Proofs

Continuing on chapter 1

Definitions

- A ***theorem*** is a valid logical assertion which can be proved using:
  - axioms (statements which are given to be true)
  - other theorems, 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

- Rules of inference are ***tautologies*** of the following form:

$$H_1 \wedge H_2 \wedge \ldots H_n \rightarrow C$$

- Where each H_i is a *hypothesis*, and C is the *conclusion.*
- I.e., *all* rules of inference (and theorems!) are of the form

$$(H_1 \wedge H_2 \wedge \ldots H_n \rightarrow C) \equiv T$$

Alternative (symbolic) notation

- $(H_1 \wedge H_2 \wedge \ldots H_n \rightarrow C) \equiv T$ is often written in the following form:

$$\begin{array}{l} H_1 \\ H_2 \\ \vdots \\ H_n \\ \therefore C \end{array}$$

- E.g., the tautology $(P \wedge (P \rightarrow Q)) \rightarrow Q$

  is written as

$$\begin{array}{l} P \\ P \rightarrow Q \\ \therefore Q \end{array}$$

- It is known as *modus ponens*

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**
$\dfrac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	**Conjunction**
$\dfrac{p \quad p \rightarrow q}{\therefore q}$	$(p \wedge [p \rightarrow q]) \rightarrow q$	**Modus ponens**

Rule of Inference	Tautology	Name
$\neg q$ $\underline{p \rightarrow q}$ $\therefore \neg p$	$\left[\neg q \wedge (p \rightarrow q)\right] \rightarrow \neg p$	**Modus tollens**
$p \rightarrow q$ $\underline{q \rightarrow r}$ $\therefore p \rightarrow r$	$\left[(p \rightarrow q) \wedge (q \rightarrow r)\right] \rightarrow (p \rightarrow r)$	**Hypothetical syllogism**
$p \vee q$ $\underline{\neg p \quad\quad}$ $\therefore q$	$\left[(p \vee q) \wedge (\neg p)\right] \rightarrow q$	**Disjunctive syllogism**
$p \vee q$ $\underline{\neg p \vee r}$ $\therefore q \vee r$	$\left[(p \vee q) \wedge (\neg p \vee r)\right] \rightarrow (q \vee r)$	**Resolution**

Example of a proof using inference

Consider the argument given in Example 7 in the text:

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.

If I go to sleep early, then I will wake up feeling refreshed.

Therefore:

If I do not finish writing the program, then I will wake up feeling refreshed

Example continued…

- We need to determine what are the building blocks of this argument.
- Let
  - e: you send me an e-mail message.
  - p: I finish writing the program.
  - s: I go to sleep early
  - r: I wake up feeing refreshed.
- What we need to prove is that

$$\begin{array}{l} e \rightarrow p \\ \neg e \rightarrow s \\ s \rightarrow r \\ \hline \therefore \neg p \rightarrow r \end{array}$$

Truth Table

$$[(e \to p) \wedge (\neg e \to s) \wedge (s \to r)] \to (\neg p \to r)$$

p	s	r	e	$e \to p$	$\neg e \to s$	$s \to r$	$\neg p \to r$	
T	T	T	T	T	T	T	T	T
T	T	T	F	T	T	T	T	T
T	T	F	T	T	T	F	T	T
T	T	F	F	T	T	F	T	T
T	F	T	T	T	T	T	T	T
T	F	T	F	T	F	T	T	T
T	F	F	T	T	T	T	T	T
T	F	F	F	T	T	T	T	T
F	T	T	T	F	T	T	T	T
F	T	T	F	T	F	T	T	T
F	T	F	T	F	T	F	F	T
F	T	F	F	T	T	F	F	T
F	F	T	T	F	T	T	T	T
F	F	T	F	T	F	T	T	T
F	F	F	T	F	T	T	F	T
F	F	F	F	T	F	T	F	T

Example (continued)

Steps	**Reasons**
1. $e \to p$	Hypothesis
2. $\neg p \to \neg e$	Contra-positive on Step 1
3. $\neg e \to s$	Hypothesis
4. $\neg p \to s$	Hypothetical syllogism on steps 2,3
5. $s \to r$	Hypothesis
6. $\neg p \to r$	Hypothetical syllogism on steps 4,5

Note, at each step we only used either an **equivalence rule** or a **rule of inference**

Steps

- Create a list of logical expressions
- Each entry in your list is either
  - A hypothesis
  - Obtained using inference rules on ***previous entries*** on you list, or using equivalence rules on previous entries on your list.
  - Your final entry on your list should be the conclusion you are trying to reach.

Fallacies (i.e. screw-ups!!!)

- Fallacies are **incorrect inferences**
- *The fallacy of affirming the consequent*
  – if the butler did it, he has blood in his hands
  – the butler had blood in his hands
  – therefore, the butler did it
- This (invalid!!!) argument has the form:

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

$$((p \rightarrow q) \wedge q) \rightarrow p$$

IT IS NOT A TAUTOLOGY!

More fallacies

- *Fallacy of denying the antecedent (hypothesis)*
  - If the butler is nervous, he did it.
  - The butler is really mellow (relaxed)
  - Therefore, the butler didn't do it.
- This (invalid!!!) argument has the form:

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

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

IT IS NOT A TAUTOLOGY!

Rules of Inference for Quantifiers

$\forall x P(x)$

$\therefore P(c)$

Universal Instantiation (UI)

(c can be any element of U that you want)

$P(c)$ for an arbitrary c

$\therefore \forall x P(x)$

Universal Generalization (UG)

$P(c)$

$\therefore \exists x P(x)$

(Here, you do need to know the specific value of c)

Existential Generalization (EG)

$\exists x P(x)$

$\therefore P(c)$ for some c

Existential Instantiation (EI)

(Here, you don't know the specific value of c!)

Example

- Prove the following:
  - 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

$$\begin{array}{l} \forall x\left(M(x) \rightarrow L(x)\right) \\ \underline{\quad M(J) \quad} \\ \therefore L(J) \end{array}$$

Example continued

Steps	**Reasons**
1. $\forall x\big(M(x) \rightarrow L(x)\big)$	Hypothesis
2. $M(J) \rightarrow L(J)$	Universal instantiation on Step 1
3. $M(J)$	Second Hypothesis
4. $L(J)$	Modus ponens on steps 2,3

Proof of Lewis Carroll's earlier example

Recall

$$\forall x\,(L(x) \rightarrow F(x))$$
$$\exists x\,(L(x) \wedge \neg C(x))$$
$$\therefore\ \exists x\,(F(x) \wedge \neg C(x))$$

Step	Reason
1. $\exists x\,(L(x) \wedge \neg C(x))$	Hypothesis
2. $(L(c_0) \wedge \neg C(c_0))$	Existential instantiation
3. $\forall x\,(L(x) \rightarrow F(x))$	Hypothesis
4. $(L(c_0) \rightarrow F(c_0))$	Universal instantiation
5. $\neg C(c_0)$	Simplification, step 2
6. $L(c_0)$	Simplification, step 2
7. $F(c_0)$	Modus ponens, step 4,6
8. $F(c_0) \wedge \neg C(c_0)$	Conjunction step 5,7
9. $\exists x\,(F(x) \wedge \neg C(x))$	Existential generalization

Theorems in practice

- Assume that someone has proven the following tautology.

$$(H_1 \wedge H_2 \wedge \ldots H_n \rightarrow C) \equiv T$$

- Assume also that H_1 through H_n have been proven true by someone else (or perhaps they are simply assumed to be true, i.e., axioms) then,
  - We know the implication $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ always returns true (it is a tautology)
  - If we have that someone else proved that $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ is true then,
    - C ***must*** be true (which is what you want) because only true can imply true (recall that the implication was shown to be a tautology).

Direct Proof Method

- Using rules of inference to derive your result is known as the "direct" method.

Example

- Show the following
  - *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.*
- Proposition
  - F Horses fly
  - A Cows eat artichokes
  - M The mosquito is the national bird
  - P Peanut butter tastes good on hot dogs

Continued …

- Represent the formal argument using the variables

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

$2. M \rightarrow P$

$3. \neg P$

$\therefore \neg A$

- Use the three hypotheses and the rules of inference and any logical equivalences obtain the conclusion.

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

Trivial Proofs

- You want to show $H \rightarrow C$, and you "know" C is true,
  - I.e. if you assume that C is true
  - then you can conclude that $H \rightarrow C$ *regardless* of H
  - H could be ``dogs can fly'' and we are still fine.
- Why? This is because

$$\begin{array}{l} p \\ \therefore \\ q \rightarrow p \end{array}$$

is a rule of inference (i.e. $p \rightarrow (q \rightarrow p)$) is a tautology

Trivial Proof (continued …)

- E.g.,
  - *if Dr. Cobb is ten feet tall then 0 + 1 = 1*
  - *If the moon is made of cheese then UT Dallas is part of the UT system*

Vacuous Proof

- If we know the hypothesis H is false, then we know $H \rightarrow C$ for any C.
  - This is because $F \rightarrow C$ is a tautology.

- E.g.,
  - *if 0 = 1 then I am ten feet tall*
  - *If the moon is made of cheese then UT Dallas has a football team*

Indirect Proof

- Remember direct proofs?
- An indirect proof is that, instead of a direct proof of $H \rightarrow C$, we do a direct proof of $\neg C \rightarrow \neg H$
- Note that by the contra-positive rule, these two are the same.

Abbreviated Proofs

- Writing things down in “perfect logic” often would yield pages and pages and pages of proof
- Thus, people use abbreviated (often just English) arguments
- This simplifies reading a proof, but if one is not careful, it can introduce errors (invalid proofs!)

Direct Method 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.

Indirect Proof 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

- To show *M*, assume $\neg M$ is true, then derive a contradiction (i.e., derive *false*)
- I.e., we are proving that

  $\neg M \rightarrow F$
- Note that if we take the contra-positive of the above we have

  $T \rightarrow M$
- This is just equivalent to *M*.

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:

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

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

This contradicts the assumption that there is a largest prime.

Q.E.D.

Proof by Cases

- Assume we want to show that $(H_1 \vee H_2 \vee H_3) \rightarrow C$
- Then, we take advantage of the following equivalence

$$((H_1 \vee H_2 \vee H_3) \rightarrow C)$$
$$\equiv ((H_1 \rightarrow C) \wedge (H_2 \rightarrow C) \wedge (H_3 \rightarrow C))$$

- It is important to show that it holds for ALL cases (in this case, three cases)

Example

Let $\otimes$ be the operation 'max' on the set of integers:

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

Theorem: *The operation $\otimes$ is associative.*

For all a, b, c

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

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: $a \otimes b = a$, $a \otimes c = a$, and $b \otimes c = b$.

Hence

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

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

- To prove that $\exists x\, P(x)$, we have **constructive** and **non-constructive** proofs
- In a *constructive proof*, simply exhibit a c such that $P(c)$ is true (finding c may be by brute force)
- E.g., there exists an integer solution to the equation $x^2 + y^2 = z^2$
  - Proof: simply choose $x = 3$, $y = 4$, and $z = 5$
  - (finding these values may be by exhaustive search, e.g., by a computer program)

Non-constructive Existence Proof

- Want to show that $\exists x\, P(x)$
- We do so by assuming no c exists such that $P(c)$ is true, and then arrive at a contradiction
  – We thus prove $\neg\exists x\, P(x) \rightarrow F$, i.e. a contradiction proof.
- Note you never exhibit a c' such that $P(c')$ is true!
  – Hence, it is ``non-constructive''

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 (rational + irrational) in the interval [0, 1] is a countable set.

But we have already shown this set is not countable (page 160).

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

Therefore, there must exist an irrational number.

Universal Quantification

- To show that $\forall x\, P(x)$,
  - We consider any element c in the universe
    - There is *nothing* specific about c, it can be *any* element
  - Show $P(c)$ is true
    - Your argument must hold irrespective of which c value is chosen (zero is a typical screw up for numbers, think division by zero!).
  - From universal generalization, $\forall x\, P(x)$ is true.

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 $(P \to Q) \wedge (Q \to P)$.

continued …

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.

Negation of Universal Quantifier

- To show that $\neg\forall x\, P(x)$
  - Typically, you do a *constructive proof* of $\exists x\, \neg P(x)$, which is equivalent to $\neg\forall x\, P(x)$
    - I.e., find an element c such that $\neg P(c)$ holds
  - This is known as finding a **counter-example** to $\forall x\, P(x)$

Negation of Existential Quantifier

- To show that $\neg\exists x\, P(x)$ (which equals $\forall x\, \neg P(x)$)
  - Typically, do a contradiction proof
    - *Assume* that for an element c, $P(c)$ holds (i.e., $\exists x\, P(x)$)
    - There is *nothing* specific about c, it can be *any* element
    - Reach false from this
    - Note: I cannot apply the constructive method since it is used to prove $\exists x\, P(x)$ rather than $\neg\exists x\, P(x)$.
      - I.e., if you choose a specific c_0, so what? If $P(c_0)$ is true, you just proved that $\neg\exists x\, P(x)$ is false! If $P(c_0)$ is false, it is not helpful since you need to show $\forall x\, \neg P(x)$ not just for one c_0.
  - Or, you can use the method of the previous slides but with $\forall x\, \neg P(x)$ rather than $\forall x\, P(x)$

Remarks

- *Learning how to construct proofs is quite difficult, and is a slow learning process. One only learns how to do it by practicing.*
- *Be careful of fallacies and incorrect arguments*
- *The book gives you examples of some incorrect proofs.*