

Methods of Proofs

We are now prepared to begin our main topic: mathematical proofs. It is essential to know what methods are available to us if we wish to verify the truth of a mathematical statement.

1. Rules for Proving

Using a truth table is one of the methods of proving but it is not convenient when we have to prove the statement that combines many statements together. To solve this problem we use the *Rules for Proving* instead of the truth table.

In proving, we use the following principle.

- 1) The truth value of the given statement is always true.
- 2) Use the given statements, laws of tautology, rules for proving, and the statements that have been proved to prove the given conclusion that its truth value is true.

Note that we will only write the statements that truth value is true and we will write only “ p ” when we want to say “*the truth value of p is true.*”

Rules for Proving

1.1 Rule of Modus Ponens or Rule of Implication

If $p \rightarrow q$ and p , then q

Proof:

1.2 Rule of Substitution

There are two types of using Rule of Substitution.

- 1) Substitute the statement that is tautology (or contradiction) with the other statement
- 2) Substitute the statement with its equivalent statement.

Proof: By the theorem of tautology, theorem of contradiction, and the theorem of equivalence.

For example,

1.3 Definition of Conjunction

There are two types of using Definition of Conjunction.

- 1) If $p \wedge q$, then p and q .
- 2) If p and q , then $p \wedge q$

1.4 Rule of Modus Tollens

If $p \rightarrow q$ and $\sim q$, then $\sim p$

Proof:

1.5 Disjunctive Syllogism

There are two types of using Disjunctive Syllogism.

1) If $p \vee q$ and $\sim p$, then q .

2) If $p \vee q$ and $\sim q$, then p .

Proof:

1.6 Constructive Dilemma

If $(p \rightarrow q) \wedge (r \rightarrow s)$ and $p \vee r$, then $q \vee s$

2. Direct Proof

The direct proof is the proof that start with what is given then use the rules for proving, axioms, theorems, laws of tautology, or the statements that have been proved to make a conclusion.

Example 1: Prove that if $u \vee (r \rightarrow t)$ and $\sim u \wedge \sim t$, then $\sim r$.

Example 2: Prove that if $x \rightarrow (y \rightarrow z)$, $\sim y \rightarrow \sim x$, and x , then z .

3. Indirect Proof or Proof by Contradiction

The direct proof is sometimes not very easy to do use the other method of proof which is called indirect proof or proof by contradiction.

To use the method of indirect proof, we assume that the statement we want to proof is false then we try to show that it contradicts with the given statement.

Example 1: Prove that if $(\sim x \vee \sim y) \rightarrow (z \wedge w)$, $z \rightarrow t$, and $\sim t$, then x .

4. Proof of statements in the form of “ $p \rightarrow q$ ”

There are two ways to proof the statements in the form of $p \rightarrow q$.

- 1) Assume p , then prove q .
- 2) Use Law of Contraposition, that is $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$ or $(p \rightarrow q) \equiv (\sim q \rightarrow \sim p)$, then we prove $(\sim q \rightarrow \sim p)$ instead of $(p \rightarrow q)$. To prove $(\sim q \rightarrow \sim p)$, we assume $\sim q$, then prove $\sim p$

Example 1: Prove that if $x \vee \sim y$, and $z \rightarrow \sim(x \vee t)$, then $y \rightarrow \sim z$.

Example 2: Prove that $[\sim a \rightarrow (b \wedge \sim b)] \rightarrow a$

5. Proof of statements in the form of “ $p \vee q$ ”

Since $(p \vee q) \leftrightarrow (\sim p \rightarrow q)$, by Law of Implication, we can then prove $\sim p \rightarrow q$ instead of $p \vee q$. To prove $\sim p \rightarrow q$, we can assume $\sim p$ and show that q is true. Moreover, since $(p \vee q) \equiv (q \vee p)$ and $(q \vee p) \leftrightarrow (\sim q \rightarrow p)$, hence there are two ways to prove $p \vee q$.

- 1) Assume $\sim p$ and show that q is true.
- 2) Assume $\sim q$ and show that p is true

6. Proof of statements in the form of “ $p \leftrightarrow q$ ”

Since $(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$, by Law of Equivalence, we can then prove $(p \rightarrow q) \wedge (q \rightarrow p)$ instead of $p \leftrightarrow q$. To prove $(p \rightarrow q) \wedge (q \rightarrow p)$, we have to prove that $p \rightarrow q$ is true and also $q \rightarrow p$ is true by the method of proving the statements in the form of $p \rightarrow q$.

7 Proof of statements in the form of “ $(p \vee q) \rightarrow r$ ”

Note that

$$\begin{aligned}
 [(p \vee q) \rightarrow r] &\equiv [\sim(p \vee q) \vee r] && \text{Law of Implication} \\
 &\equiv [(\sim p \wedge \sim q) \vee r] && \text{De Morgan's Laws} \\
 &\equiv [(\sim p \vee r) \wedge (\sim q \vee r)] && \text{Distributive Laws} \\
 &\equiv [(p \rightarrow r) \wedge (q \rightarrow r)] && \text{Law of Implication}
 \end{aligned}$$

Hence, we can prove $(p \rightarrow r) \wedge (q \rightarrow r)$ instead of $(p \vee q) \rightarrow r$. In order to show that

$(p \rightarrow r) \wedge (q \rightarrow r)$ is true, we must show that $p \rightarrow r$ is true and also $q \rightarrow r$ is true.

8. Mathematical Induction

Carl Friedrich Gauss is considered to be one of the most brilliant mathematicians of all time. The story goes that when he was very young (in grade school in Germany) his teacher gave him and his classmates the supposedly unpleasant task of adding the integers from 1 to 100. He obtained the correct result of 5050 quickly. It is believed that he considered both the sum $1+2+\dots+100$ and its reverse $100+99+\dots+1$ and added these to obtain the sum $101+101+\dots+101$, which has 100 terms and so equals 10100. Since this is twice the required sum, $1+2+\dots+100=10100/2=5050$. This, of course, can be quite easily generalized to find a formula for $1+2+\dots+n$, where $n \in \mathbb{N}$. Let

$$S = 1 + 2 + \dots + n. \quad (3.1)$$

If we reverse the order of the terms on the right side of (3.1), then we obtain

$$S = n + (n-1) + (n-2) + \dots + 1 \quad (3.2)$$

Adding (3.1) and (3.2), we have

$$2S = (n+1) + (n+1) + \dots + (n+1) \quad (3.3)$$

Since there are n terms on the right side of (3.3), we conclude that $2S = n(n+1)$ or $S = n(n+1)/2$. Hence

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

This formula can be verified by a totally different technique. As we shall see, this technique called **mathematical induction**, or simply **induction**, is very powerful. First, we present a theorem, called the **Principle of Mathematical Induction**.

Suppose that we have a sequence of statements which we would like to show are true, say one statement for each positive integer. More specifically, let $S_1, S_2, S_3, \dots$ be statements. We wish to show that all of these statements are true. Of course, it is not at all practical to establish the truth of these statements individually. An alternative is now presented.

Theorem 8.1 (The Principle of Mathematical Induction) *Let $S_1, S_2, S_3, \dots$ be statements satisfying the following properties:*

(1) S_1 is true;

(2) if S_k is true, where $k \in N$, then S_{k+1} is true. (i.e. $\forall k (S_k \rightarrow S_{k+1})$ where $k \in N$)

Then all of the statements $S_1, S_2, S_3, \dots$ are true.

Example 1: Use mathematical induction to prove that

$$S_n : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

is true for every positive integer n .

Example 2: Prove that for every positive integer n ,

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n+1)(n+2)} = \frac{n}{2n+4}$$

By a nearly identical argument, we can prove a somewhat more general result.

Theorem 8.2 *Let $S_m, S_{m+1}, S_{m+2}, \dots$ be statements satisfying the following properties:*

(1) S_m is true;

(2) if S_k is true, where $k \in I$ and $k \geq m$, then S_{k+1} is true.

Then all of the statements $S_m, S_{m+1}, S_{m+2}, \dots$ are true.

Example 3: Let n be positive integer and $n \geq 2$, prove that $1 + 2n < 3^n$.

Theorem: For all statements p , q , and r , the following statements are tautologies.

1. Law of Identity: $p \leftrightarrow p$
2. Law of Double Negation: $p \leftrightarrow \sim(\sim p)$
3. Law of Excluded Middle: $p \vee \sim p$
4. Law of Contradiction: $\sim(p \wedge \sim p)$
5. Idempotent Laws: $(p \wedge p) \leftrightarrow p$, $(p \vee p) \leftrightarrow p$
6. Law of Addition: $p \rightarrow (p \vee q)$
7. Law of Equivalence: $[p \leftrightarrow q] \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$
8. Law of Contraposition: $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$
9. Law of (Hypothetical) Syllogism: $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow [p \rightarrow r]$
10. Commutative Laws: $(p \wedge q) \leftrightarrow (q \wedge p)$
 $(p \vee q) \leftrightarrow (q \vee p)$
11. Associative Laws: $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge r] \leftrightarrow [p \wedge q \wedge r]$
 $[p \vee (q \vee r)] \leftrightarrow [(p \vee q) \vee r] \leftrightarrow [p \vee q \vee r]$
12. Distributive Laws: $[p \wedge (q \vee r)] \leftrightarrow [(p \wedge q) \vee (p \wedge r)]$
 $[p \vee (q \wedge r)] \leftrightarrow [(p \vee q) \wedge (p \vee r)]$
13. Absorption Laws: $[p \wedge (p \vee q)] \leftrightarrow p$
 $[p \vee (p \wedge q)] \leftrightarrow p$
14. De Morgan's Laws: $\sim(p \wedge q) \leftrightarrow (\sim p \vee \sim q)$
 $\sim(p \vee q) \leftrightarrow (\sim p \wedge \sim q)$
15. Law of Implication: $(p \rightarrow q) \leftrightarrow (\sim p \vee q)$
 $(p \vee q) \leftrightarrow (\sim p \rightarrow q)$
16. Law of Negation for Implication: $\sim(p \rightarrow q) \leftrightarrow (p \wedge \sim q)$

Rules for Proving:

1. Rule of Modus Ponens or Rule of Implication

If $p \rightarrow q$ and p , then q

2. Rule of Substitution

2.1 Substitute the statement that is tautology (or contradiction) with the other statement

2.2 Substitute the statement with its equivalent statement.

3. Definition of Conjunction

3.1 If $p \wedge q$, then p and q .

3.2 If p and q , then $p \wedge q$

4. Rule of Modus Tollens

If $p \rightarrow q$ and $\sim q$, then $\sim p$

5. Disjunctive Syllogism

5.1 If $p \vee q$ and $\sim p$, then q .

5.2 If $p \vee q$ and $\sim q$, then p .

6. Constructive Dilemma

If $(p \rightarrow q) \wedge (r \rightarrow s)$ and $p \vee r$, then $q \vee s$