Section 1.6
Introduction to Proofs

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.

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•3•5•7•11•....•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 ≥ b then a b = max{a, b} = a = b a.

Theorem: *The operation is associative.*

For all a, b, c

(a b) c = a (b 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.
