

Introduction to Proofs

Section 1.7

Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
 - Proof of the Contrapositive
 - Proof by Contradiction

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs (非形式化证明) which are generally shorter, are generally used.
 - More than one rule of inference are often used in a step.
 - Steps may be skipped.
 - The rules of inference used are not explicitly stated.
 - Easier for to understand and to explain to people.
 - But it is also easier to introduce errors.
- Proofs have many practical applications:
 - verification that computer programs are correct
 - establishing that operating systems are secure
 - enabling programs to make inferences in artificial intelligence
 - showing that system specifications are consistent

Definitions

- A *theorem* (定理) is a statement that can be shown to be true using:
 - definitions
 - other theorems
 - *axioms* (公理) (statements which are given as true)
 - rules of inference
- A *lemma* (引理) is a 'helping theorem' or a result which is needed to prove a theorem.
- A *corollary* (推论) is a result which follows directly from a theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* (猜想) 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.

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

really means

“For all positive real numbers x and y , if $x > y$, then $x^2 > y^2$.”

Proving Theorems

- Many theorems have the form:

$$\forall x (P(x) \rightarrow Q(x))$$
- To prove them, we show that where c is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof* (平凡证明) : If we know q is true, then $p \rightarrow q$ is true as well.

“If it is raining then $1=1$.”

- *Vacuous Proof* (空证明) : If we know p is false then $p \rightarrow q$ is true as well.

“If I am both rich and poor then $2 + 2 = 5$.”

[Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5]

Even and Odd Integers

Definition: 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 $n = 2k + 1$. Note that every integer is either even or odd and no integer is both even and odd.

We will need this basic fact about the integers in some of the example proofs to follow. We will learn more about the integers in Chapter 4.

Proving Conditional Statements: $p \rightarrow q$

- **Direct Proof** (直接证明法) : Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Example: Give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k . Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer. ◀

(◀ marks the end of the proof. Sometimes QED is used instead.)

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number r is *rational* if there exist integers p and q where $q \neq 0$ such that $r = p/q$

Example: Prove that the sum of two rational numbers is rational.

Solution: Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w} \quad \text{where } v = pu + qt, \quad w = qu \neq 0$$

Thus the sum is rational. ◀

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contraposition* (反证法) : Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.

Why does this work?

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

Solution: Assume n is even. So, $n = 2k$ for some integer k . Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even). ◀

Proving Conditional Statements: $p \rightarrow q$

Example: Prove that for an integer n , if n^2 is odd, then n is odd.

Solution: Use proof by contraposition. Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,

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

and n^2 is even (i.e., not odd).

We have shown that if n is an even integer, then n^2 is even. Therefore by contraposition, for an integer n , if n^2 is odd, then n is odd. ◀

Proving Conditional Statements: p

- **Proof by Contradiction** (归谬证明法) : (AKA *reductio ad absurdum*).

To prove p , assume $\neg p$ and derive a contradiction such as $r \wedge \neg r$ (an indirect form of proof). Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true, it follows that the contrapositive $\mathbf{T} \rightarrow p$ also holds.

Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week. Because there are 7 days of the week, we could only have picked 21 days. This contradicts the assumption that we have picked 22 days. ◀

Proof by Contradiction

- A preview of Chapter 4.

Example: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (see Chapter 4). Then

$$2 = \frac{a^2}{b^2} \quad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (an exercise). Since a is even, $a = 2c$ for some integer c . Thus,

$$2b^2 = 4c^2 \quad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b . This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational. ◀

Proof by Contradiction

- A preview of Chapter 4.

Example: Prove that there is no largest prime number.

Solution: Assume that there is a largest prime number. Call it p_n . Hence, we can list all the primes $2, 3, \dots, p_n$. Form

$$r = p_1 \times p_2 \times \dots \times p_n + 1$$

None of the prime numbers on the list divides r . Therefore, by a theorem in Chapter 4, either r is prime or there is a smaller prime that divides r . This contradicts the assumption that there is a largest prime. Therefore, there is no largest prime. ◀

Theorems that are Biconditional Statements

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

Example: Prove the theorem: “If n is an integer, then n is odd if and only if n^2 is odd.”

Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for “if and only if,” as in
 “If n is an integer, then n is odd iff n^2 is odd.”

What is wrong with this?

“Proof” that $1 = 2$

Step	Reason
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Step 5. $a - b = 0$ by the premise and division by 0 is undefined.

Looking Ahead

- If direct methods of proof do not work:
 - We may need a clever use of a proof by contraposition.
 - Or a proof by contradiction.
 - In the next section, we will see strategies that can be used when straightforward approaches do not work.
 - In Chapter 5, we will see mathematical induction and related techniques.
 - In Chapter 6, we will see combinatorial proofs

Homework

- 第8版: Sec. 1.7 7, 8, 36

Proof Methods and Strategy

Section 1.8

Section Summary

- Proof by Cases (分情形证明法)
- Existence Proofs
 - Constructive
 - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions
- Open Problems

Proof by Cases

- To prove a conditional statement of the form:

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

- Use the tautology

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

- Each of the implications $p_i \rightarrow q$ is a case.

Proof by Cases

Example: Let $a @ b = \max\{a, b\} = a$ if $a \geq b$, otherwise $a @ b = \max\{a, b\} = b$.

Show that for all real numbers a, b, c

$$(a @ b) @ c = a @ (b @ c)$$

(This means the operation $@$ is associative.)

Proof: Let a, b , and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases

Case 1: $a \geq b \geq c$

$$(a @ b) = a, a @ c = a, b @ c = b$$

$$\text{Hence } (a @ b) @ c = a = a @ (b @ c)$$

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.



Without Loss of Generality

(不失一般性)

Example: Show that if x and y are integers and both $x \cdot y$ and $x + y$ are even, then both x and y are even.

Proof: Use a proof by contraposition. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m .

Case 1: y is even. Then $y = 2n$ for some integer n , so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n , so $x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd. ◀

We only cover the case where x is odd because the case where y is odd is similar. The use phrase *without loss of generality* (WLOG) indicates this.

Existence Proofs

(存在性证明)



Srinivasa Ramanujan
(1887-1920)

- Proof of theorems of the form $\exists x P(x)$.
- **Constructive** (构造性) existence proof:
 - Find an explicit value of c , for which $P(c)$ is true.
 - Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \quad \blacktriangleleft$$



Godfrey Harold Hardy
(1877-1947)

Nonconstructive Existence Proofs

- In a *nonconstructive* (非构造性) existence proof, we assume no c exists which makes $P(c)$ true and derive a contradiction.

Example: Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$. But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2. \quad \blacktriangleleft$$

Counterexamples (反例)

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$.
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a c such that $\neg P(c)$ is true or $P(c)$ is false.
- In this case c is called a *counterexample* to the assertion $\forall x P(x)$.

Example: “Every positive integer is the sum of the squares of 3 integers.” The integer 7 is a counterexample. So the claim is false.

Uniqueness Proofs (唯一性证明)

- Some theorems assert the existence of a unique element with a particular property, $\exists!x P(x)$. The two parts of a *uniqueness proof* are
 - Existence*: We show that an element x with the property exists.
 - Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence*: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness*: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$. ◀

Proof Strategies for proving $p \rightarrow q$

- Choose a method.
 - First try a direct method of proof.
 - If this does not work, try an indirect method (e.g., try to prove the contrapositive).
- For whichever method you are trying, choose a strategy.
 - First try *forward reasoning*. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q , or start with $\neg q$ and prove $\neg p$.
 - If this doesn't work, try *backward reasoning*. When trying to prove q , find a statement p that we can prove with the property $p \rightarrow q$.

Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let n be the last step of the game.

Step n : Player₁ can win if the pile contains 1, 2, or 3 stones.

Step $n-1$: Player₂ will have to leave such a pile if the pile that he/she is faced with has 4 stones.

Step $n-2$: Player₁ can leave 4 stones when there are 5, 6, or 7 stones left at the beginning of his/her turn.

Step $n-3$: Player₂ must leave such a pile, if there are 8 stones.

Step $n-4$: Player₁ has to have a pile with 9, 10, or 11 stones to ensure that there are 8 left.

Step $n-5$: Player₂ needs to be faced with 12 stones to be forced to leave 9, 10, or 11.

Step $n-6$: Player₁ can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

Universally Quantified Assertions

- To prove theorems of the form $\forall x P(x)$, assume x is an arbitrary member of the domain and show that $P(x)$ must be true. Using UG it follows that $\forall x P(x)$.

Example: An integer x is even if and only if x^2 is even.

Solution: The quantified assertion is

$$\forall x [x \text{ is even} \leftrightarrow x^2 \text{ is even}]$$

We assume x is arbitrary.

Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

So, we have two cases to consider. These are considered in turn.

Continued on next slide →

Universally Quantified Assertions

Case 1. We show that if x is even then x^2 is even using a direct proof (the *only if* part or *necessity*).

If x is even then $x = 2k$ for some integer k .

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

Universally Quantified Assertions

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even then it must be odd. So, $x = 2k + 1$ for some k . Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is odd and hence not even. This completes the proof of case 2.

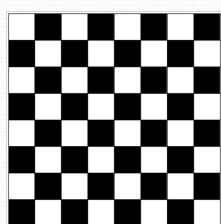
Since x was arbitrary, the result follows by UG.

Therefore we have shown that x is even if and only if x^2 is even. ◀

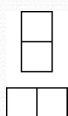
Proof and Disproof: Tilings

Example 1: Can we tile the standard checkerboard using dominos?

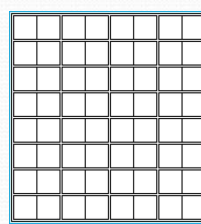
Solution: Yes! One example provides a constructive existence proof.



The Standard Checkerboard



Two Dominoes



One Possible Solution

Tilings

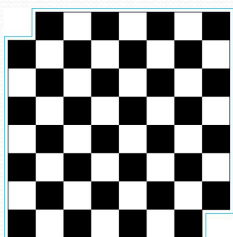
Example 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

Solution:

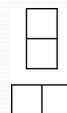
- Our checkerboard has $64 - 1 = 63$ squares.
- Since each domino has two squares, a board with a tiling must have an even number of squares.
- The number 63 is not even.
- We have a contradiction. ◀

Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?



Nonstandard Checkerboard



Dominoes

Continued on next slide →

Tilings

Solution:

- There are 62 squares in this board.
- To tile it we need 31 dominos.
- *Key fact:* Each domino covers one black and one white square.
- Therefore the tiling covers 31 black squares and 31 white squares.
- Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares.
- Contradiction! ◀

The Role of Open Problems

- Unsolved problems have motivated much work in mathematics. Fermat's Last Theorem was conjectured more than 300 years ago. It has only recently been finally solved.

Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no solutions in integers x , y , and z , with $xyz \neq 0$ whenever n is an integer with $n > 2$.

A proof was found by Andrew Wiles in the 1990s.

An Open Problem

- **The $3x + 1$ Conjecture:** Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$. For all positive integers x , when we repeatedly apply the transformation T , we will eventually reach the integer 1.

For example, starting with $x = 13$:

$T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$,
 $T(10) = 10/2 = 5$, $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 16/2 = 8$,
 $T(8) = 8/2 = 4$, $T(4) = 4/2 = 2$, $T(2) = 2/2 = 1$

The conjecture has been verified using computers up to 112589990684262400.

Additional Proof Methods

- Later we will see many other proof methods:
 - Mathematical induction (数学归纳法), which is a useful method for proving statements of the form $\forall n P(n)$, where the domain consists of all positive integers.
 - Structural induction (结构归纳法), which can be used to prove such results about recursively defined sets.
 - Cantor diagonalization (康托尔对角线方法) is used to prove results about the size of infinite sets.
 - Combinatorial proofs (组合证明) use counting arguments.

Exercise

- 第8版: Sec. 1.8 24, 26