Mat2033 - Discrete Mathematics

Methods of Proof

METHODS OF PROOF

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, establishing that operating sytems are secure, making inferences in the area of artificial intelligence, showing that system specifications are consistent, and so on. Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Rules of Inference

We will now introduce rules of inference for propositional logic. These rules provide the justification of the steps used to show that a conclusion follows logically from a set of hypotheses. The tautology

$$(p \wedge (p \to q)) \to q$$

is the basis of the rule of inference called MODUS PONENS. This tautology is written in the following way

$$\begin{array}{l} p \\ \underline{p \to q} \\ \therefore q \end{array}$$

Using this notation, the hypotheses are written in a column and the conclusion below a bar.

The symbol $\therefore$ denotes "therefore." Modus ponens states that if both an implication and its hypotheses are known to be true, then the conclusion of this implication is true.

Example: Suppose that the implication

"If it snows today, then we will go skiing"

and its hypotheses,

"It is snowing today,"

are true. Then, by modus ponens, it follows that the conclusion of the implication, "We will go skiing," is true.

<u>Example:</u> Assume that the implication

"If n is greater than 3, then n^2 is greater than 9"

is true. Consequently, if n is greater than 3, then, by modus ponens, it follows that n^2 is greater than 9.

Table Lists some important rules of inference.

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore\ p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \rightarrow p$	Simplification

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore\ p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{l} p \\ \underline{q} \\ \therefore\ p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore\ p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \rightarrow p$	Simplification
$\dfrac{\begin{array}{c} p \\ q \end{array}}{\therefore\ p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\dfrac{\begin{array}{c} p \\ p \rightarrow q \end{array}}{\therefore\ q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore\ p \vee q}$	$p \to (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \to p$	Simplification
$\dfrac{\begin{array}{l} p \\ q \end{array}}{\therefore\ p \wedge q}$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$\dfrac{\begin{array}{l} p \\ p \to q \end{array}}{\therefore\ q}$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\dfrac{\begin{array}{l} \neg q \\ p \to q \end{array}}{\therefore\ \neg p}$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\begin{array}{l} p \\ \hline \therefore\ p \vee q \end{array}$	$p \to (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \hline \therefore\ p \end{array}$	$(p \wedge q) \to p$	Simplification
$\begin{array}{l} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$\begin{array}{l} p \\ p \to q \\ \hline \therefore\ q \end{array}$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore\ \neg p \end{array}$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r \end{array}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\dfrac{p}{\therefore\ p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \rightarrow p$	Simplification
p $\dfrac{q}{\therefore\ p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
p $\dfrac{p \rightarrow q}{\therefore\ q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\neg q$ $\dfrac{p \rightarrow q}{\therefore\ \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $\dfrac{q \rightarrow r}{\therefore\ p \rightarrow r}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\dfrac{\neg p}{\therefore\ q}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $\therefore p \vee q$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \rightarrow p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
p $p \rightarrow q$ $\therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p: It is below freezing now.

q: It is raining now.

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p: It is below freezing now.

q: It is raining now.

Then this argument is of the form

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

Example: State which rule of inference is the basis of the following argument:

"It is below freezing now. Therefore, it is either below freezing or raining now."

Solution: Let p and q be:

p: It is below freezing now.

q: It is raining now.

Then this argument is of the form

$$\begin{array}{l} \quad p \\ \hline \therefore p \vee q \end{array}$$

This is an argument that uses the addition rule.

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now Therefore, it is below freezing now."

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now Therefore, it is below freezing now."

solution: Let p and q be:

p: It is below freezing now

q: It is raining now.

Example: State which rule of inference is the basis of the following argument "It is below freezing and raining now Therefore, it is below freezing now."

solution: Let p and q be:

p: It is below freezing now

q: It is raining now.

This argument is of the form

$$\frac{p \wedge q}{\therefore\ p}$$

__Example:__ State which rule of inference is the basis of the following argument "It is below freezing and raining now Therefore, it is below freezing now."

__solution:__ Let p and q be:

p: It is below freezing now

q: It is raining now.

This argument is of the form

$$\frac{p \wedge q}{\therefore\ p} \qquad \text{(simplification rule)}$$

Example: State which rule of inference is used in the argument:

If it rains today, then will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

Example: State which rule of inference is used in the argument:

If it rains today, then will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

solution: Let propositions p, q and r be:

p: It is raining today.

q: We will not a have a barbecue today.

r: We will have a barbecue tomorrow.

Solution: Let propositions p, q and r be:

p: It is raining today.

q: We will not a have a barbecue today.

r: We will have a barbecue tomorrow.

Then this argument is of the form

Solution: Let propositions p, q and r be:

p: It is raining today.

q: We will not a have a barbecue today.

r: We will have a barbecue tomorrow.

Then this argument is of the form

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r \end{array}$$

<u>solution:</u> Let propositions p, q and r be:

p: It is raining today.

q: We will not a have a barbecue today.

r: We will have a barbecue tomorrow.

Then this argument is of the form

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r \end{array}$$

(Hypothetical syllogism)

These examples show how arguments in English can be analyzed using rules of inference.

Example: Show that the hypotheses "It is not sunny this afternoon and it is colder than yesterday," "We will go swimming only if it is sunny," "If we do not go swimming, then we will take a canoe trip," and "If we take a canoe trip, then we will be home by sunset" lead to the conclusion "We will be home by sunset."

Solution: Let $p, q, r, s,$ and t be:

p: It is sunny this afternoon

q: It is colder than yesterday

r: We will go swimming

s: We will take a canoe trip

t: We will be home by sunset

<u>Solution:</u> Let $p, q, r, s,$ and t be:

p: It is sunny this afternoon

q: It is colder than yesterday

r: We will go swimming

s: We will take a canoe trip

t: We will be home by sunset

Then the hypotheses become $\neg p \wedge q$, $r \to p$, $\neg r \to s$, and $s \to t$.

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \rightarrow p$	Hypotheses

Then the hypotheses become $\neg p \wedge q$, $r \to p$, $\neg r \to s$, and $s \to t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \to p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses

Then the hypotheses become $\neg p \wedge q$, $r \to p$, $\neg r \to s$, and $s \to t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \to p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \to s$	Hypotheses
6. s	Modus ponens using steps 4 and 5

Then the hypotheses become $\neg p \wedge q$, $r \to p$, $\neg r \to s$, and $s \to t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \to p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \to s$	Hypotheses
6. s	Modus ponens using steps 4 and 5
7. $s \to t$	Hypothesis

Then the hypotheses become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$.

Step	Reason
1. $\neg p \wedge q$	hypothesis
2. $\neg p$	Simplification using step 1
3. $r \rightarrow p$	Hypotheses
4. $\neg r$	Modus tollens using steps 2 and 3
5. $\neg r \rightarrow s$	Hypotheses
6. s	Modus ponens using steps 4 and 5
7. $s \rightarrow t$	Hypothesis
8. t	Modus ponens using steps 6 and 7

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Solution: Let p, q, r, s, t be

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Example: Show that the hypotheses "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Solution: Let p, q, r, s, t be

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

Step	Reason
1. $p \to q$	Hypotheses

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

Step	Reason
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of step 1

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

Step	Reason
1. $p \to q$	Hypotheses
2. $\neg q \to \neg p$	contrapositive of step 1
3. $\neg p \to r$	Hypotheses

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

Step	Reason
1. $p \to q$	Hypotheses
2. $\neg q \to \neg p$	contrapositive of step 1
3. $\neg p \to r$	Hypotheses
4. $\neg q \to r$	Hypothetical syllogism using steps 2 and 3

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \to q$, $\neg p \to r$, and $r \to s$.

Step	Reason
1. $p \to q$	Hypotheses
2. $\neg q \to \neg p$	contrapositive of Step 1
3. $\neg p \to r$	Hypotheses
4. $\neg q \to r$	Hypothetical syllogism using steps 2 and 3
5. $r \to s$	Hypotheses

p: You send me an e-mail message

q: I will finish writing the program

r: I will go to sleep early

s: I will wake up feeling refreshed

Then the hypotheses are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$.

Step	Reason
1. $p \rightarrow q$	Hypotheses
2. $\neg q \rightarrow \neg p$	contrapositive of step 1
3. $\neg p \rightarrow r$	Hypotheses
4. $\neg q \rightarrow r$	Hypothetical syllogism using steps 2 and 3
5. $r \rightarrow s$	Hypotheses
6. $\neg q \rightarrow s$	Hypothetical syllogism using steps 4 and 5

Rules of Inference for Quantified Statements

We discussed rules of inference for propositions. We will now describe some important rules of inference for statements involving quantifiers.

<u>Universal instantiation</u>: is the rule of inference used to conclude that $P(c)$ is true, where c is a particular member of the universe of discourse, given the premise $\forall x\, P(x)$.

$$\begin{array}{l} \forall x\, P(x) \\ \hline \therefore P(c) \end{array}$$

Universal generalization: is the rule of inference that states that $\forall x\, P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the universe of discourse. Universal generalization is used when we show that $\forall x\, P(x)$ is true by taking an arbitrary element c from the universe of discourse and showing that $P(c)$ is true. The element c that we select must be an arbitrary, and not a specific element of the universe of discourse.

$$\begin{array}{rl} & P(c) \text{ for an arbitrary } c \\ \hline \therefore & \forall x\, P(x) \end{array}$$

Existential instantiation: is the rule that allows us to conclude that there is an element c in the universe of discourse for which $P(c)$ is true if we know that $\exists x\, P(x)$ is true. We cannot select an arbitrary value of c here, but rather it must be a c for which $P(c)$ is true. Usually we have no knowledge of what c is, only that it exists. Since it exists, we may give it a name (c) and continue our argument.

$$\begin{array}{l} \exists x\, P(x) \\ \hline \therefore\ P(c) \text{ for some element } c \end{array}$$

Existential generalization: is the rule of inference that is used to conclude that $\exists x\, P(x)$ is true when a particular element c with $P(c)$ true is known. That is, if we know one element c in the universe of discourse for which $P(c)$ is true, then we know that $\exists x\, P(x)$ is true.

$$\frac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$$

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, P(x)}$	Universal generalization
$\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$	Existential generalization

EXAMPLE

Show that the premises "Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science."

EXAMPLE

Show that the premises "Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science."

Solution: Let $D(x)$ denote "x is in this discrete mathematics class," and let $C(x)$ denote "x has taken a course in computer science." Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Marla})$. The conclusion is $C(\text{Marla})$.

EXAMPLE

Show that the premises "Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science."

Solution: Let $D(x)$ denote "x is in this discrete mathematics class," and let $C(x)$ denote "x has taken a course in computer science." Then the premises are $\forall x(D(x) \rightarrow C(x))$ and D(Marla). The conclusion is C(Marla).

The following steps can be used to establish the conclusion from the premises.

Step	Reason
1. $\forall x(D(x) \rightarrow C(x))$	Premise
2. $D(\text{Marla}) \rightarrow C(\text{Marla})$	Universal instantiation from (1)
3. $D(\text{Marla})$	Premise
4. $C(\text{Marla})$	Modus ponens from (2) and (3)

EXAMPLE

Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

Solution: Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book," and $P(x)$ be "x passed the first exam." The premises are $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$. The conclusion is $\exists x(P(x) \land \neg B(x))$. These steps can be used to establish the conclusion from the premises.

Step	**Reason**
1. $\exists x(C(x) \land \neg B(x))$	Premise
2. $C(a) \land \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \land \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	Existential generalization from (8)

Methods of Proving Theorems

Direct Proofs

The implication $p \rightarrow q$ 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 even if there exists an integer k such that $n=2k$ and it is odd 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 $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$, the implication $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, 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 $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$ 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 trivial proof, 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. □