Mat2033 - Discrete Mathematics

Methods of Proving Theorems

Methods of Proving Theorems

Direct Proofs

The implication $p \to q$ can be proved by showing that if p is true, then q must be true. This shows that the combination p true and q false never occurs. A proof of this kind is called a direct proof.

To carry out such a proof, assume that p is true and use rules of inference and theorems already proved to show that q must also be true.

Direct Proofs

- The implication $p \to q$ can be proved by showing that if *p* is true then *q* must also be true. This shows that the combination *p* true and *q* false never occurs.
- A proof of this kind is called a direct proof.

Example: Show that if $a|b$ and $b|c$ then $a|c$.

Proof: Assume that $a|b$ and $b|c$.
This means that there exists integer x and y such that $b = ax$ and $c = by$. But, by substitution we can then say that $c = (ax)y = a(xy)$. But xy is an integer, call it k. Therefore $c = ak$ and by the definition of divisibility, $a|c$.

Definition: The integer n is <u>even</u> if there exists an integer k such that $n = 2k$ and it is <u>odd</u> if there exists an integer k such that $n = 2k+1$.

Example: Give an indirect proof of the theorem "If n is odd, then n^2 is odd."

Solution: Assume that the hypotheses of the theorem is true, namely, suppose that n is odd. Then $n = 2k+1$, where k is an integer. It follows that $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore, n^2 is an odd integer.

Indirect Proofs

Since the implication $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$, the implication $p \to q$ can be proved by showing that its contrapositive, $\neg q \to \neg p$, is true. This related implication is usually proved directly, but any proof technique can be used. An argument of this type is called an <u>indirect proof</u>.

Indirect Proof

- Since the implication $p \to q$ is equivalent to its contrapositive $\neg q \to \neg p$ the original implication can be proven by showing that the contrapositive is true.

Example: Show that if ab is even then a or b are even.

To prove a number is even you must show that it can be written as $2k$ for some integer k. Since we know that ab is even, $ab = 2k$ for some integer k. But what does that say about a and b? Not much.

Consider the contrapositive of the implication:

If a and b are **not** even then ab is **not** even. That is, if a and b are odd then ab is odd.

Example – continued

If a number (*ab* in this case) is odd, we must show that it can be written as $2k+1$ for some integer k.

But, a and b are odd so there exists integers x and y such that $a=2x+1$ or $b=2y+1$.
Therefore,

$$ab=(2x+1)(2y+1)=4xy+2x+2y+1= 2(2xy+x+y)+1$$

Since $2xy+x+y$ is an integer (call it k) we can write ab as $2k+1$ and ab must be odd.

Example: Give an indirect proof of the theorem "If $3n+2$ is odd, then n is odd."

Example: Give an indirect proof of the theorem "If $3n+2$ is odd, then n is odd."

Solution: Assume that the conclusion of this implication is false; namely assume that n is even. Then $n = 2k$ for some integer k. It follows that $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$, so $3n+2$ is even and therefore not odd. Because the negation of the conclusion of the implication implies that the hypotheses is false, the original implication is true.

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

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

Solution: **Direct Proof:** Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k+1$. If we solve this equation for n we get $n = \mp\sqrt{2k+1}$. But we can not say anything about n whether n is an odd or even integer. So direct proof does not give any result.

Indirect Proof: (We use $\neg q \rightarrow \neg p$, since this is equivalent $p \rightarrow q$.) Assume n is not odd. Then n is even and there exist an integer k such that $n = 2k$. By squaring both sides of this equation we get $n^2 = 4k^2 = 2(2k^2)$. Let $t = 2k^2$ then n^2 can be written as $n^2 = 2t$. This means n^2 is even. The proof is completed. This means that indirect proof gives the result.

Vacuous and Trivial Proofs

Suppose that the hypotheses p of an implication $p \to q$ is false. Then the implication is true, because the statement has the form $F \to T$ or $F \to F$, and hence is true. Consequently, if it can be shown that p is false, then a proof, called a vacuous proof, of the implication $p \to q$ can be given.

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n>1$, then $n^2>n$."

Exercise: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n > 1$, then $n^2 > n$."

Solution: $P(0)$ is the implication "If $0 > 1$, then $0^2 > 0$." Since the hypothesis $0 > 1$ is false, the implication $P(0)$ is automatically true.

Trivial Proof

Suppose that the conclusion q of an implication $p \to q$ is true. Then $p \to q$ is true, since the statement has the form $T \to T$ or $F \to T$, which are true. Hence, if it can be shown that q is true, then a proof, called a <u>trivial proof</u>, of $p \to q$ can be given.

EXAMPLE

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

EXAMPLE

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

Solution: The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof. ◀

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

Solution: (The real number r is **rational** if there exist integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$.

A real number that is not rational is called **irrational**.)

Direct proof: Let $r, s \in \mathbb{Q}$. Then there exists integers p, q, t, u such that $r = \frac{p}{q}$ $(q \neq 0)$ and $s = \frac{t}{u}$ $(u \neq 0)$.

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + tq}{uq} \quad (uq \neq 0 \text{ since } u \neq 0, q \neq 0)$$

Therefore $r + s$ is rational.

Vacuous Proof Example

Theorem. (For all n) If n is both odd and even, then $n^2 = n + n$.

Proof. The statement "n is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. □

Trivial Proof Example

Theorem.(For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.

Proof. *Any* integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially. □

Proof by Contradiction

- We want to prove that a statement *p* is true.
- Suppose that a contradiction q can be found so that $\neg p \to q$ is true, that is, $\neg p \to F$ true. Then the proposition $\neg p$ must be false and consequently *p* must be true.
- This technique can be used when a contradiction, such as $r \wedge \neg r$, can be found so that it is possible to show that the implication $\neg p \to (r \wedge \neg r)$ is true.
- An argument of this type is called a proof by contradiction.

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

Solution: Let p be the proposition "$\sqrt{2}$ is irrational". Suppose that $\neg p$ is true. Then $\sqrt{2}$ is rational. We will show that this leads to a contradiction. Under the assumption that that $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors (so that the fraction $\frac{a}{b}$ is in lowest terms). Since $\sqrt{2} = \frac{a}{b}$, when both sides of this equation are squared, it follows that

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

Hence,

$$2b^2 = a^2.$$

This means that a^2 is even, implying that a is even.

Furthermore, since a is even, $a = 2c$ for some integer c. Thus

$$2b^2 = 4c^2$$

so

$$b^2 = 2c^2$$

This means that b^2 is even. Hence, b must be even as well.

It has been shown that $\neg p$ implies that $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors, and 2 divides a and b. This is a contradiction since we have shown that $\neg p$ implies both r and $\neg r$ where r is the statement that a and b are integers with no common factors. Hence, $\neg p$ is false, so that p: "$\sqrt{2}$ is irrational" is true.

Existence Proofs

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x\, P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x\, P(x)$ is called an existence proof. There are several ways to prove a theorem of this type. Sometimes an existence proof of $\exists x\, P(x)$ can be given by finding an element $\underline{a}$ such that $P(a)$ is true.

Such an existence proof is called <u>constructive</u>. It is also possible to give an existence proof that is <u>nonconstructive</u>; that is, we do not find an element a such that $P(a)$ is true, but rather prove that $\exists x\, P(x)$ is true in some other way. One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Example: (A constructive Existence Proof): Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution: After considerable computation we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

We have proved the assertion.

<u>Example:</u> (A nonconstructive Existence Proof): Show that there exist irrational numbers x and y such that x^y is rational.

Example: (A nonconstructive Existence Proof): Show that there exist irrational numbers x and y such that x^y is rational.

Solution: $\sqrt{2}$ is irrational. Let $x=\sqrt{2}$ and $y=\sqrt{2}$. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational. On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$ so that $x^y=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=(\sqrt{2})^{\sqrt{2}\sqrt{2}}=(\sqrt{2})^2=2$. We have shown that either the pair $x=\sqrt{2}$, $y=\sqrt{2}$ or the pair $x=\sqrt{2}^{\sqrt{2}}$, $y=\sqrt{2}$ have the desired property, but we do not know which of these two pairs work!

Nonconstructive Existence Proof

Theorem: There are infinitely many prime numbers.

- Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is *no* largest prime number.
- *I.e.*, show that for any prime number, there is a larger number that is *also* prime.
- More generally: For *any* number, $\exists$ a larger prime.
- Formally: Show $\forall n\ \exists p>n : p$ is prime.

- Given $n>0$, prove there is a prime $p>n$.
- Consider $x = n!+1$. Since $x > 1$, we know (x is prime)$\vee$(x is composite).
- **Case 1:** x is prime. Obviously $x > n$, so let $p = x$ and we're done.
- **Case 2:** x has a prime factor p. But if $p \leq n$, then p divides 1. So $p > n$, and we're done.

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a uniqueness proof are:

Existence: We show that an element x with the desired property exists.

Uniqueness: We show that if $y \neq x$, then y does not have the desired property.

Remark: Showing that there is a unique element x such that $P(x)$ is the same as proving the statement

$$\exists x \, (P(x) \wedge \forall y \, (y \neq x \rightarrow \neg P(y))).$$

Example: Show that every integer has a unique additive inverse. Show that if p is an integer, then there exists a unique integer q such that $p+q=0$.

Example: Show that every integer has a unique additive inverse. Show that if p is an integer, then there exists a unique integer q such that $p+q=0$.

Solution: If p is an integer, we find that $p+q=0$ when $q=-p$ and q is also an integer. To show that q is unique suppose r is an integer with $r \neq q$ such that $p+r=0$. Then

$$p+q=p+r$$
$$p-p=r-q=0 \Rightarrow r=q$$

We find $r=q$ which contradicts our assumption. Consequently there exist a unique integer q such that $p+q=0$

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: First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$. Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, 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, we find that $ar = as$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$. This means that if $s \neq r$, then $as + b \neq 0$. This establishes the uniqueness part of the proof. ◀

Counterexamples

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

<u>Example</u>: "Every positive integer is the sum of the squares of three integers". Show that this is fals

<u>Solution</u>: If we can show that there is a particular integer that is not the sum of the squares of three integers then the statement is false. To look for a counterexample, we try to write successive positive integers as a sum of three squares. We find that

$$1 = 0^2 + 0^2 + 1^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + 2^2$$

$$1 = 0^2 + 0^2 + 1^2$$

$$2 = 0^2 + 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$4 = 0^2 + 0^2 + 2^2$$

$$5 = 0^2 + 1^2 + 2^2$$

$1 = 0^2 + 0^2 + 1^2$

$2 = 0^2 + 1^2 + 1^2$

$3 = 1^2 + 1^2 + 1^2$

$4 = 0^2 + 0^2 + 2^2$

$5 = 0^2 + 1^2 + 2^2$

$6 = 1^2 + 1^2 + 2^2$

$1 = 0^2 + 0^2 + 1^2$

$2 = 0^2 + 1^2 + 1^2$

$3 = 1^2 + 1^2 + 1^2$

$4 = 0^2 + 0^2 + 2^2$

$5 = 0^2 + 1^2 + 2^2$

$6 = 1^2 + 1^2 + 2^2$

But we can not write 7 as the sum of three squares. 7 is a counterexample. We conclude that the statement is false.

Mathematical induction

- Frequently we want to prove a proposition of the form $\forall n\ P(n)$, in which the universe of discourse is the set of positive integers.

Mathematical induction

- Principle of Mathematical Induction (weak induction): Suppose that P(1) is true and that for every positive integer n, if P(n) is true then P(n+1) is true as well. Then for every positive integer n, the proposition P(n) is true.

- Principle of Mathematical Induction (strong induction): Suppose that P(1) is true and that for every positive integer n, if P(1), P(2),…, and P(n) are true then P(n+1) is true as well. Then for every positive integer n, the proposition P(n) is true.

Well-Ordering Principle: Every nonempty set of positive integers has a least element.

Mathematical induction

- Intuitively the idea of induction is this. I prove P(1). This is called the ***basis step***. Then for a fixed but arbitrary n, I assume P(n) is true and I use it to prove P(n+1). This is called the ***inductive step***, and the assumption that P(n) is true is called the ***induction hypothesis*** (sometimes IH for short). Thus $P(n) \rightarrow P(n+1)$ is always true. Since, P(1) is true, then P(2) is as well. So P(3) is, and thus P(4) is, etc. It is typical to require beginning students to label their basis and inductive steps. With practice, however, mathematicians find that induction proofs are usually mechanical, and they write them quite casually.

Mathematical induction

Example: The sum of the first n positive odd integers is n^2. That is, for all positive integers,

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Solution:

1. Basis Step: If n=1, the proposition states that

$$1 = 1^2,$$

which is true.

2. Induction Hypothesis: For some positive integer n, assume the proposition holds. That is, assume

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Mathematical induction

Example: The sum of the first n positive odd integers is n^2.
That is, for all positive integers,

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Solution:

3. Inductive Step: We want to show that it also holds for n+1.
That is, we want to show

$$1 + 3 + \ldots + (2n-1) + (2n+1) = (n+1)^2.$$

Using the induction hypothesis we see

$$[1+3+\ldots+(2n-1)] + (2n+1) = n^2 + (2n+1) = (n+1)^2.$$

By the principle of mathematical induction,

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

for all positive integers n.

<u>Example:</u> If n is a positive integer, then $n^3 - n$ is a multiple of 3.

Solution:

1. Basis Step: If n=1, then we have

$$1^3 - 1 = 0 = 3 \cdot 0,$$

which is a multiple of 3.

2. Induction Hypothesis: For some positive integer n, assume $n^3 - n$ is a multiple of 3. So, for instance, $n^3 - n = 3m$, for some integer m.

<u>Example:</u> If n is a positive integer, then $n^3 – n$ is a multiple of 3.

Solution:

3. Inductive Step: We wish to show

$$(n+1)^3 - (n+1) \text{ is a multiple of 3.}$$

We may rewrite

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3+3n^2+3n+1) – (n+1) \\ &= (n^3–n) + 3n^2 + 3n \\ &= 3m + 3n^2 + 3n \\ &= 3(m+n^2+n),\end{aligned}$$

which is a multiple of 3.

Therefore by the principle of mathematical induction, for all positive integers n, it holds that $n^3–n$ is a multiple of 3.

Theorem: Every positive integer greater than 1 has a prime factor.

Proof:

1. Basis Step: The positive integer 2 has itself for a prime factor.

2. Induction Hypothesis: For some positive integer n, suppose integers 2, 3, 4, …, n all have prime factors.

3. Inductive Step: We want to show that n+1 has a prime factor. Let us consider two cases: If n+1 is prime, then it is a prime factor of itself. If n+1 is not prime, it has factors a and b such that n+1=ab. Necessarily a and b are smaller than n+1. Therefore by the induction hypothesis a has a prime factor, say p. Then n+1=ab. But p is a factor of a and therefore of ab, so n+1 has a prime factor. By the principle of mathematical induction, every positive integers greater than 1 has a prime factor.