Section 3.1
Methods of Proof

Definition: 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.

Rules of Inference

Many of the tautologies in Chapter 1 are rules of inference. They have the form

$$H_1 \quad H_2 \quad ..... \quad H_n \rightarrow C$$

where

H_i are called the *hypotheses*

and

C is the *conclusion*.

As a rule of inference they take the symbolic form:

$$H_1$$
$$H_2$$
$$.$$
$$.$$
$$H_n$$
$$\therefore C$$

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

Examples:

The tautology $P \quad (P \rightarrow Q) \rightarrow Q$ 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*.

Other famous rules of inference:

P

$P \quad Q$ Addition

$P \quad Q$

P Simplification

$\neg Q$

$P \rightarrow Q$ *Modus Tollens*

$\neg P$

$P \rightarrow Q$

$Q \rightarrow R$ Hypothetical syllogism

$P \rightarrow R$

$P \quad Q$

$\neg P$ Disjunctive syllogism

Q

P

Q Conjunction

$P \quad Q$

$(P \rightarrow Q) \quad (R \rightarrow S)$

$P \quad R$ Constructive dilemma

$Q \quad S$

Formal Proofs

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.

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 takes good on hot dogs. But peanut butter tastes terrible on hot dogs. Therefore, cows don't eat artichokes.*

- 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

• Represent the formal argument using the variables

$$1.(F \quad A) \rightarrow M$$
$$2.M \rightarrow P$$
$$3.\neg P$$
$$\neg A$$

• Use the hypotheses 1., 2., and 3. and the above rules of inference and any logical equivalences to construct the proof.

Assertion	Reasons
$1.(F \quad A) \rightarrow M$	Hypothesis 1.
$2.M \rightarrow P$	Hypothesis 2.
$3.(F \quad A) \rightarrow P$`	steps 1 and 2 and *hypothetical syll.*
$4.\neg P$	Hypothesis 3.
$5.\neg (F \quad A)$	steps 3 and 4 and *modus tollens*
$6.\neg F \quad \neg A$	step 5 and DeMorgan
$7.\neg A \quad \neg F$	step 6 and commutativity of 'and'
$8.\neg A$	step 7 and simplification

Q. E. D.

Rules of Inference for Quantifiers

$$\begin{array}{l} xP(x) \\ P(c) \end{array}$$ Universal Instantiation (UI)

$$\begin{array}{l} P(x) \\ \quad xP(x) \end{array}$$ Universal Generalization (UG)

$$\begin{array}{l} P(c) \\ \quad xP(x) \end{array}$$ Existential Generalization (EG)

$$\begin{array}{l} xP(x) \\ P(c) \end{array}$$ Existential Instantiation (EI)

Note:

• In Universal Generalization, x must be arbitrary.

• In Universal Instantiation, c need not be arbitrary but often is assumed to be.

• In Existential Instantiation, c must be an element of the universe which makes P(x) true.

Example:

Every man has two legs. John Smith is a man.
Therefore, John Smith has two legs.

Define the predicates:

M(x): x is a man
L(x): x has two legs
J: John Smith, a member of the universe

The argument becomes

$$\begin{aligned} &1.\ \ \forall x[M(x) \rightarrow L(x)] \\ &2. M(J) \\ &\quad\ L(J) \end{aligned}$$

The proof is

$1.\ \ \forall x[M(x) \rightarrow L(x)]$	Hypothesis 1
$2. M(J) \rightarrow L(J)$	step 1 and UI
$3. M(J)$	Hypothesis 2
$4. L(J)$	steps 2 and 3 and *modus ponens*

Q. E. D.

Note: Using the rules of inference requires lots of practice.

Fallacies

Fallacies are incorrect inferences.

Some common fallacies:

- ***The Fallacy of Affirming the Consequent***

If the butler did it he has blood on his hands.
The butler had blood on his hands.
Therefore, the butler did it.

This argument has the form

$$P \rightarrow Q$$
$$Q$$
$$\therefore P$$

or

$$[(P \rightarrow Q) \quad Q] \rightarrow P$$

which is not a tautology and therefore not a rule of inference!

• ***The Fallacy of Denying the Antecedent*** (or the *hypothesis*)

If the butler is nervous, he did it.
The butler is really mellow.
Therefore, the butler didn't do it.

This argument has the form

$$P \rightarrow Q$$
$$\neg P$$
$$\neg Q$$

or

$$[(P \rightarrow Q) \quad \neg P] \rightarrow \neg Q$$

which is also not a tautology and hence not a rule of inference.

• ***Begging the question* or *circular reasoning***

This occurs when we use the truth of statement being proved (or something equivalent) in the proof itself.

Example:

Conjecture: *if x^2 is even then x is even.*

Proof: If x^2 is even then $x^2 = 2k$ for some k. Then $x = 2l$ for some l. Hence, x must be even.

Methods of Proof

We wish to establish the truth of the 'theorem'

$$P \rightarrow Q.$$

P may be a conjunction of other hypotheses.

$P \rightarrow Q$ is a *conjecture* until a proof is produced.

- ***Trivial*** proof

  If we know Q is true then $P \rightarrow Q$ is true.

Example:

If it's raining today then the void set is a subset of every set.

The assertion is *trivially* true independent of the truth of *P.*

- ***Vacuous*** *proof*

  If we know one of the hypotheses in P is false then $P \rightarrow Q$ is *vacuously* true.

Example:

If I am both rich and poor then hurricane Fran was a mild breeze.

This is of the form

$$(P \quad \neg P) \rightarrow Q$$

and the hypotheses form a contradiction.

Hence Q follows from the hypotheses vacuously.

• ***Direct*** proof

- assumes the hypotheses are true

- uses the rules of inference, axioms and any logical equivalences to establish the truth of the conclusion.

Example: the *Cows don't eat artichokes* proof above

• ***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.

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.

Example:

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.

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

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.

• ***Proof by contradiction*** or ***reductio ad absurdum***

- assumes the conclusion Q is false

- derives a contradiction, usually of the form $P \quad \neg P$ which establishes $\neg Q \rightarrow 0$.

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

Example:

Theorem: *There is no largest prime number*.

(Note that there are no formal hypotheses here.)

We assume the conclusion 'there is no largest prime number' is false.

There is a largest prime number.

Call it p.

Hence, the set of all primes lie between 1 and p.

Form the product of these primes:

$$r = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot .... \cdot p.$$

But r + 1 is a prime larger than p. (Why?).

This contradicts the assumption that there is a largest prime.

Q.E.D.

The formal structure of the above proof is as follows:

Let P be the assertion that there is no largest prime.
Let Q be the assertion that p is the largest prime.

Assume $\neg P$ is true.

Then (for some p) Q is true so $\neg P \rightarrow Q$ is true.

We then construct a prime greater than p so $Q \rightarrow \neg Q$.

Applying *hypothetical syllogism* we get $\neg P \rightarrow \neg Q$.

From two applications of *modus ponens* we conclude that Q is true and $\neg Q$ is true so by conjunction $\neg Q \quad Q$ or a contradiction is true.

Hence the assumption must be false and the theorem is true.

- ***Proof by Cases***

Break the premise of $P \rightarrow Q$ into an equivalent disjunction of the form

$$P_1 \quad P_2 \quad \ldots \quad P_n.$$

Then use the tautology

$$[(P_1 \rightarrow Q) \quad (P_2 \rightarrow Q) \quad \ldots \quad (P_n \rightarrow Q)] \leftrightarrow$$
$$[(P_1 \quad P_2 \quad \ldots \quad P_n) \rightarrow Q]$$

Each of the implications $P_i \rightarrow Q$ is a *case.*

You must

• Convince the reader that the cases are inclusive, i.e., they exhaust all possibilities

• establish all implications

Example:

Let be the operation 'max' on the set of integers:

if $a \geq b$ then $a \quad b = \max\{a, b\} = a = b \quad a$.

Theorem: *The operation is associative.*

For all a, b, c

$$(a \quad b) \quad c = a \quad (b \quad c).$$

Proof:

Let a, b, c be arbitrary integers.

Then one of the following 6 cases must hold (are exhaustive):

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

Case 1: a b = a, a c = a, and b c = b.

Hence

(a b) c = a = a (b c).

Therefore the equality holds for the first case.

The proofs of the remaining cases are similar (and are left for the student).

Q. E. D.

Existence Proofs

We wish to establish the truth of

$$xP(x).$$

- ***Constructive*** existence proof:

- Establish P(c) is true for some c in the universe.

- Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example:

Theorem: *There exists an integer solution to the equation* $x^2 + y^2 = z^2$.

Proof:

Choose x = 3, y = 4, z = 5.

Example:

Theorem: *There exists a bijection from A= [0,1] to B= [0, 2].*

Proof:

We build two injections and conclude there must be a bijection without ever exhibiting the bijection.

Let f be the identity map from A to B.

Then f is an injection (and we conclude that $| A | \leq | B |$).

Define the function g from B to A as g(x) = x/4.

Then g is an injection.

Therefore, | B | ≤ | A |.

We now apply a previous theorem which states that

if | A | ≤ | B | and | B | ≤ | A | then | A | = | B |.

Hence, there must be a bijection from A to B.

(Note that we could have chosen g(x) = x/2 and obtained a bijection directly).

Q. E. D.

• ***Nonconstructive*** existence proof.

- Assume no c exists which makes P(c) true and derive a contradiction.

Example:

Theorem: *There exists an irrational number*.

Proof:

Assume there doesn't exist an irrational number.

Then all numbers must be rational.

Then the set of all numbers must be countable.

Then the real numbers in the interval [0, 1] is a countable set.

But we have already shown this set is not countable.

Hence, we have a contradiction (The set [0,1] is countable and not countable).

Therefore, there must exist an irrational number.

Q. E. D.

Note: we have not produced such a number!

• Disproof by ***Counterexample***:

Recall that $x\neg P(x) \leftrightarrow \neg \ \ xP(x)$.

To establish that $\neg \ \ xP(x)$ is true (or $\ \ xP(x)$ is false) construct a c such that $\neg P(c)$ is true or P(c) is false.

In this case c is called a *counterexample* to the assertion $xP(x)$

Nonexistence Proofs

We wish to establish the truth of

$\neg \ \ xP(x)$ (which is equivalent to $\ \ x\neg P(x)$).

Use a proof by contradiction by assuming there is a c which makes P(c) true.

Example:

The (infamous) Halting Problem

We wish to establish the nonexistence of a universal debugging program.

Theorem: *There does not exist a program which will always determine if an arbitrary program P halts.*

We say the Halting Problem is *undecidable.*

Sidenote: this is not the same as determining if a specific program or finite set of programs halts which is decidable.

There is always exists a program to determine if a specific program P halts:

- Construct program P1 which always prints 'yes' and halts.

- Construct program P2 which always prints 'no' and halts.

One of the two programs, P1 or P2, is the correct (deciding) program (we may not know which one!).

Hence this problem is decidable.

To simplify the argument: consider input-free programs only (which may call other procedures)

Proof:

Suppose there is such a program called HALT which will determine if any input-free program P halts.

HALT(P) prints 'yes' and halts if P halts,

otherwise,

HALT(P) prints 'no' and halts.

We now construct another procedure as follows:

```
procedure ABSURD;
if HALT(ABSURD) = 'yes' then
    while true do print 'ha'
```

Note that ABSURD is input-free.

• If ABSURD halts then we execute the loop which prints unending gales of laughter and thus the procedure does not halt.

• If ABSURD does not halt then we will exit the program and halt.

Hence,

• ABSURD

- halts if it doesn't

and

- doesn't halt if it does

which is an obvious contradiction. (You are free to loose sleep over this).

Hence such a program does not exist.

Q. E. D.

Note: This is not the same as asserting a program exists and we don't know how to write it or that it is very difficult to write such a program!

Universally Quantified Assertions

We wish to establish the truth of

$$\forall x P(x).$$

We assume that x is an arbitrary member of the universe and show P(x) must be true. Using UG it follows that $\forall x P(x)$.

Example:

Theorem: *For the universe of integers, x is even iff x^2 is even.*

Proof: The quantified assertion is

$$\forall x[x \text{ is even } \leftrightarrow x^2 \text{ is even}]$$

We assume x is arbitrary.

Recall that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \quad (Q \rightarrow P)$.

Case 1. We show if x is even then x^2 is even using a direct proof (the *only if* part or *necessity*).

If x is even then x = 2k for some integer k.

Hence, $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer which is divisible by 2.

This completes the proof of case 1.

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*) .

We use an indirect proof:

Assume x is not even and show x^2 is not even.

If x is not even then it must be odd.

So, x = 2k + 1 for some k.

Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

which is odd and hence not even.

This completes the proof of the second case.

Therefore we have shown x is even iff x^2 is even.

Since x was arbitrary, the result follows by UG.

Q.E.D.

Dear students: Learning how to construct proofs is probably one of the most difficult things you will face in life. Few of us are gifted enough to do it with ease. One only learns how to do it by practicing.