# CH.1 The Foundations: Logic and Proofs

## III. Introduction to Proofs

- Methods of Proving Theorems
- Mistakes in Proofs

## Ch. 5 . Induction and Recursion

- Mathematical Induction
- Strong Induction

# II. Introduction to Proofs

In this section we introduce the notion of a proof and describe methods for constructing proofs.

The methods of proof discussed in this chapter are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science. These applications include verifying that computer programs are correct,

A proof is a valid argument that establishes the truth of a theorem

A proof can use the **hypotheses of the theorem**, if any, **axioms** assumed to be true, and previously proven theorems. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

# Understanding How Theorems Are Stated

Many theorems assert that a property holds for all elements in a domain, such as the integers or the real numbers. Although the precise statement of such theorems needs to include a universal quantifier, the standard convention in mathematics is to omit it. **For example**:

"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 $x^2 > y^2$ ."

when theorems of this type are proved, the first step of the proof usually involves selecting a general element of the domain. Subsequent steps show that this element has the property in question. Finally, universal generalization implies that the theorem holds for all members of the domain.

| | |
|---|---|
| $\therefore \dfrac{P(c) \text{ for an arbitrary } c}{\forall x P(x)}$ | Universal generalization |

# • Methods of Proving Theorems

## Proving Conditional Statements: $p \rightarrow q$

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, our goal is to show that $P(c) \rightarrow Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization.

Recall that $p \rightarrow q$ is true unless p is true but q is false.

**Note that**

to prove the statement $p \rightarrow q$,

we need only show that:

q is true if p is true.

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

"If it is raining then 1=1."

- If we know p is false then $p \rightarrow q$ is true as well . **Vacuous Proof**

"If I am both rich and poor then 2 + 2 = 5."

# 1. Direct Proofs

A **direct proof** of a conditional statement p → q is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.

we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, 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**

**Note that** this theorem states ∀n ( P (n) → Q(n)), where P(n) is "n is an odd integer" and Q(n) is "$n^2$ is odd."

we assume that the **hypothesis** of this conditional statement is true, namely, we assume that n is odd. We want to show that $n^2$ is also odd.

By the definition of an odd integer, it follows that n = 2k + 1, where k is some integer. We want to show that $n^2$ is also odd. We can square both sides of the equation n = 2k + 1, we find that

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

By the definition of an odd integer, we can conclude that $n^2$ is an odd integer (it is one more than twice an integer). Consequently, we have proved that if n is an odd integer, then $n^2$ is an odd integer.

**Example**

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

(An integer a is **a perfect square** if there is an integer b such that $a = b^2$)

**Solution**

we assume that m and n are both perfect squares By the definition of a perfect square, it follows that there are integers s and t such that $m = s^2$ and $n = t^2$ by substituting $s^2$ for m and $t^2$ for n into mn

This tells us that

mn = $s^2$ $t^2$ = (ss)(t t ) = (st )(st ) = $(st)^2$ ,
using commutativity and associativity of multiplication.

it follows that mn is also a perfect square, because it is the square of st, which is an integer.

**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

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

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$
$w = qu \neq 0$

Thus the sum is rational.

# 2. Proof by Contraposition

**Proofs by contraposition** make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$.

We take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

sometimes called an **indirect proof method**

**Example**

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

**Solution**

To construct a direct proof, we first assume that $3n + 2$ is an odd integer. This means that $3n + 2 = 2k + 1$ for some integer k. Can we use this fact show that n is odd? We see that $3n + 1 = 2k$, but there does not seem to be any direct way to conclude that n is odd.

The first step in a **proof by contraposition** is to Assume n is even (not odd) . So, n = 2k for some integer k. Thus

3n + 2 = 3(2k) + 2 =6k +2 = 2(3k + 1) = 2j for j = 3k +1

Therefore 3n + 2 is even (not odd).

Since we have shown ¬q → ¬p , p → q must hold as well.

If n is an integer and 3n + 2 is odd (not even) , then n is odd (not even).

**Quiz (1)**

1. **Prove that if** n = ab, where a and b are positive integers, **then** $a \leq \sqrt{n}$ or $a \leq \sqrt{n}$

2. **Prove** that for an integer n, **if** $n^2$ is odd, **then n** is odd.

3. Show that the proposition P(0) is true, where P(n) is :

"If n >1, then $n^2 > n$"

and the domain consists of all integers.

4. Let P(n) be "If a and b are positive integers with a ≥ b, then $a^n \geq b^n$" where the domain consists of all nonnegative integers. Show that P(0) is true.

# 3. Proofs by Contradiction

To prove p, assume ¬p and derive a contradiction such as p ∧ ¬p. Since we have shown that ¬p →F is true , it follows that the contrapositive T→p also holds. Proofs of this type are called **proofs by contradiction**. Because a proof by contradiction does not prove a result directly, it is another type of indirect proof.

**Example**

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

**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 . Then

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

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,

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

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.

PROOFS OF EQUIVALENCE 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. The validity of this approach is based on the tautology:

$$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$$



**Example**

Prove the theorem "If n is an integer, then n is odd if and only if $n^2$ is odd."

**COUNTEREXAMPLES** In Section 1.4 we stated that 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.

**Example**

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

**Solution**

we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers.

note that the only perfect squares not exceeding 3 are 0 $0^2 = 0$ and $1^2 = 1$. Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1.

Consequently, we have shown that "Every positive integer is the sum of the squares of two integers" is false.

# Mistakes in Proofs

Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it.

**Example**

| 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**

We use these steps, where a and b are two equal positive integers.

Every step is valid except for one, step 5 where we divided both sides by a - b. The error is that a - b equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero.

# Ch. 5 . Induction and Recursion

## • Mathematical Induction

Proof methods: direct proof, proof by contraposition, proof by contradiction, disproof by counterexample and **mathematical 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, we complete two steps:

BASIS STEP:

We verify that P (1) is true.

INDUCTIVE STEP:

We show that the conditional statement

P (k) → P (k + 1) is true for all positive integers k.

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 and show that under this assumption, P(k+ 1) must also be true. The assumption that P(k)is true is called the **inductive hypothesis**.

- Expressed as a rule of inference, this proof technique can be stated as

$$(P(1) \wedge \forall k(P(k) \rightarrow P(k+1))) \rightarrow \forall n P(n),$$

when the domain is the set of positive integers.

To prove that $\forall n P(n)$, where $n \in Z^+$ and $P(n)$ is a propositional function, we complete two steps:

1- Basis step: Verify $P(1)$ is true

2-Inductive hypothesis: Assume $P(k)$ is true

3-Inductive step: Show $P(k) \rightarrow P(k+1)$ is true for arbitrary $k \in Z^+$

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.

**Example**

Show that if n is a positive integer, then

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

**Solution**

Let *P (n)* be the proposition that the sum of the first *n* positive integers, $1 + 2 + \cdots n = n(n + 1)/2$ , is $n(n + 1)/2$. We must do two things to prove that *P (n)* is true for $n = 1, 2, 3, \ldots$. Namely, we must show that *P (1)* is true and that the conditional statement *P (k)* implies *P (k + 1)* is true for $k = 1, 2, 3, \ldots$.

BASIS STEP: P (1) is true, because $1 = 1(1 + 1)/2$. (The left-hand side of this equation is 1 because 1 is the sum of the first positive integer. The right-hand side is found by substituting 1 for *n* in n(n + 1)/2.)
INDUCTIVE STEP: For the inductive hypothesis we assume that P (k) holds for an arbitrary positive integer k. That is, we assume that

$$1 + 2 + \cdots + k = k(k + 1)/2$$

Under this assumption, it must be shown that P (k + 1) is true, namely, that

$$1 + 2 + \cdots + k + (k + 1) = \frac{(k + 1)[(k + 1) + 1]}{2} = \frac{(k + 1)(k + 2)}{2}$$

is also true. When we add $k + 1$ to both sides of the equation in $P(k)$, we obtain

$$\begin{aligned} 1 + 2 + \cdots + k + (k + 1) &\overset{\text{IH}}{=} \frac{k(k + 1)}{2} + (k + 1) \\ &= \frac{k(k + 1) + 2(k + 1)}{2} \\ &= \frac{(k + 1)(k + 2)}{2}. \end{aligned}$$

This last equation shows that P (k + 1) is true under the assumption that P (k) is true. This completes the inductive step.

We have completed the basis step and the inductive step, so by mathematical induction we know that P (n) is true for all positive integers n. That is, we have proven that 1 + 2 + · · · + n = n(n + 1)/2 for all positive integers n

**Example**

that the sum of the first n positive odd integers is $n^2$

**Solution**

Let P(n) denote the proposition that the sum of the first n odd positive integers is $n^2$. that is

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

We now attempt to complete these two steps.

*BASIS STEP: P(1) states that the sum of the first one odd positive integer is* $1^2$. This is true because the sum of the first odd positive integer is 1. The basis step is complete.

*INDUCTIVE STEP: To complete the inductive step we must show that the proposition* P(k) → P(k+ 1) is true for every positive integer k. To do this, we first assume the inductive hypothesis. The inductive hypothesis is the statement that P(k) is true for an arbitrary positive integer k, that is,

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

Note that P(k+ 1) is the statement that

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$$

So, assuming that P(k) is true, it follows that

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) &= [1 + 3 + \cdots + (2k - 1)] + (2k + 1) \\ &\overset{\text{IH}}{=} k^2 + (2k + 1) \\ &= k^2 + 2k + 1 \\ &= (k + 1)^2. \end{aligned}$$

This shows that P(k+ 1) follows from P(k). Note that we used the inductive hypothesis P(k) in the second equality to replace the sum of the first k odd positive integers by $k^2$ .

we have shown that P(1) is true and the conditional statement P(k) → P(k+ 1) is true for all positive integers k. Consequently, by the principle of mathematical induction we can conclude that P(n) is true for all positive integers n.

**Example**

Use mathematical induction to show that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers n.

**Solution**

Let P(n) be the proposition that

$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for the integer n.

*BASIS STEP: P(0) is true because* $2^0 = 1 = 2^1 - 1$. This completes the basis step.

*INDUCTIVE STEP: For the inductive hypothesis, we assume that P(k) is true for an arbitrary* nonnegative integer k. That is, we assume that

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1.$$

To carry out the inductive step using this assumption, we must show that when we assume that P(k) is true, then P(k+ 1) is also true. That is, we must show that

$$1+2+2^2+\cdots+2^k+2^{k+1}=2^{(k+1)+1}-1=2^{k+2}-1$$

assuming the inductive hypothesis P(k). Under the assumption of P(k), we see that

$$\begin{aligned}1+2+2^2+\cdots+2^k+2^{k+1} &= (1+2+2^2+\cdots+2^k)+2^{k+1}\\ &\overset{\text{IH}}{=} (2^{k+1}-1)+2^{k+1}\\ &= 2\cdot 2^{k+1}-1\\ &= 2^{k+2}-1.\end{aligned}$$

Note that we used the inductive hypothesis in the second equation in this string of equalities to replace $1 + 2 + 2^2 + \cdots + 2^k$ by $2^{k+1} - 1$. We have completed the inductive step.

**Example**

**Sums of Geometric Progressions** Use mathematical induction to prove this formula for the sum of a finite number of terms of a geometric progression with initial term a and common ratio r:

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1} \qquad \text{when } r \neq 1,$$

where n is a nonnegative integer.

**Solution**

BASIS STEP: P(0) is true, because

$$\frac{ar^{0+1} - a}{r - 1} = \frac{ar - a}{r - 1} = \frac{a(r - 1)}{r - 1} = a.$$

**Inductive hypothesis:** Assume P(k) is true for arbitrary $k \in N$, $a+ar+ar^2.... +ar^k = (ar^{k+1} -a)/(r-1)$

To complete the inductive step we must show that if P(k)is true, then P(k+ 1) is also true. To show that this is the case, we first add a $r^{k+1}$ to both sides of the equality asserted by P(k).We find that

**Lecture 3**

$$a + ar + ar^2 + \cdots + ar^k + ar^{k+1} \overset{\text{IH}}{=} \frac{ar^{k+1} - a}{r - 1} + ar^{k+1}.$$

Rewriting the right-hand side of this equation shows that

$$\begin{aligned}\frac{ar^{k+1} - a}{r - 1} + ar^{k+1} &= \frac{ar^{k+1} - a}{r - 1} + \frac{ar^{k+2} - ar^{k+1}}{r - 1} \\ &= \frac{ar^{k+2} - a}{r - 1}.\end{aligned}$$

Combining these last two equations gives

$$a + ar + ar^2 + \cdots + ar^k + ar^{k+1} = \frac{ar^{k+2} - a}{r - 1}.$$

This shows that if the inductive hypothesis P(k) is true, then P(k+ 1) must also be true. This completes the inductive argument.

# PROVING INEQUALITIES

**Example**

Use mathematical induction to prove the inequality

$n < 2^n$ for all positive integers n.

**Solution**

Let P(n) be the proposition that $n < 2^n$

*BASIS STEP: P(1) is true, because* $1 < 2^1 = 2$. This completes the basis step.
*INDUCTIVE STEP: We first assume the inductive hypothesis that P(k) is true for an arbitrary* positive integer k. That is, the inductive hypothesis P(k)is the statement that $k < 2^k$ To complete the inductive step, we need to show that if P(k) is true, then P(k+ 1), which is the statement that $k+1 < 2^{k+1}$ , is true. we first add 1 to both sides of $k < 2^k$, and then note that $1 < 2^k$ . This tells us that

$$k + 1 \overset{\text{IH}}{<} 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}.$$

This shows that P(k+ 1) is true, namely, that $k+1 < 2^{k+1}$, based on the assumption that P(k) is true. The induction step is complete.

**Example**

Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for n = 1, 2, and 3.)

**Solution**

Let P(n) be the proposition that $2^n < n!$

BASIS STEP: To prove the inequality for n = 4 requires that the basis step be P(4). Note that P(4) is true, because $2^4 = 16 < 24 = 4!$.

INDUCTIVESTEP: For the inductive step, we assume that P(k) is true for an arbitrary integer k with $k \geq 4$. That is, we assume that $2^k < k!$ for the positive integer k with $k \geq 4$. We must show that under this hypothesis, P(k+ 1) is also true.

$$
\begin{aligned}
2^{k+1} &= 2 \cdot 2^k && \text{by definition of exponent} \\
&< 2 \cdot k! && \text{by the inductive hypothesis} \\
&< (k+1)k! && \text{because } 2 < k+1 \\
&= (k+1)! && \text{by definition of factorial function.}
\end{aligned}
$$

This shows that P(k+ 1) is true when P(k) is true. This completes the inductive step of the proof.

**Example**

Use mathematical induction to prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer.

**Solution**

let P(n) denote the proposition: "$n^3 - n$ is divisible by 3."
BASIS STEP: The statement P(1) is true because $1^3 - 1 = 0$ is divisible by 3. This completes the basis step.

INDUCTIVE STEP: For the inductive hypothesis we assume that P(k) is true; that is, we assume that $k^3 - k$ is divisible by 3 for an arbitrary positive integer k.

To complete the inductive step, we must show that when we assume the inductive hypothesis, it follows that P(k+ 1), the statement that $(k + 1)^3 - (k + 1)$ is divisible by 3, is also true.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k).\end{aligned}$$

Using the inductive hypothesis, we conclude that the first term $k^3 - k$ is divisible by 3. The second term is divisible by 3 because it is 3 times an integer.

- **Strong Induction**

*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 $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers $k$.



**Example**

Show that if n is an integer greater than 1, then n can be written as the product of primes

**Solution**

Let P(n) be the proposition that n can be written as the product of primes

P(2) is true, because 2 can be written as the product of one prime, itself. (Note that P(2) is the first case we need to establish.)

INDUCTIVE STEP: The inductive hypothesis is the assumption that P(j) is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k. To complete the inductive step, it must be shown that P(k+ 1) is true under this assumption, that is, that k + 1 is the product of primes.

There are two cases to consider, namely, when k + 1 is prime and when k + 1 is composite. If k + 1 is prime, we immediately see that P(k+ 1) is true. Otherwise, k + 1 is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k+ 1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if k + 1 is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

# Quiz (2)

1. Use mathematical induction to prove that $x^{2n} - y^{2n}$ is divisible by x+y whenever n is a positive integer.

2. Use mathematical induction to prove that $3^n < n!$ for every integer n with $n \geq 7$. (Note that this inequality is false for n = 1, 2, …and 6.)

Lecture 3