AE1MCS: Mathematics for Computer Scientists

Huan Jin, Heshan Du
University of Nottingham Ningbo China

Aim and Learning Objectives

- To be able to understand different methods of proving theorems.
- To be able to apply different methods to construct proofs.

Reading

Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, 7th Edition, 2013.

- Chapter 1, Section 1.8. Introduction to Proofs
- Chapter 5, Section 5.1. Mathematical Induction
- Chapter 5, Section 5.2. Strong Induction

Methods of Proving Theorems

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction
- Proof by Induction
- ...

Direct Proof and Indirect Proof

If a proof leads from the premises of a theorem to the conclusion, then it is a direct proof, otherwise, it is an indirect proof.

- Important true propositions are called *theorems*.
- A *lemma* is a preliminary proposition useful for proving later propositions.
- A *corollary* is a proposition that follows in just a few logical steps from a theorem.

Direct Proof

A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that

$$\text{if } p \text{ is true, then } q \text{ must also be true,}$$

so that the combination p true and q false never occurs.

Direct Proof

In a direct proof,

1. we assume that p is true,
2. then, we use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Exercise

Give a direct proof of the theorem 'If n is an odd integer, then n^2 is odd'.

Even and Odd

Definition (Even and Odd)

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

Exercise Answer

Give a direct proof of the theorem ‘If n is an odd integer, then n^2 is odd’.

Proof.

Suppose n is an odd integer. Then there exists an integer k such that $n = 2k + 1$. $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, n^2 is odd. $\square$

Proof by Contraposition

- An extremely useful type of indirect proof is known as proof by contraposition.
- Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$.
- The conditional statement $p \to q$ is proved by showing that its contrapositive, $\neg q \to \neg p$, is true.

Exercise

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Exercise Answer

Prove that if n is an integer and $3n+2$ is odd, then n is odd.

Proof.

To prove that if n is an integer and $3n+2$ is odd, then n is odd, we show if n is an even integer, then $3n+2$ is even.

Suppose n is an even integer. Then there exists an integer k such that $n = 2k$. $3n+2 = 3 \times 2k + 2 = 2 \times (3k+1)$. Since $3k+1$ is an integer, $3n+2$ is even.

By contraposition, we showed that if n is an integer and $3n+2$ is odd, then n is odd. $\square$

Proof by Contradiction

- Suppose we want to prove that a statement p is true.
- Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true.
- Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

Proof by Contradiction

- Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r.
- Proofs of this type are called **proofs by contradiction.**
- A proof by contradiction is another type of indirect proof.

Exercise

Prove that $\sqrt{2}$ is irrational.

Exercise Answer

Prove that $\sqrt{2}$ is irrational.

Proof.

Suppose $\sqrt{2}$ is rational. Then there exist integers p and q with $q \neq 0$ such that $\sqrt{2} = p/q$ and p and q do not have any common factor. Thus, $2 = p^2/q^2$. $p^2 = 2q^2$. Thus, p^2 is even. Since if n is odd, then n^2 is odd (proved in previous slides), p is even. Hence there exists an integer k such that $p = 2k$. Then $p^2 = (2k)^2 = 2q^2$. $q^2 = 2k^2$. Thus q^2 is even, hence q is even. Thus, p and q are both even, which contradicts the fact that p and q do not have any common factor. □

Proof of Equivalence

To prove a theorem that is a biconditional statement or a bi-implication, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Proof of Equivalence

Sometimes a theorem states that several propositions are equivalent. Such a theorem states that propositions $p_1, p_2, p_3, ..., p_n$ are equivalent. This can be written as

$$p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n,$$

which states that all n propositions have the same truth values, and consequently, that for all i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$, p_i and p_j are equivalent. One way to prove these mutually equivalent is to use the tautology

$$[p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge ... \wedge (p_n \rightarrow p_1)].$$

This shows that if the n conditional statements $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$,..., $p_n \rightarrow p_1$ can be shown to be true, then the propositions p_1, p_2,..., p_n are all equivalent.

Counterexamples

To show that a statement of the form $\forall x\, P(x)$ is false, we need only find a counterexample, that is, an example x for which $P(x)$ is false.

Exercise

Show that the statement ‘Every positive integer is the sum of the squares of two integers’ is false.

Exercise

Show that the statement ‘Every positive integer is the sum of the squares of two integers’ is false.

Proof.

3 is a positive integer but is not the sum of the squares of two integers. Note that the only perfect squares not exceeding 3 are $0^2 = 0$ and $1^2 = 1$. Therefore, the statement ‘Every positive integer is the sum of the squares of two integers’ is false. $\square$

Proof by Cases

- Sometimes we cannot prove a theorem using a single argument that holds for all possible cases.
- Need to consider different cases separately.
- **Rationale:** To prove a conditional statement of the form

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

can be used as a rule of inference.

Proof by Cases

- The original conditional statement with a hypothesis made up of a disjunction of the propositions p_1, p_2,..., p_n can be proved by proving each of the n conditional statements $p_i \rightarrow q$, $i = 1, 2, ..., n$, individually. Such an argument is called a **proof by cases.**
- A proof by cases must cover **all possible cases** that arise in a theorem.

Exercise

Prove that if n is an integer, then $n^2 \geq n$.

Exercise

Prove that if n is an integer, then $n^2 \geq n$.

Proof.

Let us prove by cases.

- If $n = 0$, then $0^2 \geq 0$.
- If $n \geq 1$, we multiply both sides of the inequality $n \geq 1$ by the positive integer n, then we have $n^2 \geq n$.
- If $n \leq -1$, $n^2 \geq n$ holds, since $n^2 \geq 0$.

Thus, in each case, $n^2 \geq n$. □

Induction

In general, mathematical induction can be used to prove statements that assert that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function.

Proofs using mathematical induction have two parts.

1. **Basis Step:** We show that the statement holds for the positive integer 1 (i.e. $P(1)$ is true).
2. **Inductive Step:** We show that if the statement holds for a positive integer then it must also hold for the next larger integer (i.e. for all positive integers k, if $P(k)$ is true, then $P(k+1)$ is true).

Principle of Mathematical Induction

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

Basis Step: We verify that $P(1)$ is true.

Inductive Step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

Inductive Step

To complete the inductive step of a proof using the principle of mathematical induction,

- we assume that $P(k)$ is true for an *arbitrary* positive integer k
- we show that under this assumption, $P(k+1)$ must also be true.

The assumption that $P(k)$ is true is called the **inductive hypothesis.**

Mathematical Induction

Mathematical induction can be expressed as the following rule of inference

$$\begin{array}{rl} & P(1) \\ & \forall k\,(P(k) \rightarrow P(k+1)) \\ \hline \therefore & \forall n\, P(n) \end{array}$$

where the domain is the set of positive integers.

Detailed Explanations about Mathematical Induction

- The first thing we do to prove that $P(n)$ is true for all positive integers n is to show that $P(1)$ is true.
- This amounts to showing that the particular statement obtained when n is replaced by 1 in $P(n)$ is true.
- Then we must show that $P(k) \rightarrow P(k+1)$ is true for every positive integer k.
- To prove that this conditional statement is true for every positive integer k, we need to show that $P(k+1)$ cannot be false when $P(k)$ is true.
- This can be accomplished by assuming that $P(k)$ is true and showing that *under this hypothesis* $P(k+1)$ must also be true.

Mathematical Induction: Remark

In a proof by mathematical induction it is **not** assumed that $P(k)$ is true for all positive integers!

It is only shown that if it is assumed that $P(k)$ is true, then $P(k+1)$ is also true.

Explanations about Mathematical Induction

When we use mathematical induction to prove a theorem,

- we first show that $P(1)$ is true.
- Then we know that $P(2)$ is true, because $P(1)$ implies $P(2)$.
- Further, we know that $P(3)$ is true, because $P(2)$ implies $P(3)$.
- ...

Continuing along these lines, we see that $P(n)$ is true for every positive integer n.

Using Mathematical Induction

- Mathematical induction can be used to prove statements of the form $\forall n\, P(n)$, where the domain is the set of positive integers.
- Mathematical induction can be used to prove an extremely wide variety of theorems, each of which is a statement of this form.
  - summation formulae, inequalities, identities for combinations of sets, divisibility results, theorems about algorithms, and some other creative results
  - the correctness of computer programs and algorithms

Proving Summation Formulae: Examples

- Show that if n is a positive integer, then $1 + 2 + ... + n = \frac{n(n+1)}{2}$.
- Use mathematical induction to show that $1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.
- Use mathematical induction to prove the inequality $n < 2^n$ for all positive integers n.

Strong Induction

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

Basis Step We verify that the proposition $P(1)$ is true.

Inductive Step We show that the conditional statement $[P(1) \wedge P(2) \wedge ... \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.

Strong Induction

- The difference between mathematical induction and strong induction is the inductive step.
  - Mathematical induction: $\forall k\,(P(k) \rightarrow P(k+1))$.
  - Strong induction: $\forall k\,((P(1) \land P(2) \land ... \land P(k)) \rightarrow P(k+1))$.
- Mathematical induction and strong induction are actually equivalent.
- This is, each can be shown to be a valid proof technique assuming that the other is valid.

Expected Learning Outcomes

- To be able to understand different methods of proving theorems.
- To be able to apply different methods to construct proofs.

Reading

Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, 7th Edition, 2013.

- Chapter 1, Section 1.8. Introduction to Proofs
- Chapter 5, Section 5.1. Mathematical Induction
- Chapter 5, Section 5.2. Strong Induction