Lesson 4: Introduction to Proofs

- **Topics to be covered.**
  - **Methods of Proving Theorems**
  - **Direct Proof**
  - **Proof by Contraposition**
  - **Proofs by Contradiction**
  - **Proof by Cases**
  - **Existence Proofs**
  - **Proof Strategies**

Proof of a Theorem

A proof is a valid argument that establishes the truth of a mathematical statement.

A proof can use axioms, statements 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.

Note: Formal proofs of theorems can be extremely long and hard to follow. In practice, the proofs of theorems designed for human consumption are almost always informal proof.

Proofs

We can use a proof to demonstrate that a particular statement is true. A proof consists of a sequence of statements that form an argument.

The steps that connect the statements in such a sequence are the rules of inference.

Cases of incorrect reasoning are called **fallacies**.

Terminology

A **Theorem** is a statement that can be shown to be true.

A **lemma** is a simple theorem used as an intermediate result in the proof of another theorem.

A **Corollary** is a proposition that follows directly from a theorem that has been proved.

A **Conjecture** is a statement whose truth value is unknown. Once it is proven, it becomes a theorem.

Informal Proofs

In Mathematics, Computer Science, and other disciplines, informal proofs are generally used. Informal proofs are easy to understand and to explain to people.

In informal proofs:

- More than one rule of inference may be used in a step.
- Steps may be skipped.
- The axioms being assumed and the rules of inference used are not explicitly stated.

Practical Applications of Proofs

- Verifying that computer programs are correct
- Establishing that operating systems are secure
- Making inferences in artificial intelligence
- Showing that system specifications are consistent.

Understanding How Theorems Are Stated

Most of the theorems are conditional statement or quantified conditional statement.

Usual way of stating theorem (Example):

The sum of two odd integers is even

Formal way of stating theorem:

$\forall\, m, n \in \mathbb{Z} \quad (m, n \text{ are odd} \rightarrow \quad m + n \text{ is even})$

$\forall\, m, n \in \mathbb{Z} \quad [(O(m) \& O(n)) \rightarrow \neg O(m + n)]$, where O(n) is the predicate " n is odd".

Methods of Proving Theorems of the form $p \rightarrow q$

1. **Vacuous Proof**- Showing that p is false
2. **Trivial Proof** - Showing that q is true
3. **Direct Proof** - In a direct proof, 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.
4. **Indirect Proof** –
   - **Proof by Contraposition**: Since $p \rightarrow q \equiv \neg q \rightarrow \neg p$, the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true.
   - **Proof by Contradiction**: To prove that q is true whenever p is true, we assume that q is false and derive a contradiction.

Vacuous Proof

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

When p is false $p \rightarrow q$ *is true irrespective of the truth value of* q.
*Theefore it is sufficient to prove t*hat p is false to prove $p \rightarrow q$ is true

Vacuous Proof - Example

$\forall\, x \in R \quad (x^2 < -1 \rightarrow x^2 + 1 < 0)$

$\forall\, x \in R \quad x^2 < -1$ is False

Therefore

$\forall\, x \in R \quad (x^2 < -1 \rightarrow x^2 + 1 < 0)$ is True

Trivial Proof - Examples

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

When q is true $p \rightarrow q$ *is true irrespective of the truth value of* p.
*Theefore it is suffficient to prove t*hat q is true to prove $p \rightarrow q$ is true

Trivial Proof - Examples

$$\forall\, x \in R \quad (x \geq= 0 \rightarrow x^2+2x+1 \geq 0)$$

Proof :

$$x^2+2x+1 = (x+1)2 \quad >= 0 \;\forall\, x \in R$$

Therefore

$$\forall\, x \in R \quad (x \geq= 0 \rightarrow x^2+2x+1 \geq 0)$$

Direct Proofs: Example 1

Theorem: *The sum of two odd integers is even.*

Proof: Let n, m be two arbitrary integers.

Suppose that *n* and *m* are odd.

$\Longrightarrow \quad n = 2k_1 + 1 \;\&\; m = 2k_2 + 1, \text{ for some } k_1, k_2 \in \mathbb{Z}$

$\Longrightarrow \quad n + m = 2k_1 + 1 + 2k_2 + 1$

$= 2k_1 + 2k_2 + 2$

$= 2(k_1 + k_2 + 1)$

$\Longrightarrow \quad \mathrm{m} + \mathrm{n} = 2\mathrm{k}', \text{where } \mathrm{k}' \in \mathbb{Z}$

$\Longrightarrow \quad m + n$ is an even integer

Definition: An integer n is odd if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Since n, m are arbitrary we have, the sum of any two odd integers is even.

Direct Proofs: Example 1

Prove that the sum of two rational numbers is rational.

Proof: Let p, q be two arbitrary rational numbers.

Suppose that $p = \frac{a}{b},\ q = \frac{c}{d},\ where\ a, c \in \mathbb{Z}\ \&\ b, d \in \mathbb{Z}^{+}.$

$\Rightarrow p + q = \frac{a}{b} + \frac{c}{d}$

$\Rightarrow \quad p + q = \frac{ad+bc}{bd},$ where $ad + bc \in \mathbb{Z}\ \&\ bd \in \mathbb{Z}^{+}.$

$\Rightarrow$ p + q is a rational number.

Hence the sum of two rational numbers is rational.

Direct Proofs: Example 3

Prove that "If n is an odd integer, then n^2 is odd."

Let $O(n)$ be the predicate " n is odd". Then the statement that we have to prove is $\forall n \in \mathbb{Z}\left(O(n) \longrightarrow O(n^2)\right)$.

Proof: Let $n \in \mathbb{Z}$ be arbitrary.

Suppose that n is odd.

$\Longrightarrow \quad n = 2k + 1$ for some $k \in \mathbb{Z}$.

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

$\Longrightarrow \quad n^2 = 2(2k^2 + 2k) + 1 = 2k_1 + 1$, where $k_1 = 2k^2 + 2k \in \mathbb{Z}$.

$\Longrightarrow n^2$ is odd.

Indirect Proofs: Example 1 (Proof by contraposition)

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

Let $O(n)$ be the predicate " n is odd". Then the statement that we have to prove is $\forall n \in \mathbb{Z}\left(O(n^2) \longrightarrow O(n)\right)$. That is equivalent to $\forall n \in \mathbb{Z}\left(\neg O(n) \longrightarrow \neg O(n^2)\right)$.

Proof: Let $n \in \mathbb{Z}$ be arbitrary.

Suppose that n is even.

$\Longrightarrow \quad n = 2k$ for some $k \in \mathbb{Z}$.

$\Longrightarrow \quad n^2 = (2k)^2 = 4k^2$.

$\Longrightarrow \quad n^2 = 2(2k^2) = 2k_1$, where $k_1 = 2k^2 \in \mathbb{Z}$.

$\Longrightarrow n^2$ is even.

Proof by contraposition – Example-2

Prove that if $n = ab$, where $a, b \in \mathbb{Z}^+$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
$\neg\,(a \leq \sqrt{n}$ or $b \leq \sqrt{n}) \Longrightarrow n \neq ab$

Proof: Suppose that $\neg\,(a \leq \sqrt{n}$ or $b \leq \sqrt{n})$ is true.

$\Longrightarrow$ $\neg\,(a \leq \sqrt{n})$ and $\neg\,(b \leq \sqrt{n})$ is true

$\Longrightarrow$ $a > \sqrt{n}$ and $b > \sqrt{n}$

$\Longrightarrow$ $ab > \sqrt{n} \times \sqrt{n} = n$

$\Longrightarrow$ $ab \neq n$.

Hence, we have proved by contraposition that if $n = ab$, where $a, b \in \mathbb{Z}^+$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proofs by Contradiction

- Suppose we want to prove that a statement p is true.
- Now 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.
- 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.

Proof by Contradiction – Example -1

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

Proof: Let p be the proposition "$\sqrt{2}$ is irrational."

Suppose that $\neg p$ is true. That is; $\sqrt{2}$ is rational.

$\Rightarrow \sqrt{2} = \frac{a}{b}$, where $b \neq 0, \gcd(a, b) = 1.$

$\Rightarrow \ a^2 = 2b^2$

$\Rightarrow$ a^2 is even

$\Rightarrow$ a is even (It can be proved that a^2 is even implies a is even)

$\Rightarrow a = 2k,$ for some $k \in \mathbb{Z}.$

$\Rightarrow \ 2b^2 = a^2 = \ (2k)^2 = 4k^2 = 2\ (2k^2)$

$\Rightarrow \ b^2$ is even

$\Rightarrow$ b is even

$\Rightarrow \gcd(a, b) \geq 2$

$\Rightarrow \ \gcd(a, b) \neq 1 \ and \ \gcd(a, b) = 1$. (a Contradiction!)

$\Rightarrow$ $\neg p$ is false. That is $\sqrt{2}$ is irrational.

Proofs of Equivalence

Some of the Mathematical theorems are bi-conditional statements $p \leftrightarrow q$.

To prove a statement of the form $p \leftrightarrow q$, we have to show both $p \rightarrow q$ & $q \rightarrow p$ are true. This is because of $p \leftrightarrow q \equiv p \rightarrow q \wedge q \rightarrow p$.

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

Proofs of Equivalence

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

On way of proving this theorem is to show that the following nx(n-1) = $n^2 - n$ conditional statements are true:

$$p_i \rightarrow p_j \ \ for\ all\ i \neq j\ \ with\ \ 1 \leq i \leq n\ \&\ 1 \leq j \leq n.$$

However the following identity shows that if the *n* conditional statements $p_1 \rightarrow p_2,\ p_2 \rightarrow p_3,\ \ldots, p_n \rightarrow p_1$ can be shown to be true, then the propositions $p_1, p_2,\ \ldots, p_n$ are all equivalent:

$$p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \cdots \leftrightarrow p_n \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1)$$

Example

Show that these statements about the integer n are equivalent:

p_1: n is even.

p_2: n−1 is odd.

p_3: n^2 is even.

Proof: $p_1 \implies p_2$

Suppose that n is even

$\implies n = 2k,$ for some $k \in \mathbb{Z}$

$\implies n - 1 = 2k - 1 = 2(k-1) + 1$

$\implies n - 1 = 2k_1 + 1$, where $k_1 \in \mathbb{Z}$

$\implies n - 1$ is odd.

Proof: $p_2 \implies p_3$

Suppose that $n - 1$ is odd

$\implies n - 1 = 2k + 1,$ for some $k \in \mathbb{Z}$

$\implies n = 2k+2$

$\implies n^2 = 4k^2 + 8k + 4 = 2k_1$, where $k_1 = 2k^2 + 4k + 2 \in \mathbb{Z}$

$\implies n^2$ is even.

Proof: $p_3 \implies p_1 \equiv \neg p_1 \implies \neg p_3$

Suppose that n is odd

$\implies n = 2k + 1,$ for some $k \in \mathbb{Z}$

$\implies n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$\implies n^2 = 2(2k^2 + 2k) + 1$

$\implies n^2 = 2k_1 + 1$, where $k_1 = 2k^2 + 2k \in \mathbb{Z}$

$\implies n^2$ is odd

Counter Example

Prove or disprove the following statement.
For any integer n, If n^2 is positive, then n is positive.

Let P(n) be “n is positive ” and Q(n) be “ n^2 is positive”.

Given statement is $\forall n \in \mathbb{Z}\ (Q(n) \rightarrow P(n))$.

This is not a true statement. Counter example is $n = -1$.

Exhaustive Proof and Proof by Cases

We now introduce a method that can be used to prove a theorem, by considering different cases separately. That is; theorems of the form $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$.

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q \equiv \neg(p_1 \vee p_2 \vee \cdots \vee p_n) \vee q$$

$$\equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n) \vee q$$

$$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \cdots \wedge (\neg p_n \vee q)$$

$$\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$$

This shows that the statement $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ can be proved by proving each of the n conditional statement $p_i \rightarrow q$ for $i = 1,2,\ldots,n$.

Proof by Cases – Example -1

Let $\sqcup$ be an operator defined by $\sqcup(a,b) = Min(a,b)\ \forall\ a,b \in \mathbb{Z}$.
Show that

$$a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c \quad for\ all\ \ a,b,c\ \in \mathbb{Z}.$$

Solution: Let $a,b,c\ \in \mathbb{Z}$ be arbitrary. There are 6 =(3 x 2 x 1)possible cases:

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

Case 1: Suppose that $a \leq b \leq c$. Then

LHS $= a \sqcup (b \sqcup c) = a \sqcup b = a$ and RHS $= (a \sqcup b) \sqcup c = a \sqcup c =$ a.

Therefore, the result is true for case 1.

Other cases can be proved similarly.

Proof by Cases – Example - 2

Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.

Solution: $|x| \geq 3 \implies x^2 > 8$ and $|y| \geq 2 \implies 3y^2 > 8$.

Hence it is enough to consider the cases $x = -2, -1, 0, 1, 2$ & $y = -1, 0, 1$.

Possible values for x^2 are $0, 1, 4$ and possible values for $3y^2$ are $0, 3$ and the largest sum of possible values for x^2 and $3y^2$ is 7.

Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when x and y are integers.

Proof by Cases – Example - 3

Prove that for all $x \in \mathbb{R}$, $-5 \leq |x+2| - |x-3| \leq 5$.

Proof:

$$|x+2| = \begin{cases} x+2, if\ x \geq -2 \\ -(x+2), if\ x < -2. \end{cases} \qquad |x-3| = \begin{cases} x-3, if\ x \geq 3 \\ -(x-3), if\ x < 3. \end{cases}$$

Given the way the functions are broken apart, we shall consider the cases

$$x < -2, \qquad -2 \leq x < 3, \qquad x \geq 3.$$

Case 1: Suppose that $x < -2$. Then

$|x+2| - |x-3| = -(x+2) - \big(-(x-3)\big) = -5.$

Hence, $-5 \leq |x+2| - |x-3| \leq 5.$

Case 2: Suppose that $-2 \leq x < 3$. Then

$|x+2| - |x-3| = (x+2) - \big(-(x-3)\big) = 2x - 1.$

Hence, $-5 \leq |x+2| - |x-3| \leq 5.$

$$-2 \leq x < 3$$
$$\Rightarrow \quad -4 \leq 2x < 6$$
$$\Rightarrow \quad -5 \leq 2x - 1 < 5$$

Example – 3 Cont.

Case 2: Suppose that$x \geq 3$. Then
$|x + 2| - |x - 3| = (\mathrm{x} + 2) - (\mathrm{x} - 3) = 5.$
Hence, $-5 \leq |x + 2| - |x - 3| \leq 5.$

Since $-5 \leq |x + 2| - |x - 3| \leq 5$ holds all three cases, we have
$-5 \leq |x + 2| - |x - 3| \leq 5, \forall x \in \mathbb{R}.$

Exercise:
Using Proof by cases, show that the following statement is true.
If n is an integer, then $2n^2 + n + 1$ is not divisible by 3.

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.

- **Constructive Existence Proof:** Finding an element *a* such that $P(a)$ is true.
- **Non-constructive Existence Proof:** In this, 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.

An Example of 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: 1729 is an integer that can be written as a sum of cubes of two positive integers in two different ways.

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

An Example of a Non-constructive Existence Proof

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

Solution: we know that $\sqrt{2}$ is irrational. Consider the real 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 $y = \sqrt{2}$.
- 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 $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2.$

Uniqueness Proofs

Some theorems asset the existence of a unique element with a particular property ($\exists!x\, P(x)$).

The two parts of a *uniqueness proof* are

1. ***Existence***: We show that an element x with the property exists.
2. ***Uniqueness***: We show that if $y \neq x$ then y does not have the property.

That is $\exists!\, x\, P(x) \equiv \exists x \left(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y))\right)$

$\equiv \exists x\, (P(x) \wedge \forall y(P(y) \rightarrow y = x))$

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

Example

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 we shall show that $r = \frac{-b}{a} \in \mathbb{R}$, satisfies the equation $ar + b = 0$.

$$a \times \frac{-b}{a} + b = -b + b = 0.$$

- Suppose that $\exists y \in \mathbb{R}$ such that $ay + b = 0$.

$\Rightarrow y = \frac{-b}{a} = r.$

Backward Reasoning

Example: Prove that $\frac{(x+y)}{2} > \sqrt{xy}$ when x and y are distinct positive real numbers.

$$\frac{(x+y)}{2} > \sqrt{xy}$$

$$\Leftrightarrow \frac{(x+y)^2}{4} > xy$$

$$\Leftrightarrow (x+y)^2 > 4xy$$

$$\Leftrightarrow x^2 + 2xy + y^2 > 4xy$$

$$\Leftrightarrow x^2 - 2xy + y^2 > 0$$

$$\Leftrightarrow (x-y)^2 > 0$$

Proof: Suppose that x and y are distinct positive real numbers.

$$\Rightarrow (x-y)^2 > 0$$

$$\Rightarrow x^2 - 2xy + y^2 > 0$$

$$\Rightarrow x^2 + 2xy + y^2 > 4xy$$

$$\Rightarrow (x+y)^2 > 4xy$$

$$\Rightarrow (x+y) > 2\sqrt{xy}$$

$$\Rightarrow \frac{(x+y)}{2} > \sqrt{xy}.$$

The 3x +1 Conjecture

A **Conjecture** is a statement whose truth value is unknown. Once it is proven, it becomes a theorem.

Let $T: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ be a function defined by

$$T(x) = \begin{cases} \frac{x}{2} & if \;\; x \; is \; even \\ (3x+1) & if \; x \; is \; odd. \end{cases}$$

This is a famous conjecture, sometimes known as the 3x +1 conjecture, states that for all positive integers x, when we repeatedly apply the transformation T , we will eventually reach the integer 1.

$$\left(\forall n \; \exists m \; (T^m(n) = 1)\right)$$

$$T(5) = 16 \implies T^2(5) = T\big(T(5)\big) = T(16) = 8 \implies T^3(5) = T\big(T^2(5)\big) = \mathrm{T}(8) = 4$$

$$T^4(5) = T\big(T^3(5)\big) = T(4) = 2 \implies T^5(5) = T(T^4(5)) = \mathrm{T}(2) = 1.$$

The $3x + 1$ conjecture has been verified using computers for all integers x up to $5.6 \cdot 10^{13}$.