Fundamentals of Mathematical Proofs

TU152: Fundamental Mathematics

Saifon Chaturantabut

Department of Mathematics and Statistics
TU

1/2014

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:

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

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

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 "$\forall$" 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**

   $\Rightarrow$ This should be used when D is finite or
   when only a finite number of elements satisfy $P(x)$.
   $\Rightarrow$ 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**

   $\Rightarrow$ 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: