & U_{n-1}^H \end{bmatrix}.
\]

Let \( U \) be the matrix given by

\[ U = U_n \begin{bmatrix} 1 & 0^T \\ 0 & U_{n-1} \end{bmatrix}, \]

and note that \( U \) is unitary. It follows that

\[ U^H A U = \begin{bmatrix} \lambda_1 & s^T U_{n-1} \\ 0 & T_{n-1} \end{bmatrix}. \]

That is, \( U \) is a unitary matrix such that \( U^H A U \) is upper-triangular.

We use this lemma to prove the following theorem.

**Theorem 9.1.2.** *Every Hermitian \( n \times n \) matrix \( A \) can be diagonalized by a unitary matrix,*

\[ U^H A U = \Lambda, \]

*where \( U \) is unitary and \( \Lambda \) is a diagonal matrix.*
Proof. Note that $A^H = A$ and $T = U^H A U$. Consider the matrix $T^H$ given by

$$T^H = (U^H A U)^H = U^H A^H U = U^H A U = T.$$  

That is, $T$ is also Hermitian. Since $T$ is upper triangular, this implies that $T$ is a diagonal matrix. We must conclude that every Hermitian matrix is diagonalized by a unitary matrix.

This proves every Hermitian matrix has a complete set of orthonormal eigenvectors.

9.2 Singular Value Decomposition

The singular value decomposition (SVD) provides a matrix factorization related to the eigenvalue decomposition that works for all matrices. In general, any matrix $A \in \mathbb{C}^{m \times n}$ can be factored into a product of unitary matrices and a diagonal matrix, as explained below.

**Theorem 9.2.1.** Let $A$ be a matrix in $\mathbb{C}^{m \times n}$. Then $A$ can be factored as

$$A = U \Sigma V^H$$

where $U \in \mathbb{C}^{m \times m}$ is unitary, $V \in \mathbb{C}^{n \times n}$ is unitary, and $\Sigma \in \mathbb{R}^{m \times n}$ has the form

$$\Sigma = \text{diag}(\sigma_1, \sigma_2, \ldots, \sigma_p),$$

where $p = \min(m, n)$.

The diagonal elements of $\Sigma$ are called the singular values of $A$ and are typically ordered so that

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_p \geq 0.$$

**Proof.** Let

$$A^H A = V \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$$

be the spectral decomposition of $A^H A$, where the columns of $V$ are orthonormal eigenvectors

$$V = \begin{bmatrix} \psi_1 & \psi_2 & \cdots & \psi_n \end{bmatrix},$$

and

$$U = \begin{bmatrix} u_1 & u_2 & \cdots & u_n \end{bmatrix}.$$
with \( \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0 = \lambda_{r+1} = \cdots = \lambda_n \) and \( r \leq p \). For \( i \leq r \), let
\[
u_i = \frac{A v_i}{\sqrt{\lambda_i}},
\]
and observe that
\[
\langle u_i, u_j \rangle = \frac{v_j^H A^H A v_i}{\sqrt{\lambda_i \lambda_j}} = \frac{v_j^H v_i \lambda_i}{\sqrt{\lambda_i \lambda_j}} = \delta_{ij}.
\]
Also note that \( \{u_i\} \) are eigenvectors of \( A A^H \) since
\[
A A^H u_i = A A^H A \frac{v_i}{\sqrt{\lambda_i}} = \sqrt{\lambda_i} A v_i = \lambda_i u_i.
\]
The set \( \{u_i : i = 1, \ldots, r\} \) can be extended using the Gram-Schmidt procedure to form an orthonormal basis for \( \mathbb{C}^m \). Let
\[
U = \begin{bmatrix} u_1 & \cdots & u_m \end{bmatrix}.
\]
For the zero eigenvalues, the eigenvectors must come from the nullspace of \( A A^H \) since the eigenvectors with zero eigenvalues are, by construction, orthogonal to the eigenvectors with nonzero eigenvalues that are in the range of \( A A^H \).

For \( u_i \) where \( i \leq r \), we get
\[
u_i^H A V = \frac{1}{\sqrt{\lambda_i}} v_i^H A^H A V = \sqrt{\lambda_i} \xi_i^H.
\]
On the other hand, if \( i > r \) then \( u_i^H A V = 0 \). Hence,
\[
U^H A V = \text{diag} \left( \sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n} \right) = \Sigma,
\]
as desired. \( \square \)

This proof gives a recipe for computing the SVD of an arbitrary matrix. Consider the matrix
\[
A = \begin{bmatrix} 1 & 1 \\ 5 & -1 \\ -1 & 5 \end{bmatrix}.
\]
The eigenvalue decomposition of \( A^H A \) is given by
\[
A^H A = \begin{bmatrix} 27 & -9 \\ -9 & 27 \end{bmatrix} = V \Lambda V^H = \left( \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 36 & 0 \\ 0 & 18 \end{bmatrix} \left( \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \right).
\]
This implies that $\Sigma_1 = \Lambda^{1/2}$ and $V_1 = V$. Therefore, we can compute $U_1 = AV_1\Sigma_1^{-1}$ with

$$
U_1 = \begin{bmatrix}
1 & 1 \\
5 & -1 \\
-1 & 5
\end{bmatrix} \begin{bmatrix}
1 \\
\frac{1}{\sqrt{2}} \\
-1
\end{bmatrix} \begin{bmatrix}
-1 & 1 \\
1 & 1 \\
0 & \frac{1}{\sqrt{18}}
\end{bmatrix} = \begin{bmatrix}
0 & \frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} \\
\frac{1}{\sqrt{2}} & \frac{2}{3}\sqrt{2}
\end{bmatrix}.
$$

Putting this all together, we have the compact SVD

$$
A = U_1\Sigma_1V_1^H = \begin{bmatrix}
0 & \frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} \\
\frac{\sqrt{36}}{2} & 0 & \sqrt{18}
\end{bmatrix} \begin{bmatrix}
1 & -1 & 1 \\
1 & 1 & 1
\end{bmatrix}.
$$

### 9.3 Properties of the SVD

Many of the important properties of the SVD can be understood better by separating the non-zero singular values from the zero singular values. To do this, we note that every rank $r$ matrix $A \in \mathbb{C}^{m \times n}$ has a singular value decomposition

$$
A = U\Sigma V^H = \begin{bmatrix}
U_1 & U_2
\end{bmatrix} \begin{bmatrix}
\Sigma_1 & 0 \\
0 & 0
\end{bmatrix} \begin{bmatrix}
V_1^H \\
V_2^H
\end{bmatrix} = U_1\Sigma_1V_1^H,
$$

where $U \in \mathbb{C}^{m \times m}$ and $V \in \mathbb{C}^{n \times n}$ are unitary and $U_1 \in \mathbb{C}^{m \times r}$, $U_2 \in \mathbb{C}^{m \times m-r}$, $V_1 \in \mathbb{C}^{n \times r}$, and $V_2 \in \mathbb{C}^{n \times n-r}$ have orthonormal columns. The diagonal matrix $\Sigma_1 \in \mathbb{R}^{r \times r}$ contains the non-zero singular values

$$
\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0.
$$

The factorization $A = U\Sigma V^H$ is called the **full SVD** of the matrix $A$ while the factorization $A = U_1\Sigma_1V_1$ is called the **compact SVD** of $A$. The compact SVD of a rank-$r$ matrix retains only the $r$ columns of $U, V$ associated with non-zero singular values.

Let $X, Y$ be inner product spaces and let $A$ define a mapping from $X$ to $Y$. Then, the columns of $V_1$ form an orthonormal basis for the vectors in $X$ that are mapped to non-zero vectors (i.e., $\mathcal{N}(A)^\perp$) while the columns of $V_2$ form an orthonormal basis of $\mathcal{N}(A)$. Likewise, the columns of $U_1$ form an orthonormal basis for the vectors in $Y$ that lie in the range of $A$ while the vectors in $U_2$ form orthonormal basis for $\mathcal{R}(A)^\perp$. It follows that the full SVD computes orthonormal bases for
all of the four fundamental subspaces of the matrix $A$. For example, it is easy to show that

$$\mathcal{R}(A) = \text{span}(U_1)$$
$$\mathcal{R}(A^H) = \text{span}(V_1)$$
$$\mathcal{N}(A) = \text{span}(V_2)$$
$$\mathcal{N}(A^H) = \text{span}(U_2)$$

To see this, notice that $A \sum_{i=1}^t c_i u_i = \sum_{i=1}^t c_i \sigma_i u_i$.

From this, we can compute easily any projection onto a fundamental subspace. First, we point out that the projection onto the column space of any matrix $W \in \mathbb{C}^{m \times n}$ with orthonormal columns (i.e., $W^H W = I$) is given by

$$P_W = W (W^H W)^{-1} W^H = WW^H.$$ 

Therefore, the projection matrices for the fundamental subspaces are given by

$$P_{\mathcal{R}(A)} = U_1 U_1^H$$
$$P_{\mathcal{R}(A^H)} = V_1 V_1^H$$
$$P_{\mathcal{N}(A)} = V_2 V_2^H = I - V_1 V_1^H$$
$$P_{\mathcal{N}(A^H)} = U_2 U_2^H = I - U_1 U_1^H.$$

This decomposition also provides a rank revealing decomposition of a rank-$r$ matrix

$$A = \sum_{i=1}^r \sigma_i u_i v_i^H,$$

where $u_i$ is the $i$th column of $U$ and $v_i$ is the $i$th column of $V$. This shows $A$ as the sum of $r$ rank-1 matrices. It also allows one to compute

$$\|A\|_F^2 = \sum_{i=1}^r \sigma_i^2$$
$$\|A\|_2 = \sigma_1$$

The pseudoinverse of $A$ is also very easy to compute from the SVD. In particular, one finds that

$$A^\dagger = V \Sigma^\dagger U^H = V_1 \Sigma_1^{-1} U_1^H.$$ 

One can verify this by computing $A^\dagger A$ and $AA^\dagger$. It also follows from the fact that the pseudoinverse of a scalar $\sigma$ is $\sigma^{-1}$ if $\sigma \neq 0$ and zero otherwise.
Appendix A

Optional Topics

A.1 Dealing with Infinity*

A.1.1 The Axiom of Choice

The axiom of choice, formulated by Zermelo in 1904, is innocent-looking. However, one can prove theorems with its aid that some mathematicians were originally reluctant to accept in the past.

Definition A.1.1 (The Axiom of Choice). Given a collection \( \mathcal{X} \) of disjoint nonempty sets, there exists a set \( C \) having exactly one element in common with each element of \( \mathcal{X} \). That is, for each \( X \in \mathcal{X} \) the set \( C \cap X \) contains a single element.

Most mathematicians today accept the axiom of choice as part of the set theory on which they base their mathematics. A straightforward consequence of the axiom of choice is the existence of a choice function.

Lemma A.1.2 (Existence of a Choice Function). Given a collection \( \mathcal{Y} \) of non-empty sets, there exists a function

\[
c : \mathcal{Y} \to \bigcup_{Y \in \mathcal{Y}} Y
\]

satisfying \( c(Y) \in Y \) for every \( Y \in \mathcal{Y} \).

Proof. The difference between the axiom of choice and the lemma is that in the latter statement the sets of the collection \( \mathcal{Y} \) need not be disjoint. Given an element \( Y \in \mathcal{Y} \), define the set \( Y' \) by

\[
Y' = \{(Y, y) \mid y \in Y\}.
\]
That is, $Y'$ is the collection of all ordered pairs where the first coordinate of the ordered pair is the set $Y$, and the second coordinate is an element of $Y$. Because $Y$ contains at least one element, the set $Y'$ is nonempty. Furthermore, $Y'$ is a subset of the cartesian product

$$Y \times \bigcup_{Y \in \mathcal{Y}} Y.$$ 

If $Y_1$ and $Y_2$ are two different sets in $\mathcal{Y}$, then the sets $Y_1'$ and $Y_2'$ are disjoint; specifically, the elements of $Y_1'$ and $Y_2'$ differ at least in their first coordinates.

Consider the collection

$$\mathcal{Z} = \{Y'|Y \in \mathcal{Y}\}.$$ 

This is a collection of disjoint nonempty subsets of

$$Y \times \bigcup_{Y \in \mathcal{Y}} Y.$$ 

By the axiom of choice, there exists a set $Z$ having exactly one element in common with each element of $\mathcal{Z}$. Define the function

$$c : \mathcal{Z} \rightarrow Y \times \bigcup_{Y \in \mathcal{Y}} Y$$

by $c(Y') = Y' \cap Z$. This function $c$ implicitly provides the rule for a function from $\mathcal{Y}$ to the set $\bigcup_{Y \in \mathcal{Y}} Y$ such that $y$ belongs to $Y$ whenever $(Y, y) \in Z$. This rule is the desired choice function.

A.1.2 Well-Ordered Sets

A simple order $<$ on a set $X$ is a relation such that, for all $x, y, z \in X$,

1. if $x \neq y$ then either $x < y$ or $y < x$
2. if $x < y$ then $x \neq y$
3. if $x < y$ and $y < z$ then $x < z$.

**Definition A.1.3.** A set $X$ with an order relation $<$ is said to be well-ordered if every nonempty subset of $X$ has a smallest element.

The set of natural numbers, for example, is well-ordered. On the other hand, the set of integers is not well-ordered.
Fact A.1.4 (Well-ordering theorem). If $X$ is a set, there exists an order relation on $X$ that is a well-ordering.

This theorem was proved by Zermelo using the axiom of choice. It startled the mathematical community in 1904 and spurred much controversy about the axiom of choice. It is given here without a proof.

Corollary A.1.5. There exists an uncountable well-ordered set.

Definition A.1.6. Let $X$ be an ordered set. Given $x \in X$, the set

$$Y_x = \{ y \in Y | y < x \}$$

is called the section of $X$ by $x$.

Corollary A.1.7. There exists an uncountable well-ordered set, every section of which is countable.

The well-ordering principle is a necessary tool in proofs by induction when the set over which the induction process is applied is not a segment of the natural numbers; this is the so-called transfinite induction.

A.1.3 The Maximum Principle

A strict partial order $\prec$ on a set $X$ is a relation such that for all $x, y, z \in X$

1. if $x \prec y$ then $x \neq y$

2. if $x \prec y$ and $y \prec z$ then $x \prec z$.

A strict partial order is similar to a simple order, except that it need not be true that for every distinct $x, y \in X$, either $x \prec y$ or $y \prec x$.

Fact A.1.8 (The maximum principle). Let $X$ be a set and suppose that $\prec$ is a strict partial order on $X$. If $Y$ is a subset of $X$ that is simply ordered by $\prec$, then there exists a maximal simply ordered subset $Z$ of $X$ containing $Y$.

The maximum principle is given here without a proof. It is interesting to note that the well-ordering theorem and the maximum principle are equivalent; either of
them implies the other. Furthermore, each of them is equivalent to the axiom of choice.

Let $\prec$ be a strict partial order on $X$. For $x, y \in X$, the relation $x \preceq y$ holds if $x \prec y$ or $x = y$. The relation $\preceq$ so defined is called a partial order on $X$. For example, the inclusion relation $\subset$ on a collection of sets is a partial order, whereas proper inclusion is a strict partial order.
Bibliography

Index

applications, 95
  linear regression, 95
  Wiener-Hopf, 97

Banach space
  strictly convex, 116

eigenvalues, 157
  algebraic multiplicity, 158
  characteristic polynomial, 158
  defective, 163
  diagonalizable, 159
  eigenspace, 158
  eigenvalue, 157
  eigenvector, 157
  generalized eigenspace, 164
  generalized eigenvector, 165
  geometric multiplicity, 158
  Jordan chain, 165
  Jordan normal form, 164
  similar, 160
  spectrum, 157

domain, 20
  global minimum value, 115
  image, 20
  injective, 20
  inverse function, 20
  inverse image, 20
  one-to-one, 20
  one-to-one correspondence, 20
  onto, 20
  preimage, 20
  surjective, 20

inner-product space, 69
  adjoint, 141
  best approximation, 83
  Cauchy-Schwarz inequality, 73
  dual approximation, 100
  Euclidean space, 71
  Gram-Schmidt orthogonalization, 76
  half space, 105
  Hilbert space, 78
  induced norm, 72
  inner product, 68
  least-squares, 91
  normal equations, 89
  orthogonal, 71, 74, 77
  orthogonal complement, 77
  orthogonal set, 74
orthonormal basis, 78
Parseval identity, 78
projection, 72
Riesz representation theorem, 140
standard inner product, 69
unitary, 77
integral, 65
almost everywhere, 64
Lebesgue integral, 64, 65
Lebesgue measure, 64
Riemann integral, 65
linear transform, 58
algebra, 131
Banach algebra, 131
bounded, 136
coordinate matrix, 60
idempotent, 86
invertible, 131
linear operator, 130
non-singular, 59
nullity, 61
nullspace, 61
operator norm, 135
orthogonal projection, 87
projection, 86
pseudoinverse, 146
range, 60
rank, 61
singular, 59
transpose, 134
vector product, 131
logic, 1
biconditional, 4
complete, 9
conditional connective, 3, 4
conjecture, 1
conjunction, 2
consistent, 9
contradiction, 5
contrapositive, 9
converse, 7
corollary, 12
decidable, 9
disjunction, 3
existence quantifier, 10
fallacy, 9
free variable, 10
implication relation, 4
lemma, 12
logical equivalence, 8
logical implication, 6
mathematical induction, 14
negation, 3
predicate, 10
proof, 1
proposition, 12
semidecidable, 12
tautology, 5
theorem, 12
universal instantiation, 10
universal quantifier, 10
matrix
compact SVD, 173
convergent, 166
elementary column operation, 50
elementary row operation, 50
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frobenius norm</td>
<td>140</td>
</tr>
<tr>
<td>Gramian</td>
<td>90</td>
</tr>
<tr>
<td>Hermitian transpose</td>
<td>49</td>
</tr>
<tr>
<td>inverse</td>
<td>50</td>
</tr>
<tr>
<td>invertible</td>
<td>50</td>
</tr>
<tr>
<td>matrix product</td>
<td>49</td>
</tr>
<tr>
<td>orthogonal</td>
<td>156</td>
</tr>
<tr>
<td>positive-definite</td>
<td>90</td>
</tr>
<tr>
<td>positive-semidefinite</td>
<td>90</td>
</tr>
<tr>
<td>projection matrix</td>
<td>93</td>
</tr>
<tr>
<td>pseudoinverse</td>
<td>93</td>
</tr>
<tr>
<td>reduced row echelon form</td>
<td>50</td>
</tr>
<tr>
<td>row echelon form</td>
<td>49</td>
</tr>
<tr>
<td>spectral radius</td>
<td>139</td>
</tr>
<tr>
<td>trace</td>
<td>80</td>
</tr>
<tr>
<td>transpose</td>
<td>49</td>
</tr>
<tr>
<td>unitary</td>
<td>156</td>
</tr>
<tr>
<td>matrix factorization</td>
<td>147</td>
</tr>
<tr>
<td>backward substitution</td>
<td>148</td>
</tr>
<tr>
<td>Cholesky factorization</td>
<td>154</td>
</tr>
<tr>
<td>forward substitution</td>
<td>147</td>
</tr>
<tr>
<td>LDLT decomposition</td>
<td>154</td>
</tr>
<tr>
<td>lower triangular</td>
<td>147</td>
</tr>
<tr>
<td>LU decomposition</td>
<td>149</td>
</tr>
<tr>
<td>orthogonal</td>
<td>155</td>
</tr>
<tr>
<td>unit triangular</td>
<td>147</td>
</tr>
<tr>
<td>unitary</td>
<td>155</td>
</tr>
<tr>
<td>upper triangular</td>
<td>147</td>
</tr>
<tr>
<td>metric space</td>
<td>24</td>
</tr>
<tr>
<td>$d$-open ball</td>
<td>26</td>
</tr>
<tr>
<td>boundary</td>
<td>29</td>
</tr>
<tr>
<td>Cauchy sequence</td>
<td>26</td>
</tr>
<tr>
<td>closed</td>
<td>27</td>
</tr>
<tr>
<td>closure</td>
<td>29</td>
</tr>
<tr>
<td>compact</td>
<td>37</td>
</tr>
<tr>
<td>complete</td>
<td>34</td>
</tr>
<tr>
<td>completion</td>
<td>35</td>
</tr>
<tr>
<td>continuous</td>
<td>29</td>
</tr>
<tr>
<td>contraction</td>
<td>35</td>
</tr>
<tr>
<td>converges</td>
<td>26</td>
</tr>
<tr>
<td>dense</td>
<td>35</td>
</tr>
<tr>
<td>distance</td>
<td>26</td>
</tr>
<tr>
<td>Euclidean metric</td>
<td>25</td>
</tr>
<tr>
<td>interior</td>
<td>28</td>
</tr>
<tr>
<td>isolated point</td>
<td>28</td>
</tr>
<tr>
<td>isometry</td>
<td>35</td>
</tr>
<tr>
<td>limit</td>
<td>30</td>
</tr>
<tr>
<td>limit point</td>
<td>28</td>
</tr>
<tr>
<td>Lipschitz continuous</td>
<td>30</td>
</tr>
<tr>
<td>metric</td>
<td>25</td>
</tr>
<tr>
<td>open</td>
<td>27</td>
</tr>
<tr>
<td>points</td>
<td>26</td>
</tr>
<tr>
<td>pointwise convergence</td>
<td>32</td>
</tr>
<tr>
<td>sequence</td>
<td>26</td>
</tr>
<tr>
<td>totally bounded</td>
<td>37</td>
</tr>
<tr>
<td>uniform convergence</td>
<td>32</td>
</tr>
<tr>
<td>uniformly continuous</td>
<td>30</td>
</tr>
<tr>
<td>optimization</td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>119</td>
</tr>
<tr>
<td>convex</td>
<td>126</td>
</tr>
<tr>
<td>feasible</td>
<td>118</td>
</tr>
<tr>
<td>Fréchet derivative</td>
<td>111</td>
</tr>
<tr>
<td>Fréchet differentiable</td>
<td>111</td>
</tr>
<tr>
<td>Gâteaux differentiable</td>
<td>111</td>
</tr>
<tr>
<td>Gâteaux differential</td>
<td>110</td>
</tr>
<tr>
<td>gradient</td>
<td>111</td>
</tr>
<tr>
<td>Jacobian matrix</td>
<td>111</td>
</tr>
</tbody>
</table>

**Note:** The page numbers are approximate and may not align exactly with the original document due to the nature of the conversion process.
Lagrange multiplier, 119
Lagrangian, 119
Lagrangian dual, 123
linear program, 119
local minimum value, 115
locally optimal, 119
objective function, 118
optimal value, 119
Slater’s condition, 126
standard form, 118
strong duality, 125
weak duality, 124
rational numbers, 16
real numbers, 15
Russell’s Paradox, 16
set, 15
set difference, 17
set-builder notation, 15
simple order <, 176
singleton, 15
strict partial order, 177
subset, 17
supremum, 30
uncountably infinite, 16
union, 17
well-ordered, 176
topology, 39
basis, 39
closed, 40
closure, 40
continuous, 41
converge, 43
dense, 41
extended real numbers, 30
interior, 40
limit point, 41
metric topology, 39
metrizable, 40
neighborhood, 41
open set, 39
separable, 41, 68
vector space, 51, 68
affine hyperplane, 105
Banach space, 65
best approximation, 83
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>closed subspace</td>
<td>66</td>
</tr>
<tr>
<td>convex set</td>
<td>101</td>
</tr>
<tr>
<td>coordinate vector</td>
<td>57</td>
</tr>
<tr>
<td>dimension</td>
<td>56</td>
</tr>
<tr>
<td>direct sum</td>
<td>53</td>
</tr>
<tr>
<td>dual basis</td>
<td>133</td>
</tr>
<tr>
<td>dual space</td>
<td>132</td>
</tr>
<tr>
<td>finite-dimensional</td>
<td>54</td>
</tr>
<tr>
<td>functional</td>
<td>115</td>
</tr>
<tr>
<td>Hamel basis</td>
<td>54</td>
</tr>
<tr>
<td>Hilbert spaces</td>
<td>68</td>
</tr>
<tr>
<td>homomorphism</td>
<td>132</td>
</tr>
<tr>
<td>hyperplane</td>
<td>104</td>
</tr>
<tr>
<td>isomorphism</td>
<td>132</td>
</tr>
<tr>
<td>linear combination</td>
<td>52</td>
</tr>
<tr>
<td>linear functional</td>
<td>79</td>
</tr>
<tr>
<td>linear transform</td>
<td>58</td>
</tr>
<tr>
<td>linearly dependent</td>
<td>53</td>
</tr>
<tr>
<td>linearly independent</td>
<td>53</td>
</tr>
<tr>
<td>norm</td>
<td>62</td>
</tr>
<tr>
<td>normalized</td>
<td>65</td>
</tr>
<tr>
<td>ordered basis</td>
<td>57</td>
</tr>
<tr>
<td>Schauder basis</td>
<td>66</td>
</tr>
<tr>
<td>span</td>
<td>53</td>
</tr>
<tr>
<td>standard basis</td>
<td>54</td>
</tr>
<tr>
<td>standard Schauder basis</td>
<td>66</td>
</tr>
<tr>
<td>subspace</td>
<td>52</td>
</tr>
<tr>
<td>unit vector</td>
<td>65</td>
</tr>
</tbody>
</table>