Fundamentals of Mathematical Proofs

TU152: Fundamental Mathematics

Saifon Chaturantabut

Department of Mathematics and Statistics
Thammasat University

Outline

Introduction

A mathematical system consists of axioms, definitions, and undefined terms.

- An **axiom** is a statement that is assumed to be true.
- A **definition** is used to create new concepts in terms of existing ones.
- A **theorem** is a statement that has been proved to be true.
- A **lemma** is a theorem that is usually not interesting in its own right but is useful in proving another theorem.
- A **corollary** is a theorem that follows quickly from a theorem.
- Less important theorems are sometimes called **propositions**.
- A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Introduction to Proof

Example: The Euclidean geometry furnishes an example of mathematical system:

- "Points" and "lines" are examples of undefined terms.
- An example of a **definition**: Two angles are supplementary if the sum of their measures is 180°:
- An example of an **axiom**: Given two distinct points, there is exactly one line that contains them.
- An example of a **theorem**: If two sides of a triangle are equal, then the angles opposite them are equal.
- An example of a **corollary**: If a triangle is equilateral, then it is equiangular.

An argument that establishes the truth of a theorem is called a **proof**.
Logic is a tool for the analysis of proofs.

Definitions

In order to evaluate the truth or falsity of a statement, you must understand what the statement is about. I.e., you must know the meanings of all terms that occur in the statement. Mathematicians define terms very carefully and precisely and consider it important to learn definitions virtually word for word.

Definition (Even and Odd Integers)

- An integer n is **even** if, and only if, n equals twice some integer.
- An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even } \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k.$$

$$n \text{ is odd } \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

Example: (Even and Odd Integers) Use the definitions of even and odd to justify your answers to the following questions.

a. Is 0 even?
b. Is -301 odd?
c. If a and b are integers, is $6ab$ even?
d. If a and b are integers, is $10a + 8b + 1$ odd?
e. Is every integer either even or odd?

Definitions

Definition (Prime & Composite numbers)

An integer n is **prime** if, and only if,

- $n > 1$ and
- for all positive integers r and s, if $n = rs$, then either r or s equals n.

An integer n is **composite** if, and only if,

- $n > 1$ and
- $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

$$\boxed{n \text{ is prime}} \Leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs$$
$$\text{then either } \boxed{r = 1 \text{ and } s = n} \text{ or } \boxed{r = n \text{ and } s = 1}.$$

$$\boxed{n \text{ is composite}} \Leftrightarrow \exists \text{ positive integers } r \text{ and } s, \text{ if } n = rs$$
$$\text{then } \boxed{1 < r < n} \text{ and } \boxed{1 < s < n}.$$

Definitions

Example: (Prime and Composite Numbers)

1. Is 1 prime?
2. Is every integer greater than 1 either prime or composite?
3. Write the first six prime numbers.
4. Write the first six composite numbers.

Proving Existential Statements

Consider existential statements in the form

$$\exists x \in D \text{ such that } Q(x).$$

- Existential statement is **true** if, and only if, $Q(x)$ is true for *at least one* x in D. The existential statements can be proved by the following methods.
  1. **"Constructive proofs of existence"**
     - *Finding an x in D that makes $Q(x)$ true,* or
     - *Giving a set of directions for finding such an x.*
  2. **"Nonconstructive proof of existence "**
     - Showing that that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem, or
     - Showing that the assumption that there is no such x leads to a contradiction.

  The disadvantage of a nonconstructive proof is that it may give virtually no clue about where or how x may be found.
- Existential statement is **false** if, and only if, its **negation** in the form of **universal statement is true**.

Constructive Proof

First we discuss methods for proving a theorem of the form

$$\exists x, \quad \text{such that} \;\; P(x).$$

- This theorem guarantees the existence of at least one x for which the predicate $P(x)$ is true.
- The proof of such a theorem is constructive: that is, the proof is either by finding a particular x that makes $P(x)$ true or by exhibiting an algorithm for finding x.

Example: Show that there exists a positive integer whose square can be written as the sum of the squares of two positive integers.

Answer: One example is

Example: Show that there exists an integer x such that $x^2 = 15,129$.

Answer:

Constructive Proof

Example:

1. Prove that:
   "there exists an even integer n that can be written in two different ways as a sum of two prime numbers."
2. Suppose that r and s are integers. Prove that:
   " there is an integer k such that $22r + 18s = 2k$."

Existential Statements

Remarks on Existential Statements:

- A **nonconstructive existence proof** is a method that involves either showing the existence of x using a proved theorem (or axioms) or the assumption that there is no such x leads to a contradiction. The disadvantage of nonconstructive method is that it may give virtually no clue about where or how to find x. We will look at this method later in this class.
- To disprove a existential statement,

  $$\exists x \in D, Q(x)$$

  we can show that its negation

  $$\forall x \in D, \sim Q(x)$$

  is true. So, we will next consider the methods for proving the universal "∀" statements.

Proving Universal "∀" Statements

Consider a **universal statement** of the form:

$$\forall x \in D, P(x).$$

Two main methods for proving this type of statements are:

1. **Method of Exhaustion**

   ⇒ This should be used when D is finite or
   when only a finite number of elements satisfy $P(x)$.
   ⇒ In practice, it may be infeasible or impractical to use the method of exhaustion, especial when D is an infinite set.

2. **Method of Generalizing from the Generic Particular**

   ⇒ This technique for proving a universal statement works regardless of the size of the domain D.

Note: To **disprove** a universal statement, we can use a **counterexample**. I.e. show that its negation $\boxed{\exists x \in D, \sim P(x)}$ is true.

Method of Exhaustion

Method of exhaustion
Consider a statement of the form

$$\forall x \in D, P(x).$$

- If the domain D is a finite set, then one checks the truth value of $P(x)$ for each $x \in D$:
  - The statement is **true** if $P(x)$ is true for **every** $x \in D$.
  - The statement is **false** if $P(a)$ is false for *at least one* element $a \in D$.

  $\Rightarrow$ The element $a \in D$ is called a **counterexample**.

Method of Exhaustion

Example: Show that for each integer $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $n^2 - n + 11$ is a prime number.

Answer:

Method of Exhaustion

Example: Use the method of exhaustion to prove the following statement:

$\forall n \in \mathbb{Z}$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

Answer:

Method of Generalizing from the Generic Particular

Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen element* of the set, and show that x satisfies the property.

- This technique can be used for proving a universal statement it works regardless of the size of the domain over which the statement is quantified.
- When the method of generalizing from the generic particular is applied to a property of the form:

$$\forall x \in D, \text{if } P(x) \text{ then } Q(x)$$

where
  - $P(x)$ is the hypothesis and
  - $Q(x)$ is the conclusion,

the result is the method of **direct proof**.

Method of Generalizing from the Generic Particular: Direct Proof

Consider a universal conditional statement of the form:

$$\forall x \in D, \text{if } P(x) \text{ then } Q(x)$$

- Recall that: the only way an if-then statement can be false is for the hypothesis to be true and the conclusion to be false.
- Therefore, we can prove that the statement "If $P(x)$ then $Q(x)$" is true *if we can show that the truth of $P(x)$ implies the truth of $Q(x)$, then we will have proved the statement.*

Method of Direct Proof

1. Express the statement to be proved in the form

   "$\forall x \in D$, if $P(x)$ then $Q(x)$."

2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. I.e.

   "Suppose $x \in D$ and $P(x)$ is true."

3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Method of Generalizing from the Generic Particular:Direct Proof

Example: Prove that:

"The sum of any two even integers is even."

Proof:

Example: Disprove the statement:

$$\forall a, b \in \mathbb{R}, \text{ if a} < \text{b, then a}^2 < \text{b}^2.$$

Answer:

Method of Generalizing from the Generic Particular

Summary:
In order to use the *method of generalizing from the generic particular* for

proving
$$\forall x \in D, P(x)$$
or disproving
$$\exists x \in D, Q(x),$$

it is helpful to use the following three steps:

1. Restate the claim in a **formal** way.
2. Specify the **starting point**.
3. Identify **the conclusion to be shown**.

Method of Generalizing from the Generic Particular

Example: (Disproving an Existential Statement)
Disprove the following statement:

$$\text{There is a positive integer } n \text{ such that } n^2 + 3n + 2 \text{ is prime.}$$

Rational Numbers

Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational**. More formally, if r is a real number, then

$$r \text{ is rational } \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b}, b \neq 0.$$

Note: The word *rational* contains the word *ratio*, which is another word for *quotient*. A *rational number* can be written as a *ratio* of integers.

Example: Determine whether the following numbers are rational or irrational.

1. 0
2. $10/3$
3. $-\frac{3}{47}$
4. 0.1234
5. $0.12121212\ldots$ (where the digits 12 are assumed to repeat forever)

Rational Numbers

Example: Prove the following theorem.

Theorem

The sum of any two rational numbers is rational.

Rational Numbers

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example:

Corollary

The double of a rational number is rational.

More Methods of Proof

Vacuous Proof

A **vacuous proof** is a proof of an implication $p \to q$ in which it is shown that p is false.

Example Use the method of vacuous proof to show that if $x \in \emptyset$, then David is playing soccer.
Answer:

Trivial Proof

A **trivial proof** of an implication $p \to q$ is one in which q is shown to be true without any reference to p.

Example Use the method of trivial proof to show that if n is an even integer then n is divisible by 1.
Answer:

More Methods of Proof: Method of proof by cases

Method of Proof by Cases

The method of proof by cases is a direct method of proving the conditional statement

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \to q.$$

The method consists of proving the conditional statements

$$p_1 \to q, p_2 \to q, \ldots, p_n \to q.$$

To prove a statement of the form

"If $A1$ or $A2$ or ... or A_n, then C"

we have to prove all of the following:

- If A_1, then C,
- If A_2, then C,

  ⋮

  ⋮
- If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Method of Proof by Cases

Example: Proof the following statement.

If n is a positive integer, then $n^3 + n$ is even.

Method of Proof by Cases:Absolute value example

Definition (Absolute Value)

For any real number x, the absolute value of x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} -x, & x < 0 \\ x, & x \geq 0 \end{cases}$$

Example: Use the proof by cases to prove the triangle inequality:
For all real numbers x and y,

$$|x + y| \leq |x| + |y|.$$

Example: (Continued)

Floor $\lfloor x \rfloor$ and Ceiling $\lceil x \rceil$

Definition (Floor)

Given any real number x, the floor of x, denoted $\lfloor x \rfloor$, is defined as:

$$\lfloor x \rfloor = n, \quad n \text{ is an integer such that } n \leq x < n + 1.$$

Symbolically, if x is a real number,

$$\boxed{\lfloor x \rfloor = n \;\Leftrightarrow\; n \in \mathbb{Z},\; n \leq x < n + 1.}$$

Definition (Ceiling)

Given any real number x, the ceiling of x, denoted $\lceil x \rceil$, is defined as:

$$\lceil x \rceil = n, \quad n \text{ is an integer such that } n - 1 < x \leq n.$$

Symbolically, if x is a real number,

$$\boxed{\lceil x \rceil = n \;\Leftrightarrow\; n \in \mathbb{Z},\; n - 1 < x \leq n.}$$

Floor $\lfloor x \rfloor$ and Ceiling $\lceil x \rceil$

Example: Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ of the following values of x.

1. $x = 37.999$
2. $x = 11$
3. $x = 0.6$
4. $x = -\frac{57}{2}$
5. $x = -14.001$

Floor $\lfloor x \rfloor$ and Ceiling $\lceil x \rceil$

Example: Use the proof by a counterexample to show that the statement

$$\text{“}\forall x, y \in \mathbb{R}, \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor\text{”}$$

is **false**.

Answer:

Floor $\lfloor x \rfloor$ and Ceiling $\lceil x \rceil$

Example: Use the method of proof by cases to prove the following statement.

Let n be an integer. Then

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}.$$

Indirect Proof

Indirect Proof

1. **Method of Proof by Contradiction**
2. **Method of Proof by Contrapositive**

Proof by Contradiction

Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Example: If a man accused of holding up a bank can prove that he was some place else at the time the crime was committed, he will certainly be acquitted. The logic of his defense is as follows:

```
Suppose I did commit the crime.  Then at the time of the crime,
I would have had to be at the scene of the crime.  In fact, at
the time of the crime I was in a meeting with 20 people far from
the crime scene, as they will testify.  This contradicts the
assumption that I committed the crime since it is impossible to
be in two places at one time.  Hence that assumption is false.
```

Proof by Contradiction

Example: Use proof by contradiction to show that

> There is no greatest integer.

Proof:

Proof by Contradiction

Example: Use proof by contradiction to show the following statement is true.

> There is no integer that is both even and odd.

Proof:

Proof by Contradiction

Example: Use proof by contradiction to show the following statement is true.

> The sum of any rational number and any irrational number is irrational.

Proof:

Method of Proof by Contraposition

To prove a statement by contraposition, you take the contrapositive of the statement, prove the contrapositive by a direct proof, and conclude that the original statement is true.

Method of Proof by Contraposition

1. Express the statement to be proved in the form
$$\forall x \in D, \text{ if } P(x), \text{ then } Q(x).$$
(This step may be done mentally.)
2. Rewrite this statement in the contrapositive form
$$\forall x \in D, \text{ if } Q(x) \text{ is false, then } P(x) \text{ is false.}$$
(This step may also be done mentally.)
3. Prove the contrapositive by a **direct proof**.
   (i) Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.
   (ii) Show that $P(x)$ is false.

Proof by Contraposition

Example: Use proof by *contraposition* to show the following statement is true.

For all integers n, if n^2 is even, then n is even.

Proof:

Relation between Proof by Contradiction and Proof by Contraposition

- Proof by contraposition can only be used to prove the statements that are *universal* and *conditional*, i.e.

$$\forall x \in D, \text{ if } P(x), \text{ then } Q(x).$$

- Any proof by *contraposition* can be done by *contradiction*. I.e. Consider

$$\forall x \in D, \text{ if } P(x), \text{ then } Q(x).$$

  - Using proof by contraposition: $\forall x \in D, \text{ if } Q(x) \text{ is false, then } P(x) \text{ is false.}$

$$\boxed{\text{Suppose for any } x \in D \text{, such that } \sim Q(x)} \rightsquigarrow\rightsquigarrow\rightsquigarrow \boxed{\sim P(x)}$$

  - Using proof by contradiction:

$$\boxed{\text{Suppose } \exists x \in D \text{, such that } P(x) \text{ and } \sim Q(x)} \rightsquigarrow\rightsquigarrow\rightsquigarrow \boxed{\underbrace{P(x) \text{ and } \sim P(x)}_{\text{CONTRADICTION!}}}$$

- Some statements can be proved by contradiction but not by contraposition, such as the statement

"$\sqrt{2}$ is irrational."

- In proof by contradiction, it may be difficult to know what contradiction to head for (in the proof by contraposition, you know exactly what conclusion you need to show, namely the negation of the hypothesis).

Example: Use proof by *contradiction* to show the following statement is true.

For all integers n, if n^2 is even, then n is even.

Proof:

Example: Proof that

$\sqrt{2}$ is irrational.

Proof:
[We take the negation and suppose it to be true.] Suppose not. That is, suppose $\sqrt{2}$ is rational Then there are integers m and n with **no common factors** such that

$$\sqrt{2} = \frac{m}{n}$$

[by dividing m and n by any common factors if necessary]. [We must derive a contradiction.] Squaring both sides of equation above gives

$$2 = \frac{m^2}{n^2}$$

$$m^2 = 2n^2$$

which implies that m^2 is even (by definition of even). It follows that m is even (by Proposition 4.6.4). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k$$

for some integer k. we see that

$$m2 = (2k)^2 = 4k^2 = 2n^2.$$

Dividing both sides of the right-most equation by 2 gives $n^2 = 2k^2$. Consequently, n^2 is even, and so n is even (by Proposition 4.6.4). But we also know that m is even. [This is the fact we filed away.] **Hence both m and n have a common factor of 2. But this contradicts the supposition that m and n have no common factors.** [Hence the supposition is false and so the theorem is true.] ■