



Proof Methods

Section 1.5 Methods of Proof

Definitions

- A *theorem* is a *valid* logical assertion which can be proved using
 - other theorems
 - *axioms* (statements which are given to be true) and
 - *rules of inference* (logical rules which allow the deduction of conclusions from premises).
- A *lemma* (not a “lemon”) is a 'pre-theorem' or a result which is needed to prove a theorem.
- A *corollary* is a 'post-theorem' or a result which follows directly from a theorem.
- A *mathematical argument* is a list of statements. Its last statement is called the conclusion.

Rules of Inference

- A *logical rule of inference* is a method that depends on logic alone for deriving a new statement from a set of other statements.
- Many of the tautologies in Chapter 1 are rules of inference. They have the form
$$H1 \wedge H2 \wedge \dots \wedge Hn \rightarrow C$$
where
 H_i are called the *hypotheses*
and
 C is the *conclusion*.

Rules of Inference

- As a rule of inference they take the symbolic form:

$$H_1$$
$$H_2$$
$$\cdot$$
$$\cdot$$
$$H_n$$
$$\therefore C$$

where \therefore means 'therefore' or 'it follows that.'

Rules of Inference

- Example:

The tautology $P \wedge (P \rightarrow Q) \rightarrow Q$ becomes

P

$P \rightarrow Q$

$\therefore Q$

This means that whenever P is true and $P \rightarrow Q$ is true we can conclude logically that Q is true.

This rule of inference is the most famous and has the name

- *modus ponens*

or

- the *law of detachment*.

Famous rules of inference

- Addition

P

$\therefore P \vee Q$

- Simplification

$P \wedge Q$

$\therefore P$

- Modus Ponens

P

$P \rightarrow Q$

$\therefore Q$

- *Modus Tollens*

$\neg Q$

$P \rightarrow Q$

$\therefore \neg P$

Famous rules of inference

■ Hypothetical syllogism

$$\begin{aligned} P &\rightarrow Q \\ Q &\rightarrow R \\ \therefore P &\rightarrow R \end{aligned}$$

■ Disjunctive syllogism

$$\begin{aligned} P \vee Q \\ \neg P \\ \therefore Q \end{aligned}$$

■ Conjunction

$$\begin{aligned} P \\ Q \\ \therefore P \wedge Q \end{aligned}$$

■ Contrapositive

$$\begin{aligned} P \rightarrow Q \\ \therefore \neg Q \rightarrow \neg P \end{aligned}$$

Proofs Using Rules of Inference

- To prove an argument is valid or the conclusion follows *logically* from the hypotheses:
 - Assume the hypotheses are true.
 - Use the rules of inference and logical equivalences to determine that the conclusion is true.
- Steps involved:
 - Define proposition.
 - Represent arguments & conclusion using logical expressions.
 - Reasoning using Rules of Inferences.

Proofs Using Rules of Inference

- Example: Consider the following logical argument:

If horses fly or cows eat artichokes, then the mosquito is the national bird. If the mosquito is the national bird then peanut butter tastes good on hot dogs. But peanut butter tastes terrible on hot dogs. Therefore, cows don't eat artichokes.

- Step1: Assign propositional variables to the component propositions in the argument:

F Horses fly

A Cows eat artichokes

M The mosquito is the national bird

P Peanut butter tastes good on hot dogs

Proofs Using Rules of Inference

- Step2: Represent the formal argument using the variables

1. $(F \vee A) \rightarrow M$

2. $M \rightarrow P$

3. $\neg P$

$\therefore \neg A$

- Step3: Reasoning using Rules of Inferences

Proofs Using Rules of Inference

- Example:
 - Show that the hypotheses “Randy works hard,” “if Randy works hard, then he is a dull boy,” and “if Randy is a dull boy, he will get the job” imply “Randy will get the job”
 - step 1: define proposition
 - W: Randy works hard
 - D: Randy is a dull boy
 - J: Randy will get the job
 - Step 2: Represent the formal arguments:
 - W
 - $W \rightarrow D$
 - $D \rightarrow J$
 - Step 3: Construct reasoning

Rules of Inference with Quantifiers

- \forall related:

- Universal instantiation

$$\forall x P(x)$$

$$\therefore P(c)$$

- Universal generalization

$P(c)$ for arbitrary C

$$\therefore \forall x P(x)$$

Rules of Inference with Quantifiers

- \exists related:

- Existential instantiation

- $\exists x P(x)$

- $\therefore P(c)$ for some element C

- Existential generalization

- $P(c)$ for some element C

- $\therefore \exists x P(x)$

Rules of Inference with Quantifiers

■ Example:

- Construct a proof for the arguments of “No man is an island. Manhattan is an island. Therefore, Manhattan is not a man”

Solution:

- Step 1: define propositions

Men(x): x is a man

Island(x): x is a island

- Step 2: Represent the formal arguments:

$\forall x \text{ Men}(x) \rightarrow \neg \text{Island}(x)$

Island(Manhattan)

- Step 3: Construct reasoning

Rules of Inference with Quantifiers

- Example:

- Construct a proof for the following arguments:
Linda, a student in this class, owns a red convertible. Everyone who owns a red convertible has gotten at least one speeding ticket. Therefore, someone in this class has gotten a speeding ticket.

Solution:

- Step 1: define propositions
 $\text{red_conv}(x)$: x owns a red convertible
 $\text{speeding_ticket}(x)$: x gets a speeding ticket

Methods of Proof

- Goal: we wish to establish the truth of the 'theorem' $P \rightarrow Q$
 $P \rightarrow Q$ is a conjecture until a proof is produced.
- *Direct* proof
 - assumes the hypotheses P are true
 - implication $P \rightarrow Q$ can be proved by showing that if P is true then Q must be true

Methods of Proof: Direct Proof

■ Example:

Theorem: *If $6x + 9y = 101$, then x or y is not an integer.*

Proof: (*Direct*) Assume $6x + 9y = 101$ is true.

Then from the rules of algebra $3(2x + 3y) = 101$.

But $101/3$ is not an integer so it must be the case that one of $2x$ or $3y$ is not an integer (maybe both).

Therefore, one of x or y must not be an integer.

Q.E.D.

Methods of Proof: Direct Proof

- Something we need to know, a **axiom**:
for $n, k \in \text{integers}$,
 $n \text{ is odd} \leftrightarrow n = 2k + 1$
 $n \text{ is even, } \leftrightarrow n = 2k$
- Prove that “if n is odd, then n^2 is also odd”

Methods of Proof: Indirect Proof

- **Indirect** proof: a direct proof of the contrapositive:
 - assumes the conclusion of $P \rightarrow Q$ is false ($\neg Q$ is true)
 - uses the rules of inference, axioms and any logical equivalences to establish the premise P is false .
- Note, in order to show that a conjunction of hypotheses is false is suffices to show just one of the hypotheses is false.

Methods of Proof: Indirect Proof

- Example:

Theorem: *A perfect number is not a prime.*

A *perfect* number is one which is the sum of all its divisors except itself. For example, 6 is perfect since $1 + 2 + 3 = 6$.

So is 28.

Proof: (*Indirect*). We assume the number p is a prime and show it is not perfect.

But the only divisors of a prime are 1 and itself.

Hence the sum of the divisors less than p is 1 which is not equal to p .

Hence p cannot be perfect.

Q. E. D.

Methods of Proof: Indirect Proof

- Example:

Prove that “if $3n + 2$ is odd, then n is odd”

Methods of Proof: Proof by Contradiction

■ *Proof by contradiction*

To prove P is true:

- assumes the conclusion P is false
- derives a contradiction, usually of the form $R \wedge \neg R$ which establishes $\neg P \rightarrow 0$.

The contrapositive of this assertion is $1 \rightarrow P$ from which it follows that P must be true.

Methods of Proof: Proof by Contradiction

- Example 1:

Theorem: *There is no largest odd number.*

(Note that there are no formal hypotheses here)

- Example 2: prove that “if $3n + 2$ is odd, then n is odd”.

Methods of Proof: Proof by Cases

■ *Proof by cases*

To prove

$$(P_1 \vee P_2 \vee \dots \vee P_n) \rightarrow Q$$

Prove:

$$(P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge \dots \wedge (P_n \rightarrow Q)$$

Methods of Proof: Proof by Cases

- Example 1: prove that for $n \in \mathbb{N}$, $n^3 + n$ is even
- Example 2: prove that

$$\left\lfloor \frac{n}{2} \right\rfloor \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{n^2}{4} \right\rfloor$$