Proof Techniques

ARGUMENT

- **Argument:**

An argument is a sequence of statements that ends with a conclusion.

- All statements but the final one are called premises.
- The final statement is called the conclusion.

- **An argument is valid if:**

whenever all the premises are true, then the conclusion is true.

ARGUMENT (CONT.)

- **Example:**

If today is Wednesday, then yesterday is Tuesday.

Today is Wednesday.

Yesterday is Tuesday

Argument

- **How** to determine whether this argument is valid or not !
- **Are** the truth tables suitable for this ? **Why** ?
- If we have 10 different proposition variables how many rows we need ?

Rules of Inference for Propositional Logic

- We can always use a truth table to show that an argument form is valid.
- This is a tedious approach
- when, for example, an argument involves 9 different propositional variables
- To use a truth table to show this argument is valid
- It requires $2^9 = 512$ different rows !!!!!!!

Rules of Inference

- Fortunately, we do not have to resort to truth tables.
- Instead we can first establish the validity of some simple argument forms, called rules of inference
- These rules of inference can then be used to construct more complicated valid argument forms
- We use rules of inference to deduce new statements from statements we already have.

TABLE 1 Rules of Inference

Rules of Inference	Tautology	Name
p p → q -------------------- ∴q	[p ^ (p → q)] → q	Modus ponens
¬ q p → q ------------------------ ∴ ¬ p	[¬ q ^ (p → q)] → ¬ q	Modus tollens
p → q q → r ----------------------- ∴ p → r	[(p → q) ^ (q → r)] → (p → r)	Hypothetical syllogism
p v q ¬P --------------------- ∴ q	[(p v q) ^ ¬ p] → q	Disjunctive syllogism
p ------------------ ∴ (p v q)	p → (p v q)	Addition
p ^ q ----------------------- ∴ p	(p ^ q) → p	Simplification
p q -------------------- ∴ (p ^ q)	(p) ^ (q) → (p ^ q)	Conjunction
p v q ¬p v r ---------------- ∴ q v r	(p v q) ^ (¬p v r) → (q v r)	Resolution

RULES OF INFERENCE

EXAMPLE

State which rule of inference is the basis of the following statement:

- "it is below freezing now. Therefore, it is either freezing or raining now"
- SOLTUION:
- Let p: "it is below freezing now"

  q: "it is raining now"

Then this argument is of the form

p

------------- (Addition)

$\therefore$ p v q

Rule of Inference

EXAMPLE

- " it is below freezing and it is raining now. Therefore, it is below freezing"

SOLUTION:

Let p: "it is below freezing now"

q: "it is raining now"

Then this argument is of the form

$p \wedge q$

----------- (Simplification)

$\therefore p$

Using Rules of Inference to Build Arguments

- When there are many premises, several rules of inference are often needed to show that an argument is valid.

USING RULES OF INFERENCE TO BUILD ARGUMENTS

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, we will be home by sunset." lead to the conclusion " We will be home by sunset"

Using Rules of Inference

- SOLUTION
- Let 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"

  The hypotheses become

  $\neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t$

  the conclusion is t

CONT'D

- We construct an argument to show that our hypotheses lead to desired conclusion as follows

Step	Reason
1. $\neg p \wedge q$	Hypothesis
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Hypothesis
4. $\neg r$	Modus tollens (2,3)
5. $\neg r \rightarrow s$	Hypothesis
6. s	Modus ponens (4,5)
7. $s \rightarrow t$	Hypothesis
8. t	Modus ponens (6,7)

Note that if we used the truth table, we would end up with 32 rows !!!

RESOLUTION

- Computer programs make use of rule of inference called resolution to automate the task of reasoning and proving theorems
- This rule of inference is based on the tautology

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

RESOLUTION

- EXAMPLE

  Use resolution to show that the hypotheses

  "Jasmine is skiing or it is not snowing" and "it is snowing or Bart is playing hockey" imply that "Jasmine is skiing or Bart is playing hockey"

RESOLUTION

SOLUTION

p: “it is snowing”,

q: “Jasmine is skiing”,

r: “Bart is playing hockey”

We can represent the hypotheses as

$\neg p \vee q$ and $p \vee r$, respectively

Using Resolution, the proposition $q \vee r$, “Jasmine is skiing or Bart is playing hockey” follows

SOME TERMINOLOGY

- **Theorem:** is a statement that can be shown to be true. (fact or result)
- We demonstrate that a theorem is true with **proof**
- **Proofs:** valid arguments that establish the truth of mathematical statements.
- **Axioms (postulates):** Statements that used in a proof and are assumed to be true.
- **Proof Methods**

Proving $p \rightarrow q$

Direct proof: Assume p is true, and prove q.

Indirect proof: Assume $\neg q$, and prove $\neg p$.

Direct proof

Proving p → q

Direct proof: Assume p is true, and prove q

Direct proofs lead from the hypothesis of a theorem to the conclusion.

They begin with the premises; continue with a sequence of deductions, and ends with the conclusion.

Direct proof

Definition 1:

The integer **n** is **even** if there exists an integer **k** such that **n=2k**, and

n is **odd** if there exists an integer **k** such that **n=2k+1**.

Axiom: Every integer is either odd or even

DIRECT PROOF

Example 1:

Give direct proof that : **Theorem :** "If n is an odd integer, then n^2 is an odd integer".

Proof

We assume that the hypothesis of this condition is true " n is odd"

$n = 2k+1$ for some integer k

We want to show that n^2 is odd ,

thus $n^2 = (2k+1)^2$

$n^2 = 4k^2 + 4k + 1$

$n^2 = 2(2k^2 + 2k) + 1$

Therefore n^2 is of the form $2j + 1$

(with j the integer $2k^2 + 2k$), **thus** n^2 is odd

DIRECT PROOF

Example

Prove that if n is an integer and 3n+2 is odd, then n is odd.

We assume that 3n+2 is an odd integer

This mean that $3n+2=2k+1$

There is no direct way to proof that n is odd integer (Direct proof often reaches dead ends.)

INDIRECT PROOF

We need other method of proving theorem of $p \rightarrow q$, which is not direct

which don't start with the hypothesis and end with the conclusion (we call it **indirect proof**)

Indirect proof (proof by contraposition): Assume $\neg q$, and prove $\neg p$.

Contraposition ($p \rightarrow q \equiv \neg q \rightarrow \neg p$)

We take $\neg$ q as hypothesis , and using axioms , definitions any proven theorem to follow **$\neg$p**

Indirect proof

Example 3:
Prove that if n is an integer and 3n+2 is odd, then n is odd.

Proof

Suppose that the conclusion is false, *i.e.*, that n is even (¬q)

Then $n=2k$ for some integer k.

Then $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$.

Thus $3n+2$ is even, because it equals $2j$ for integer $j = 3k+1$.

So $3n+2$ is not odd ¬p

We have shown that ¬(n is odd)→¬($3n$+2 is odd), **thus** its contraposition ($3n$+2 is odd) → (n is odd) is also true.

Definition 2:

The real number **r** is **rational** if there exist integers **p** and **q** with **q≠0** such that **r =p/q**.

A real number that is **not rational** is called **irrational**

Examples Proof Methods

- Example 7:

Theorem: Prove that the sum of two rational numbers is rational.

- Proof
  - assume that r and s are rational numbers
  - $r=p/q$ and $s=t/u$ where p,q,t,u are integers and $p\neq 0$, $u\neq 0$
  - $r+s=(p/q)+(t/u) = (pu+qt)/(qu)$
  - Because $p\neq 0$ and $u\neq 0$, then $qu\neq 0$
  - Both (pu+qt) and (qu) are integers
  - Then the theorem is proved
  - **Note that** **:**Our attempt to find direct proof succeeded

Proofs of Equivalence

- To prove a theorem that is a bi-conditional statement $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.
- To prove a theorem that states several propositions to be equivalent $p1 \leftrightarrow p2 \leftrightarrow p3 \dots \leftrightarrow pn$,

  we must show that $p1 \rightarrow p2$, $p2 \rightarrow p3, \dots pn \rightarrow p1$

Proofs of Equivalence

- Example: Show that these statements are equivalent:
  - p1: n is even
  - p2: n -1 is odd
  - p3: n^2 is even

COUNTEREXAMPLES

- To prove a statement of the form $\forall x\, P(x)$ to be false we look for a counter example.

- Example: prove or disprove the statement

  If x and y are real number, $(x^2 = y^2) \leftrightarrow (x=y)$

- Solution:

  -3,3 are real number and $(-3)^2 = 3^2$ but $-3 \neq 3$

Hence the result is false and implication is false

Any Questions?

- Refer to Chapter 1 for further reading