1 Propositions and Predicates

Mathematical logic is the foundation on which the proofs and arguments rest. Propositions are statements used in mathematical logic, which are either true or false but not both and we can definitely say whether a proposition is true or false.

In this chapter we introduce propositions and logical connectives. Normal forms for well-formed formulas are given. Predicates are introduced. Finally, we discuss the rules of inference for propositional calculus and predicate calculus.

1.1 PROPOSITIONS (OR STATEMENTS)

A proposition (or a statement) is classified as a declarative sentence to which only one of the truth values, i.e. true or false, can be assigned. When a proposition is true, we say that its truth value is *T*. When it is false, we say that its truth value is *F*.

Consider, for example, the following sentences in English:

1. New Delhi is the capital of India.
2. The square of 4 is 16.
3. The square of 5 is 27.
4. Every college will have a computer by 2010 A.D.
5. Mathematical logic is a difficult subject.
6. Chennai is a beautiful city.
7. Bring me coffee.
8. No, thank you.
9. This statement is false.

The sentences 1–3 are propositions. The sentences 1 and 2 have the truth value *T*. The sentence 3 has the truth value *F*. Although we cannot *know* the truth value of 4 at present, we definitely know that it is true or false, but not both.

So the sentence 4 is a proposition. For the same reason, the sentences 5 and 6 are propositions. To sentences 7 and 8, we cannot assign truth values as they are not declarative sentences. The sentence 9 looks like a proposition. However, if we assign the truth value T to sentence 9, then the sentence asserts that it is false. If we assign the truth value F to sentence 9, then the sentence asserts that it is true. Thus the sentence 9 has either both the truth values (or none of the two truth values). Therefore, the sentence 9 is not a proposition.

We use capital letters to denote propositions.

1.1.1 Connectives (Propositional Connectives or Logical Connectives)

Just as we form new sentences from the given sentences using words like 'and', 'but', 'if', we can get new propositions from the given propositions using 'connectives'. But a new sentence obtained from the given propositions using connectives will be a proposition only when the new sentence has a truth value either T or F (but not both). The truth value of the new sentence depends on the (logical) connectives used and the truth value of the given propositions.

We now define the following connectives. There are five basic connectives.

(i) Negation (NOT)
(ii) Conjunction (AND)
(iii) Disjunction (OR)
(iv) Implication (IF ... THEN ...)
(v) If and Only If.

Negation (NOT)

If P is a proposition then the negation P or NOT P (read as 'not P') is a proposition (denoted by $\neg P$) whose truth value is T if P has the truth value F, and whose truth value is F if P has the truth value T. Usually, the truth values of a proposition defined using a connective are listed in a table called the **truth table** for that connective (Table 1.1).

TABLE 1.1 Truth Table for Negation

P	$\neg P$
T	F
F	T

Conjunction (AND)

If P and Q are two propositions, then the conjunction of P and Q (read as 'P and Q') is a proposition (denoted by $P \wedge Q$) whose truth values are as given in Table 1.2.

TABLE 1.2 Truth Table for Conjunction

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction (OR)

If P and Q are two propositions, then the disjunction of P and Q (read as 'P or Q') is a proposition (denoted by $P \vee Q$) whose truth values are as given in Table 1.3.

TABLE 1.3 Truth Table for Disjunction

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

It should be noted that $P \vee Q$ is true if P is true or Q is true or both are true. This OR is known as *inclusive* OR, i.e. either P is true or Q is true or both are true. Here we have defined OR in the inclusive sense. We will define another connective called *exclusive* OR (either P is true or Q is true, but not both, i.e. where OR is used in the exclusive sense) in the Exercises at the end of this chapter.

EXAMPLE 1.1

If P represents 'This book is good' and Q represents 'This book is cheap', write the following sentences in symbolic form:

(a) This book is good and cheap.
(b) This book is not good but cheap.
(c) This book is costly but good.
(d) This book is neither good nor cheap.
(e) This book is either good or cheap.

Solution

(a) $P \wedge Q$
(b) $\neg P \wedge Q$
(c) $\neg Q \wedge P$
(d) $\neg P \wedge \neg Q$
(e) $P \vee Q$

Note: The truth tables for $P \wedge Q$ and $Q \wedge P$ coincide. So $P \wedge Q$ and $Q \wedge P$ are equivalent (for the definition, see Section 1.1.4). But in natural languages this need not happen. For example, the two sentences,

namely 'I went to the railway station and boarded the train', and 'I boarded the train and went to the railway station', have different meanings. Obviously, we cannot write the second sentence in place of the first sentence.

Implication (IF ... THEN ...)

If P and Q are two propositions, then 'IF P THEN Q' is a proposition (denoted by $P \Rightarrow Q$) whose truth values are given Table 1.4. We also read $P \Rightarrow Q$ as 'P implies Q'.

TABLE 1.4 Truth Table for Implication

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

We can note that $P \Rightarrow Q$ assumes the truth value F only if P has the truth value T and Q has the truth value F. In all the other cases, $P \Rightarrow Q$ assumes the truth value T. In the case of natural languages, we are concerned about the truth values of the sentence 'IF P THEN Q' only when P is true. When P is false, we are not concerned about the truth value of 'IF P THEN Q'. But in the case of mathematical logic, we have to definitely specify the truth value of $P \Rightarrow Q$ in all cases. So the truth value of $P \Rightarrow Q$ is defined as T when P has the truth value F (irrespective of the truth value of Q).

EXAMPLE 1.2

Find the truth values of the following propositions:

(a) If 2 is not an integer, then 1/2 is an integer.
(b) If 2 is an integer, then 1/2 is an integer.

Solution

Let P and Q be '2 is an integer', '1/2 is an integer', respectively. Then the proposition (a) is true (as P is false and Q is false) and the proposition (b) is false (as P is true and Q is false).

The above example illustrates the following: 'We can prove anything if we start with a false assumption.' We use $P \Rightarrow Q$ whenever we want to 'translate' any one of the following: 'P only if Q', 'P is a sufficient condition for Q', 'Q is a necessary condition for P', 'Q follows from P', 'Q whenever P', 'Q provided P'.

If and Only If

If P and Q are two statements, then 'P if and only if Q' is a statement (denoted by $P \Leftrightarrow Q$) whose truth value is T when the truth values of P and Q are the same and whose truth value is F when the statements differ. The truth values of $P \Leftrightarrow Q$ are given in Table 1.5.

TABLE 1.5 Truth Table for If and Only If

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Table 1.6 summarizes the representation and meaning of the five logical connectives discussed above.

TABLE 1.6 Five Basic Logical Connectives

Connective	*Resulting proposition*	*Read as*
Negation $\neg$	$\neg P$	Not P
Conjunction $\wedge$	$P \wedge Q$	P and Q
Disjunction $\vee$	$P \vee Q$	P or Q (or both)
Implication $\Rightarrow$	$P \Rightarrow Q$	If P then Q (P implies Q)
If and only if $\Leftrightarrow$	$P \Leftrightarrow Q$	P if and only if Q

EXAMPLE 1.3

Translate the following sentences into propositional forms:

(a) If it is not raining and I have the time, then I will go to a movie.
(b) It is raining and I will not go to a movie.
(c) It is not raining.
(d) I will not go to a movie.
(e) I will go to a movie only if it is not raining.

Solution

Let P be the proposition 'It is raining'.
Let Q be the proposition 'I have the time'.
Let R be the proposition 'I will go to a movie'.

Then

(a) $(\neg P \wedge Q) \Rightarrow R$
(b) $P \wedge \neg R$
(c) $\neg P$
(d) $\neg R$
(e) $R \Rightarrow \neg P$

EXAMPLE 1.4

If P, Q, R are the propositions as given in Example 1.3, write the sentences in English corresponding to the following propositional forms:

(a) $(\neg P \wedge Q) \Leftrightarrow R$
(b) $(Q \Rightarrow R) \wedge (R \Rightarrow Q)$
(c) $\neg (Q \vee R)$
(d) $R \Rightarrow \neg P \wedge Q$

Solution

(a) I will go to a movie if and only if it is not raining and I have the time.
(b) I will go to a movie if and only if I have the time.
(c) It is not the case that I have the time or I will go to a movie.
(d) I will go to a movie, only if it is not raining or I have the time.

1.1.2 WELL-FORMED FORMULAS

Consider the propositions $P \wedge Q$ and $Q \wedge P$. The truth tables of these two propositions are identical irrespective of any proposition in place of P and any proposition in place of Q. So we can develop the concept of a propositional variable (corresponding to propositions) and well-formed formulas (corresponding to propositions involving connectives).

Definition 1.1 A propositional variable is a symbol representing any proposition. We note that usually a real variable is represented by the symbol x. This means that x is not a real number but can take a real value. Similarly, a propositional variable is not a proposition but can be replaced by a proposition.

Usually a mathematical object can be defined in terms of the property/condition satisfied by the mathematical object. Another way of defining a mathematical object is by recursion. Initially some objects are declared to follow the definition. The process by which more objects can be constructed is specified. This way of defining a mathematical object is called a *recursive* definition. This corresponds to a function calling itself in a programming language.

The factorial $n!$ can be defined as $n(n-1) \ldots 2.1$. The recursive definition of $n!$ is as follows:

$$0! = 1, \qquad n! = n(n-1)!$$

Definition 1.2 A well-formed formula (wff) is defined recursively as follows:

(i) If P is a propositional variable, then it is a wff.
(ii) If α is a wff, then $\neg \alpha$ is a wff.
(iii) If α and β are well-formed formulas, then $(\alpha \vee \beta)$, $(\alpha \wedge \beta)$, $(\alpha \Rightarrow \beta)$, and $(\alpha \Leftrightarrow \beta)$ are well-formed formulas.
(iv) A string of symbols is a wff if and only if it is obtained by a finite number of applications of (i)–(iii).

Notes: (1) A wff is not a proposition, but if we substitute a proposition in place of a propositional variable, we get a proposition. For example:

(i) $\neg (P \vee Q) \wedge (\neg Q \wedge R) \Rightarrow Q$ is a wff.
(ii) $(\neg P \wedge Q) \Leftrightarrow Q$ is a wff.

(2) We can drop parentheses when there is no ambiguity. For example, in propositions we can remove the outermost parentheses. We can also specify the hierarchy of connectives and avoid parentheses.

For the sake of convenience, we can refer to a wff as a formula.

1.1.3 TRUTH TABLE FOR A WELL-FORMED FORMULA

If we replace the propositional variables in a formula α by propositions, we get a proposition involving connectives. The table giving the truth values of such a proposition obtained by replacing the propositional variables by arbitrary propositions is called the truth table of α.

If α involves n propositional constants, then we have 2^n possible combinations of truth values of propositions replacing the variables.

EXAMPLE 1.5

Obtain the truth table for $\alpha = (P \vee Q) \wedge (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Solution

The truth values of the given wff are shown in Table 1.7.

TABLE 1.7 Truth Table of Example 1.5

P	Q	$P \vee Q$	$P \Rightarrow Q$	$(P \vee Q) \wedge (P \Rightarrow Q)$	$(Q \Rightarrow P)$	α
T	T	T	T	T	T	T
T	F	T	F	F	T	F
F	T	T	T	T	F	F
F	F	F	T	F	T	F

EXAMPLE 1.6

Construct the truth table for $\alpha = (P \vee Q) \Rightarrow ((P \vee R) \Rightarrow (R \vee Q))$.

Solution

The truth values of the given formula are shown in Table 1.8.

TABLE 1.8 Truth Table of Example 1.6

P	Q	R	$P \vee R$	$R \vee Q$	$(P \vee R) \Rightarrow (R \vee Q)$	$(P \vee Q)$	α
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T
F	F	T	T	T	T	F	T
F	F	F	F	F	T	F	T

Some formulas have the truth value T for all possible assignments of truth values to the propositional variables. For example, $P \vee \neg P$ has the truth value T irrespective of the truth value of P. Such formulas are called *tautologies*.

Definition 1.3 A tautology or a universally true formula is a well-formed formula whose truth value is T for all possible assignments of truth values to the propositional variables.

For example, $P \vee \neg P$, $(P \wedge Q) \Rightarrow P$, and $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ are tautologies.

Note: When it is not clear whether a given formula is a tautology, we can construct the truth table and verify that the truth value is T for all combinations of truth values of the propositional variables appearing in the given formula.

EXAMPLE 1.7

Show that $\alpha = (P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$ is a tautology.

Solution

We give the truth values of α in Table 1.9.

TABLE 1.9 Truth Table of Example 1.7

P	Q	R	$Q \Rightarrow R$	$P \Rightarrow (Q \Rightarrow R)$	$P \Rightarrow Q$	$P \Rightarrow R$	$(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$	α
T	T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	F	T
T	F	T	T	T	F	T	T	T
T	F	F	T	T	F	F	T	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	F	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

Definition 1.4 A contradiction (or absurdity) is a wff whose truth value is F for all possible assignments of truth values to the propositional variables. For example,

$$P \wedge \neg P \quad \text{and} \quad (P \wedge Q) \wedge \neg Q$$

are contradictions.

Note: α is a contradiction if and only if $\neg \alpha$ is a tautology.

1.1.4 Equivalence of Well-formed Formulas

Definition 1.5 Two wffs α and β in propositional variables $P_1, P_2, \ldots, P_n$ are equivalent (or logically equivalent) if the formula $\alpha \Leftrightarrow \beta$ is a tautology. When α and β are equivalent, we write $\alpha \equiv \beta$.

Notes: (1) The wffs α and β are equivalent if the truth tables for α and β are the same. For example,

$$P \wedge Q \equiv Q \wedge P \quad \text{and} \quad P \wedge P \equiv P$$

(2) It is important to note the difference between $\alpha \Leftrightarrow \beta$ and $\alpha \equiv \beta$. $\alpha \Leftrightarrow \beta$ is a formula, whereas $\alpha \equiv \beta$ is not a formula but it denotes the relation between α and β.

EXAMPLE 1.8

Show that $(P \Rightarrow (Q \vee R)) \equiv ((P \Rightarrow Q) \vee (P \Rightarrow R))$.

Solution

Let $\alpha = (P \Rightarrow (Q \vee R))$ and $\beta = ((P \Rightarrow Q) \vee (P \Rightarrow R))$. We construct the truth values of α and β for all assignments of truth values to the variables P, Q and R. The truth values of α and β are given in Table 1.10.

TABLE 1.10 Truth Table of Example 1.8

P	Q	R	$Q \vee R$	$P \Rightarrow (Q \vee R)$	$P \Rightarrow Q$	$P \Rightarrow R$	$(P \Rightarrow Q) \vee (P \Rightarrow R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	F	F	F	T	T	T	T

As the columns corresponding to α and β coincide, $\alpha \equiv \beta$.

As the truth value of a tautology is T, irrespective of the truth values of the propositional variables, we denote any tautology by **T**. Similarly, we denote any contradiction by **F**.

1.1.5 Logical Identities

Some equivalences are useful for deducing other equivalences. We call them identities and give a list of such identities in Table 1.11.

The identities I_1–I_{12} can be used to simplify formulas. If a formula β is part of another formula α, and β is equivalent to β', then we can replace β by β' in α and the resulting wff is equivalent to α.

TABLE 1.11 Logical Identities

I_1	Idempotent laws	$P \vee P \equiv P$, $P \wedge P \equiv P$
I_2	Commutative laws	$P \vee Q \equiv Q \vee P$, $P \wedge Q \equiv Q \wedge P$
I_3	Associative laws	$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$, $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
I_4	Distributive laws	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$, $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
I_5	Absorption laws	$P \vee (P \wedge Q) \equiv P$, $P \wedge (P \vee Q) \equiv P$
I_6	DeMorgan's laws	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$, $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
I_7	Double negation	$P \equiv \neg(\neg P)$
I_8		$P \vee \neg P \equiv \mathbf{T}$, $P \wedge \neg P \equiv \mathbf{F}$
I_9		$P \vee \mathbf{T} \equiv \mathbf{T}$, $P \wedge \mathbf{T} \equiv P$, $P \vee \mathbf{F} \equiv P$, $P \wedge \mathbf{F} \equiv \mathbf{F}$
I_{10}		$(P \Rightarrow Q) \wedge (P \Rightarrow \neg Q) \equiv \neg P$
I_{11}	Contrapositive	$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$
I_{12}		$P \Rightarrow Q \equiv (\neg P \vee Q)$

EXAMPLE 1.9

Show that $(P \wedge Q) \vee (P \wedge \neg Q) \equiv P$.

Solution

L.H.S. $= (P \wedge Q) \vee (P \wedge \neg Q)$

$\equiv P \wedge (Q \vee \neg Q)$ by using the distributive law (i.e. I_4)

$\equiv P \wedge \mathbf{T}$ by using I_8

$\equiv P$ by using I_9

$=$ R.H.S.

EXAMPLE 1.10

Show that $(P \Rightarrow Q) \wedge (R \Rightarrow Q) \equiv (P \vee R) \Rightarrow Q$

Solution

L.H.S. $= (P \Rightarrow Q) \wedge (R \Rightarrow Q)$

$\equiv (\neg P \vee Q) \wedge (\neg R \vee Q)$ by using I_{12}

$\equiv (Q \vee \neg P) \wedge (Q \vee \neg R)$ by using the commutative law (i.e. I_2)

$\equiv Q \vee (\neg P \wedge \neg R)$ by using the distributive law (i.e. I_4)

$\equiv Q \vee (\neg (P \vee R))$ by using the DeMorgan's law (i.e. I_6)

$\equiv (\neg (P \vee R)) \vee Q$ by using the commutative law (i.e. I_2)

$\equiv (P \vee R) \Rightarrow Q$ by using I_{12}

$=$ R.H.S.

1.2 NORMAL FORMS OF WELL-FORMED FORMULAS

We have seen various well-formed formulas in terms of two propositional variables, say, P and Q. We also know that two such formulas are equivalent if and only if they have the same truth table. The number of distinct truth tables for formulas in P and Q is 2^4. (As the possible combinations of truth values of P and Q are TT, TF, FT, FF, the truth table of any formula in P and Q has four rows. So the number of distinct truth tables is 2^4.) Thus there are only 16 distinct (nonequivalent) formulas, and any formula in P and Q is equivalent to one of these 16 formulas.

In this section we give a method of reducing a given formula to an equivalent form called the 'normal form'. We also use 'sum' for disjunction, 'product' for conjunction, and 'literal' either for P or for $\neg P$, where P is any propositional variable.

Definition 1.6 An elementary product is a product of literals. An elementary sum is a sum of literals. For example, $P \wedge \neg Q$, $\neg P \wedge \neg Q$, $P \wedge Q$, $\neg P \wedge Q$ are elementary products. And $P \vee \neg Q$, $P \vee \neg R$ are elementary sums.

Definition 1.7 A formula is in disjunctive normal form if it is a sum of elementary products. For example, $P \vee (Q \wedge R)$ and $P \vee (\neg Q \wedge R)$ are in disjunctive normal form. $P \wedge (Q \vee R)$ is not in disjunctive normal form.

1.2.1 CONSTRUCTION TO OBTAIN A DISJUNCTIVE NORMAL FORM OF A GIVEN FORMULA

Step 1 Eliminate $\Rightarrow$ and $\Leftrightarrow$ using logical identities. (We can use I_{12}, i.e. $P \Rightarrow Q \equiv (\neg P \vee Q)$.)

Step 2 Use DeMorgan's laws (I_6) to eliminate $\neg$ before sums or products. The resulting formula has $\neg$ only before the propositional variables, i.e. it involves sum, product and literals.

Step 3 Apply distributive laws (I_4) repeatedly to eliminate the product of sums. The resulting formula will be a sum of products of literals, i.e. sum of elementary products.

EXAMPLE 1.11

Obtain a disjunctive normal form of

$$P \vee (\neg P \Rightarrow (Q \vee (Q \Rightarrow \neg R)))$$

Solution

$P \vee (\neg P \Rightarrow (Q \vee (Q \Rightarrow \neg R)))$

$\equiv P \vee (\neg P \Rightarrow (Q \vee (\neg Q \vee \neg R)))$ (step 1 using I_{12})

$\equiv P \vee (P \vee (Q \vee (\neg Q \vee \neg R)))$ (step 1 using I_{12} and I_7)

$\equiv P \vee P \vee Q \vee \neg Q \vee \neg R$ by using I_3

$\equiv P \vee Q \vee \neg Q \vee \neg R$ by using I_1

Thus, $P \vee Q \vee \neg Q \vee \neg R$ is a disjunctive normal form of the given formula.

EXAMPLE 1.12

Obtain the disjunctive normal form of

$$(P \wedge \neg (Q \wedge R)) \vee (P \Rightarrow Q)$$

Solution

$(P \wedge \neg (Q \wedge R)) \vee (P \Rightarrow Q)$

$\equiv (P \wedge \neg (Q \wedge R)) \vee (\neg P \vee Q)$ (step 1 using I_{12})

$\equiv (P \wedge (\neg Q \vee \neg R)) \vee (\neg P \vee Q)$ (step 2 using I_7)

$\equiv (P \wedge \neg Q) \vee (P \wedge \neg R) \vee \neg P \vee Q$ (step 3 using I_4 and I_3)

Therefore, $(P \wedge \neg Q) \vee (P \wedge \neg R) \vee \neg P \vee Q$ is a disjunctive normal form of the given formula.

For the same formula, we may get different disjunctive normal forms. For example, $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)$ and $P \wedge Q$ are disjunctive normal forms of $P \wedge Q$. So, we introduce one more normal form, called *the principal disjunctive normal form* or the *sum-of-products canonical form* in the next definition. The advantages of constructing the principal disjunctive normal form are:

(i) For a given formula, its principal disjunctive normal form is unique.

(ii) Two formulas are equivalent if and only if their principal disjunctive normal forms coincide.

Definition 1.8 A minterm in n propositional variables $P_1, \ldots, P_n$ is $Q_1 \wedge Q_2 \ldots \wedge Q_n$, where each Q_i is either P_i or $\neg P_i$.

For example, the minterms in P_1 and P_2 are $P_1 \wedge P_2$, $\neg P_1 \wedge P_2$, $P_1 \wedge \neg P_2$, $\neg P_1 \wedge \neg P_2$. The number of minterms in n variables is 2^n.

Definition 1.9 A formula α is in principal disjunctive normal form if α is a sum of minterms.

1.2.2 Construction to Obtain the Principal Disjunctive Normal Form of a Given Formula

Step 1 Obtain a disjunctive normal form.

Step 2 Drop the elementary products which are contradictions (such as $P \wedge \neg P$).

Step 3 If P_i and $\neg P_i$ are missing in an elementary product α, replace α by $(\alpha \wedge P_i) \vee (\alpha \wedge \neg P_i)$.

Step 4 Repeat step 3 until all the elementary products are reduced to sum of minterms. Use the idempotent laws to avoid repetition of minterms.

EXAMPLE 1.13

Obtain the canonical sum-of-products form (i.e. the principal disjunctive normal form) of

$$\alpha = P \vee (\neg P \wedge \neg Q \wedge R)$$

Solution

Here α is already in disjunctive normal form. There are no contradictions. So we have to introduce the missing variables (step 3). $\neg P \wedge \neg Q \wedge R$ in α is already a minterm. Now,

$P \equiv (P \wedge Q) \vee (P \wedge \neg Q)$

$\equiv ((P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$

$\equiv ((P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)) \vee ((P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R))$

Therefore, the canonical sum-of-products form of α is

$$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$$

EXAMPLE 1.14

Obtain the principal disjunctive normal form of

$$\alpha = (\neg P \vee \neg Q) \Rightarrow (\neg P \wedge R)$$

Solution

$\alpha = (\neg P \vee \neg Q) \Rightarrow (\neg P \wedge R)$

$\equiv (\neg(\neg P \vee \neg Q)) \vee (\neg P \wedge R)$ by using I_{12}

$\equiv (P \wedge Q) \vee (\neg P \wedge R)$ by using DeMorgan's law

$\equiv ((P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)) \vee ((\neg P \wedge R \wedge Q) \vee (\neg P \wedge R \wedge \neg Q))$

$\equiv (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$

So, the principal disjunctive normal form of α is

$$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$$

A minterm of the form $Q_1 \wedge Q_2 \wedge \ldots \wedge Q_n$ can be represented by $a_1 a_2 \ldots a_n$, where $a_i = 0$ if $Q_i = \neg P_i$ and $a_i = 1$ if $Q_i = P_i$. So the principal disjunctive normal form can be represented by a 'sum' of binary strings. For example, $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$ can be represented by $111 \vee 110 \vee 001$.

The minterms in the two variables P and Q are 00, 01, 10, and 11. Each wff is equivalent to its principal disjunctive normal form. Every principal disjunctive normal form corresponds to the minterms in it, and hence to a

subset of {00, 01, 10, 11}. As the number of subsets is 2^4, the number of distinct formulas is 16. (Refer to the remarks made at the beginning of this section.)

The truth table and the principal disjunctive normal form of α are closely related. Each minterm corresponds to a particular assignment of truth values to the variables yielding the truth value T to α. For example, $P \wedge Q \wedge \neg R$ corresponds to the assignment of T, T, F to P, Q and R, respectively. So, if the truth table of α is given, then the minterms are those which correspond to the assignments yielding the truth value T to α.

EXAMPLE 1.15

For a given formula α, the truth values are given in Table 1.12. Find the principal disjunctive normal form.

TABLE 1.12 Truth Table of Example 1.15

P	Q	R	α
T	T	T	T
T	T	F	F
T	F	T	F
T	F	F	T
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	T

Solution

We have T in the α-column corresponding to the rows 1, 4, 5 and 8. The minterm corresponding to the first row is $P \wedge Q \wedge R$.

Similarly, the minterms corresponding to rows 4, 5 and 8 are respectively $P \wedge \neg Q \wedge \neg R$, $\neg P \wedge Q \wedge R$ and $\neg P \wedge \neg Q \wedge \neg R$. Therefore, the principal disjunctive normal form of α is

$$(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$$

We can form the 'dual' of the disjunctive normal form which is termed the conjunctive normal form.

Definition 1.10 A formula is in conjunctive normal form if it is a product of elementary sums.

If α is in disjunctive normal form, then $\neg \alpha$ is in conjunctive normal form. (This can be seen by applying the DeMorgan's laws.) So to obtain the conjunctive normal form of α, we construct the disjunctive normal form of $\neg \alpha$ and use negation.

Definition 1.11 A maxterm in n propositional variables $P_1, P_2, \cdots, P_n$ is $Q_1 \vee Q_2 \vee \cdots \vee Q_n$, where each Q_i is either P_i or $\neg P_i$.

Definition 1.12 A formula α is in principal conjunctive normal form if α is a product of maxterms. For obtaining the principal conjunctive normal form of α, we can construct the principal disjunctive normal form of $\neg \alpha$ and apply negation.

EXAMPLE 1.16

Find the principal conjunctive normal form of $\alpha = P \vee (Q \Rightarrow R)$.

Solution

$$\begin{aligned}
\neg \alpha &= \neg (P \vee (Q \Rightarrow R)) \\
&\equiv \neg (P \vee (\neg Q \vee R)) && \text{by using } I_{12} \\
&\equiv \neg P \wedge (\neg (\neg Q \vee R)) && \text{by using DeMorgan's law} \\
&\equiv \neg P \wedge (Q \wedge \neg R) && \text{by using DeMorgan's law and } I_7
\end{aligned}$$

$\neg P \wedge Q \wedge \neg R$ is the principal disjunctive normal form of $\neg \alpha$. Hence, the principal conjunctive normal form of α is

$$\neg (\neg P \wedge Q \wedge \neg R) = P \vee \neg Q \vee R$$

The logical identities given in Table 1.11 and the normal forms of well-formed formulas bear a close resemblance to identities in Boolean algebras and normal forms of Boolean functions. Actually, the propositions under $\vee$, $\wedge$ and $\neg$ form a Boolean algebra if the equivalent propositions are identified. **T** and **F** act as bounds (i.e. 0 and 1 of a Boolean algebra). Also, the statement formulas form a Boolean algebra under $\vee$, $\wedge$ and $\neg$ if the equivalent formulas are identified.

The normal forms of well-formed formulas correspond to normal forms of Boolean functions and we can 'minimize' a formula in a similar manner.

1.3 RULES OF INFERENCE FOR PROPOSITIONAL CALCULUS (STATEMENT CALCULUS)

In logical reasoning, a certain number of propositions are assumed to be true, and based on that assumption some other propositions are derived (deduced or inferred). In this section we give some important rules of logical reasoning or rules of inference. The propositions that are assumed to be true are called *hypotheses* or *premises*. The proposition derived by using the rules of inference is called a *conclusion*. The process of deriving conclusions based on the assumption of premises is called a *valid argument*. So in a valid argument we are concerned with the process of arriving at the conclusion rather than obtaining the conclusion.

The rules of inference are simply tautologies in the form of implication (i.e. $P \Rightarrow Q$). For example, $P \Rightarrow (P \vee Q)$ is such a tautology, and it is a rule of inference. We write this in the form $\dfrac{P}{\therefore P \vee Q}$. Here P denotes a premise. The proposition below the line, i.e. $P \vee Q$ is the conclusion.

We give in Table 1.13 some of the important rules of inference. Of course, we can derive more rules of inference and use them in valid arguments.

For valid arguments, we can use the rules of inference given in Table 1.13. As the logical identities given in Table 1.11 are two-way implications, we can also use them as rules of inference.

TABLE 1.13 Rules of Inference

Rule of inference	Implication form
RI_1: Addition $\frac{P}{\therefore \neg P \vee \neg Q}$	$P \Rightarrow (P \vee Q)$
RI_2: Conjunction P $\frac{Q}{\therefore P \wedge Q}$	$P \wedge Q \Rightarrow P \wedge Q$
RI_3: Simplification $\frac{P \wedge Q}{\therefore P}$	$(P \wedge Q) \Rightarrow P$
RI_4: Modus ponens P $\frac{P \Rightarrow Q}{\therefore Q}$	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
RI_5: Modus tollens $\neg Q$ $\frac{P \Rightarrow Q}{\therefore \neg P}$	$(\neg Q \wedge (P \Rightarrow Q)) \Rightarrow \neg Q$
RI_6: Disjunctive syllogism $\neg P$ $\frac{P \vee Q}{\therefore Q}$	$(\neg P \wedge (P \vee Q)) \Rightarrow Q$
RI_7: Hypothetical syllogism $P \Rightarrow Q$ $\frac{Q \Rightarrow R}{\therefore P \Rightarrow R}$	$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
RI_8: Constructive dilemma $(P \Rightarrow Q) \wedge (R \Rightarrow S)$ $\frac{P \vee R}{\therefore Q \vee S}$	$((P \Rightarrow Q) \wedge (R \Rightarrow S) \wedge (P \vee R)) \Rightarrow (Q \vee S)$
RI_9: Destructive dilemma $(P \Rightarrow Q) \wedge (R \Rightarrow S)$ $\frac{\neg Q \vee \neg S}{\therefore P \vee R}$	$((P \Rightarrow Q) \wedge (R \Rightarrow S) \wedge (\neg Q \vee \neg S)) \Rightarrow (\neg P \vee \neg R)$

EXAMPLE 1.17

Can we conclude S from the following premises?

(i) $P \Rightarrow Q$
(ii) $P \Rightarrow R$
(iii) $\neg (Q \wedge R)$
(iv) $S \vee P$

Solution

The valid argument for deducing S from the given four premises is given as a sequence. On the left, the well-formed formulas are given. On the right, we indicate whether the proposition is a premise (hypothesis) or a conclusion. If it is a conclusion, we indicate the premises and the rules of inference or logical identities used for deriving the conclusion.

1. $P \Rightarrow Q$	Premise (i)
2. $P \Rightarrow R$	Premise (ii)
3. $(P \Rightarrow Q) \wedge (P \Rightarrow R)$	Lines 1, 2 and RI_2
4. $\neg (Q \wedge R)$	Premise (iii)
5. $\neg Q \vee \neg R$	Line 4 and DeMorgan's law (I_6)
6. $\neg P \vee \neg P$	Lines 3, 5 and destructive dilemma (RI_9)
7. $\neg P$	Idempotent law I_1
8. $S \vee P$	Premise (iv)
9. S	Lines 7, 8 and disjunctive syllogism RI_6

Thus, we can conclude S from the given premises.

EXAMPLE 1.18

Derive S from the following premises using a valid argument:

(i) $P \Rightarrow Q$
(ii) $Q \Rightarrow \neg R$
(iii) $P \vee S$
(iv) R

Solution

1. $P \Rightarrow Q$	Premise (i)
2. $Q \Rightarrow \neg R$	Premise (ii)
3. $P \Rightarrow \neg R$	Lines 1, 2 and hypothetical syllogism RI_7
4. R	Premise (iv)
5. $\neg (\neg R)$	Line 4 and double negation I_2
6. $\neg P$	Lines 3, 5 and modus tollens RI_5
7. $P \vee S$	Premise (iii)
8. S	Lines 6, 7 and disjunctive syllogism RI_6

Thus, we have derived S from the given premises.

EXAMPLE 1.19

Check the validity of the following argument:

If Ram has completed B.E. (Computer Science) or MBA, then he is assured of a good job. If Ram is assured of a good job, he is happy. Ram is not happy. So Ram has not completed MBA.

Solution

We can name the propositions in the following way:

P denotes 'Ram has completed B.E. (Computer Science)'.
Q denotes 'Ram has completed MBA'.
R denotes 'Ram is assured of a good job'.
S denotes 'Ram is happy'.

The given premises are:

(i) $(P \vee Q) \Rightarrow R$
(ii) $R \Rightarrow S$
(iii) $\neg S$

The conclusion is $\neg Q$.

1. $(P \vee Q) \Rightarrow R$	Premise (i)
2. $R \Rightarrow S$	Premise (ii)
3. $(P \vee Q) \Rightarrow S$	Lines 1, 2 and hypothetical syllogism RI_7
4. $\neg S$	Premise (iii)
5. $\neg (P \vee Q)$	Lines 3, 4 and modus tollens RI_5
6. $\neg P \wedge \neg Q$	DeMorgan's law I_6
7. $\neg Q$	Line 6 and simplification RI_3

Thus the argument is valid.

EXAMPLE 1.20

Test the validity of the following argument:

If milk is black then every cow is white. If every cow is white then it has four legs. If every cow has four legs then every buffalo is white and brisk. The milk is black.

Therefore, the buffalo is white.

Solution

We name the propositions in the following way:

P denotes 'The milk is black'.
Q denotes 'Every cow is white'.
R denotes 'Every cow has four legs'.
S denotes 'Every buffalo is white'.
T denotes 'Every buffalo is brisk'.

The given premises are:

(i) $P \Rightarrow Q$
(ii) $Q \Rightarrow R$
(iii) $R \Rightarrow S \wedge T$
(iv) P

The conclusion is S.

1. P	Premise (iv)
2. $P \Rightarrow Q$	Premise (i)
3. Q	Modus ponens RI_4
4. $Q \Rightarrow R$	Premise (ii)
5. R	Modus ponens RI_4
6. $R \Rightarrow S \wedge T$	Premise (iii)
7. $S \wedge T$	Modus ponens RI_4
8. S	Simplification RI_3

Thus the argument is valid.

1.4 PREDICATE CALCULUS

Consider two propositions 'Ram is a student', and 'Sam is a student'. As propositions, there is no relation between them, but we know they have something in common. Both Ram and Sam share the property of being a student. We can replace the two propositions by a single statement 'x is a student'. By replacing x by Ram or Sam (or any other name), we get many propositions. The common feature expressed by 'is a student' is called a *predicate*. In predicate calculus we deal with sentences involving predicates. Statements involving predicates occur in mathematics and programming languages. For example, '$2x + 3y = 4z$', 'IF (D. GE. 0.0) GO TO 20' are statements in mathematics and FORTRAN, respectively, involving predicates. Some logical deductions are possible only by 'separating' the predicates.

1.4.1 PREDICATES

A part of a declarative sentence describing the properties of an object or relation among objects is called a predicate. For example, 'is a student' is a predicate.

Sentences involving predicates describing the property of objects are denoted by $P(x)$, where P denotes the predicate and x is a variable denoting any object. For example, $P(x)$ can denote 'x is a student'. In this sentence, x is a variable and P denotes the predicate 'is a student'.

The sentence 'x is the father of y' also involves a predicate 'is the father of'. Here the predicate describes the relation between two persons. We can write this sentence as $F(x, y)$, Similarly, $2x + 3y = 4z$ can be described by $S(x, y, z)$.

Note: Although $P(x)$ involving a predicate looks like a proposition, it is not a proposition. As $P(x)$ involves a variable x, we cannot assign a truth value to $P(x)$. However, if we replace x by an individual object, we get a proposition. For example, if we replace x by Ram in $P(x)$, we get the proposition 'Ram is a student'. (We can denote this proposition by P(Ram).) If we replace x by 'A cat', then also we get a proposition (whose truth value is F). Similarly, $S(2, 0, 1)$ is the proposition $2 \cdot 2 + 3 \cdot 0 = 4 \cdot 1$ (whose truth value is T). Also, $S(1, 1, 1)$ is the proposition $2 \cdot 1 + 3 \cdot 1 = 4 \cdot 1$ (whose truth value is F).

The following definition is regarding the possible 'values' which can be assigned to variables.

Definition 1.13 For a declarative sentence involving a predicate, the universe of discourse, or simply the universe, is the set of all possible values which can be assigned to variables.

For example, the universe of discourse for $P(x)$: 'x is a student', can be taken as the set of all human names; the universe of discourse for $E(n)$: 'n is an even integer', can be taken as the set of all integers (or the set of all real numbers).

Note: In most examples, the universe of discourse is not specified but can be easily given.

Remark We have seen that by giving values to variables, we can get propositions from declarative sentences involving predicates. Some sentences involving variables can also be assigned truth values. For example, consider 'There exists x such that $x^2 = 5$', and 'For all x, $x^2 = (-x)^2$'. Both these sentences can be assigned truth values (T in both cases). 'There exists' and 'For all' quantify the variables.

Universal and Existential Quantifiers

The phrase 'for all' (denoted by $\forall$) is called the universal quantifier. Using this symbol, we can write 'For all x, $x^2 = (-x)^2$' as $\forall x\, Q(x)$, where $Q(x)$ is '$x^2 = (-x)^2$'.

The phrase 'there exists' (denoted by $\exists$) is called the existential quantifier.

The sentence 'There exists x such that $x^2 = 5$' can be written as $\exists x\, R(x)$, where $R(x)$ is '$x^2 = 5$'.

$P(x)$ in $\forall x\, P(x)$ or in $\exists x\, P(x)$ is called the scope of the quantifier $\forall$ or $\exists$.

Note: The symbol $\forall$ can be read as 'for every', 'for any', 'for each', 'for arbitrary'. The symbol $\exists$ can be read as 'for some', for 'at least one'.

When we use quantifiers, we should specify the universe of discourse. If we change the universe of discourse, the truth value may change. For example, consider $\exists x\, R(x)$, where $R(x)$ is $x^2 = 5$. If the universe of discourse is the set of all integers, then $\exists x\, R(x)$ is false. If the universe of discourse is the set all real numbers, then $\exists x\, R(x)$ is true (when $x = \pm\sqrt{5}$, $x^2 = 5$).

The logical connectives involving predicates can be used for declarative sentences involving predicates. The following example illustrates the use of connectives.

EXAMPLE 1.21

Express the following sentences involving predicates in symbolic form:

1. All students are clever.
2. Some students are not successful.
3. Every clever student is successful.
4. There are some successful students who are not clever.
5. Some students are clever and successful.

Solution

As quantifiers are involved, we have to specify the universe of discourse. We can take the universe of discourse as the set of all students.

Let $C(x)$ denote 'x is clever'.
Let $S(x)$ denote 'x is successful'.

Then the sentence 1 can be written as $\forall x\, C(x)$. The sentences 2–5 can be written as

$$\exists x\, (\neg S(x)), \qquad \forall x\, (C(x) \Rightarrow S(x)),$$
$$\exists x\, (S(x) \wedge \neg C(x)), \qquad \exists x\, (C(x) \neg S(x))$$

1.4.2 Well-formed Formulas of Predicate Calculus

A well-formed formula (wff) of predicate calculus is a string of variables such as $x_1, x_2, \ldots, x_n$, connectives, parentheses and quantifiers defined recursively by the following rules:

(i) $P(x_1, \ldots, x_n)$ is a wff, where P is a predicate involving n variables $x_1, x_2, \ldots, x_n$.
(ii) If α is a wff, then $\neg \alpha$ is a wff.
(iii) If α and β are wffs, then $\alpha \vee \beta$, $\alpha \wedge \beta$, $\alpha \Rightarrow \beta$, $\alpha \Leftrightarrow \beta$ are also wffs.
(iv) If α is a wff and x is any variable, then $\forall x\, (\alpha)$, $\exists x\, (\alpha)$ are wffs.
(v) A string is a wff if and only if it is obtained by a finite number of applications of rules (i)–(iv).

Note: A proposition can be viewed as a sentence involving a predicate with 0 variables. So the propositions are wffs of predicate calculus by rule (i).

We call wffs of predicate calculus as predicate formulas for convenience. The well-formed formulas introduced in Section 1.1 can be called proposition formulas (or statement formulas) to distinguish them from predicate formulas.

Definition 1.14 Let α and β be two predicate formulas in variables $x_1, \ldots, x_n$, and let U be a universe of discourse for α and β. Then α and β are equivalent to each other over U if for every possible assignment of values to each variable in α and β the resulting statements have the same truth values. We can write $\alpha = \beta$ over U.

We say that α and β are equivalent to each other ($\alpha \equiv \beta$) if $\alpha \equiv \beta$ over U for every universe of discourse U.

Remark In predicate formulas the predicate variables may or may not be quantified. We can classify the predicate variables in a predicate formula, depending on whether they are quantified or not. This leads to the following definitions.

Definition 1.15 If a formula of the form $\exists x\, P(x)$ or $\forall x\, P(x)$ occurs as part of a predicate formula α, then such part is called an x-bound part of α, and the occurrence of x is called a bound occurrence of x. An occurrence of x is free if it is not a bound occurrence. A predicate variable in α is free if its occurrence is free in any part of α.

In $\alpha = (\exists x_1\, P(x_1, x_2)) \wedge (\forall x_2\, Q(x_2, x_3))$, for example, the occurrence of x_1 in $\exists x_1\, P(x_1, x_2)$ is a bound occurrence and that of x_2 is free. In $\forall x_2\, Q(x_2, x_3)$, the occurrence of x_2 is a bound occurrence. The occurrence of x_3 in α is free.

Note: The quantified parts of a predicate formula such as $\forall x\, P(x)$ or $\exists x\, P(x)$ are propositions. We can assign values from the universe of discourse only to the free variables in a predicate formula α.

Definition 1.16 A predicate formula is valid if for all possible assignments of values from any universe of discourse to free variables, the resulting propositions have the truth value T.

Definition 1.17 A predicate formula is satisfiable if for some assignment of values to predicate variables the resulting proposition has the truth value T.

Definition 1.18 A predicate formula is unsatisfiable if for all possible assignments of values from any universe of discourse to predicate variables the resulting propositions have the truth value F.

We note that valid predicate formulas correspond to tautologies among proposition formulas and the unsatisfiable predicate formulas correspond to contradictions.

1.5 RULES OF INFERENCE FOR PREDICATE CALCULUS

Before discussing the rules of inference, we note that: (i) the proposition formulas are also the predicate formulas; (ii) the predicate formulas (where all the variables are quantified) are the proposition formulas. Therefore, all the rules of inference for the proposition formulas are also applicable to predicate calculus wherever necessary.

For predicate formulas not involving connectives such as $A(x)$, $P(x, y)$, we can get equivalences and rules of inference similar to those given in Tables 1.11 and 1.13. For Example, corresponding to I_6 in Table 1.11 we get $\neg (P(x) \vee Q(x)) \equiv \neg (P(x)) \wedge \neg (Q(x))$. Corresponding to RI_3 in Table 1.13 $P \wedge Q \Rightarrow P$, we get $P(x) \wedge Q(x) \Rightarrow P(x)$. Thus we can replace propositional variables by predicate variables in Tables 1.11 and 1.13.

Some necessary equivalences involving the two quantifiers and valid implications are given in Table 1.14.

TABLE 1.14 Equivalences Involving Quantifiers

I_{13}	Distributivity of $\exists$ over $\vee$: $\exists x (P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$ $\exists x (P \vee Q(x)) \equiv P \vee (\exists x Q(x))$
I_{14}	Distributivity of $\forall$ over $\wedge$: $\forall x (P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$ $\forall x (P \wedge Q(x)) \equiv P \wedge (\forall x Q(x))$
I_{15}	$\neg (\exists x P(x)) \equiv \forall x \neg (P(x))$
I_{16}	$\neg (\forall x P(x)) \equiv \exists x \neg (P(x))$
I_{17}	$\exists x (P \wedge Q(x)) \equiv P \wedge (\exists x Q(x))$
I_{18}	$\forall x (P \vee Q(x)) \equiv P \vee (\forall x Q(x))$
RI_{10}	$\forall x P(x) \Rightarrow \exists x P(x)$
RI_{11}	$\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x (P(x) \vee Q(x))$
RI_{12}	$\exists x (P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$

Sometimes when we wish to derive some conclusion from a given set of premises involving quantifiers, we may have to eliminate the quantifiers before applying the rules of inference for proposition formulas. Also, when the conclusion involves quantifiers, we may have to introduce quantifiers. The necessary rules of inference for addition and deletion of quantifiers are given in Table 1.15.

TABLE 1.15 Rules of Inference for Addition and Deletion of Quantifiers

RI_{13}:	Universal instantiation $\dfrac{\forall x\, P(x)}{\therefore P(c)}$ c is some element of the universe.
RI_{14}:	Existential instantiation $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ c is some element for which $P(c)$ is true.
RI_{15}:	Universal generalization $\dfrac{P(x)}{\forall x\, P(x)}$ x should not be free in any of the given premises.
RI_{16}:	Existential generalization $\dfrac{P(c)}{\therefore \exists x\, P(x)}$ c is some element of the universe.

EXAMPLE 1.22

Discuss the validity of the following argument:

All graduates are educated.
Ram is a graduate.
Therefore, Ram is educated.

Solution

Let $G(x)$ denote 'x is a graduate'.

Let $E(x)$ denote 'x is educated'.

Let R denote 'Ram'.

So the premises are (i) $\forall x\,(G(x) \Rightarrow E(x))$ and (ii) $G(R)$. The conclusion is $E(R)$.

$\forall x\,(G(x) \Rightarrow E(x))$	Premise (i)
$G(R) \Rightarrow E(R)$	Universal instantiation RI_{13}
$G(R)$	Premise (ii)
$\therefore E(R)$	Modus ponens RI_4

Thus the conclusion is valid.

EXAMPLE 1.23

Discuss the validity of the following argument:

All graduates can read and write.
Ram can read and write.
Therefore, Ram is a graduate.

Solution

Let $G(x)$ denote 'x is a graduate'.
Let $L(x)$ denote 'x can read and write'.
Let R denote 'Ram'.
The premises are: $\forall x\,(G(x) \Rightarrow L(x))$ and $L(R)$.
The conclusion is $G(R)$.
$((G(R) \Rightarrow L(R)) \wedge L(R)) \Rightarrow G(R)$ is not a tautology.
So we cannot derive $G(R)$. For example, a school boy can read and write and he is not a graduate.

EXAMPLE 1.24

Discuss the validity of the following argument.

All educated persons are well behaved.
Ram is educated.
No well-behaved person is quarrelsome.
Therefore, Ram is not quarrelsome.

Solution

Let the universe of discourse be the set of all educated persons.
Let $P(x)$ denote 'x is well-behaved'.
Let y denote 'Ram'.
Let $Q(x)$ denote 'x is quarrelsome'.

So the premises are:

(i) $\forall x\,P(x)$.
(ii) y is a particular element of the universe of discourse.
(iii) $\forall x\,(P(x) \Rightarrow \neg Q(x))$.

To obtain the conclusion, we have the following arguments:

1. $\forall x\,P(x)$	Premise (i)
2. $P(y)$	Universal instantiation RI_{13}
3. $\forall x\,(P(x) \Rightarrow \neg Q(x))$	Premise (iii)
4. $P(y) \Rightarrow \neg Q(y)$	Universal instantiation RI_{13}
5. $P(y)$	Line 2
6. $\neg Q(y)$	Modus ponens RI_4

$\neg Q(y)$ means that 'Ram is not quarrelsome'. Thus the argument is valid.

1.6 SUPPLEMENTARY EXAMPLES

EXAMPLE 1.25

Write the following sentences in symbolic form:

(a) This book is interesting but the exercises are difficult.
(b) This book is interesting but the subject is difficult.
(c) This book is not interesting, the exercises are difficult but the subject is not difficult.
(d) If this book is interesting and the exercises are not difficult then the subject is not difficult.
(e) This book is interesting means that the subject is not difficult, and conversely.
(f) The subject is not difficult but this book is interesting and the exercises are difficult.
(g) The subject is not difficult but the exercises are difficult.
(h) Either the book is interesting or the subject is difficult.

Solution

Let P denote 'This book is interesting'.
Let Q denote 'The exercises are difficult'.
Let R denote 'The subject is difficult'.

Then:

(a) $P \wedge Q$
(b) $P \wedge R$
(c) $\neg P \wedge Q \wedge \neg R$
(d) $(P \wedge \neg Q) \Rightarrow \neg R$
(e) $P \Leftrightarrow \neg R$
(f) $(\neg R) \wedge (P \wedge Q)$
(g) $\neg R \wedge Q$
(h) $\neg P \vee R$

EXAMPLE 1.26

Construct the truth table for $\alpha = (\neg P \Leftrightarrow \neg Q) \Leftrightarrow Q \Leftrightarrow R$

Solution

The truth table is constructed as shown in Table 1.16.

TABLE 1.16 Truth Table of Example 1.26

P	Q	R	$Q \Leftrightarrow R$	$\neg P$	$\neg Q$	$\neg P \Leftrightarrow \neg Q$	α
T	T	T	T	F	F	T	T
T	T	F	F	F	F	T	F
T	F	T	F	F	T	F	T
T	F	F	T	F	T	F	F
F	T	T	T	T	F	F	F
F	T	F	F	T	F	F	T
F	F	T	F	T	T	T	F
F	F	F	T	T	T	T	T

EXAMPLE 1.27

Prove that: $\alpha = ((P \Rightarrow (Q \vee R)) \wedge (\neg Q)) \Rightarrow (P \Rightarrow R)$ is a tautology.

Solution

Let $\beta = (P \Rightarrow (Q \vee R)) \wedge (\neg Q)$

The truth table is constructed as shown in Table 1.17. From the truth table, we conclude that α is a tautology.

TABLE 1.17 Truth Table of Example 1.27

P	Q	R	$\neg Q$	$Q \vee R$	$P \Rightarrow (Q \vee R)$	β	$P \Rightarrow R$	α
T	T	T	F	T	T	F	T	T
T	T	F	F	T	T	F	F	T
T	F	T	T	T	T	T	T	T
T	F	F	T	F	F	F	F	T
F	T	T	F	T	T	F	T	T
F	T	F	F	T	T	F	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	F	T	T	T	T

EXAMPLE 1.28

State the converse, inverse and contrapositive to the following statements:

(a) If a triangle is isoceles, then two of its sides are equal.
(b) If there is no unemployment in India, then the Indians won't go to the USA for employment.

Solution

If $P \Rightarrow Q$ is a statement, then its converse, inverse and contrapositive statements are, $Q \Rightarrow P$, $\neg P \Rightarrow \neg Q$ and $\neg Q \Rightarrow \neg P$, respectively.

(a) Converse—If two of the sides of a triangle are equal, then the triangle is isoceles.

Inverse—If the triangle is not isoceles, then two of its sides are not equal.
Contrapositive—If two of the sides of a triangle are not equal, then the triangle is not isoceles.

(b) Converse—If the Indians won't go to the USA for employment, then there is no unemployment in India.
Inverse—If there is unemployment in India, then the Indians will go to the USA for employment.

(c) Contrapositive—If the Indians go to the USA for employment, then there is unemployment in India.

EXAMPLE 1.29

Show that:

$$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$$

Solution

$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R)$

$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge R) \vee (Q \wedge R) \vee (P \wedge R)$ by using the associative law

$\Leftrightarrow (\neg (P \vee Q) \wedge R) \vee (Q \wedge R) \vee (P \wedge R)$ by using the DeMorgan's law

$\Leftrightarrow (\neg (P \vee Q) \wedge R) \vee (Q \vee P) \wedge R)$ by using the distributive law

$\Leftrightarrow (\neg (P \vee Q) \vee (P \vee Q) \wedge R$ by using the commutative and distributive laws

$\Leftrightarrow \mathbf{T} \wedge R$ by using I_8

$\Leftrightarrow R$ by using I_9

EXAMPLE 1.30

Using identities, prove that:

$Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology

Solution

$Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$

$\Leftrightarrow ((Q \vee P) \wedge (Q \vee \neg Q)) \vee (\neg P \wedge \neg Q)$ by using the distributive law

$\Leftrightarrow ((Q \vee P) \wedge \mathbf{T}) \vee (\neg P \wedge \neg Q)$ by using I_8

$\Leftrightarrow (Q \vee P) \vee \neg (P \vee Q)$ by using the DeMorgan's law and I_9

$\Leftrightarrow (P \vee Q) \vee \neg (P \vee Q)$ by using the commutative law

$\Leftrightarrow \mathbf{T}$ by using I_8

Hence the given formula is a tautology.

EXAMPLE 1.31

Test the validity of the following argument:

If I get the notes and study well, then I will get first class.
I didn't get first class.
So either I didn't get the notes or I didn't study well.

Solution

Let P denote 'I get the notes'.
Let Q denote 'I study well'.
Let R denote 'I will get first class.'
Let S denote 'I didn't get first class.'

The given premises are:

(i) $P \wedge Q \Rightarrow R$
(ii) $\neg R$

The conclusion is $\neg P \vee \neg Q$.

1. $P \wedge Q \Rightarrow R$	Premise (i)
2. $\neg R$	Premise (ii)
3. $\neg (P \wedge Q)$	Lines 1, 2 and modus tollens.
4. $\neg P \vee \neg Q$	DeMorgan's law

Thus the argument is valid.

EXAMPLE 1.32

Explain (a) the conditional proof rule and (b) the indirect proof.

Solution

(a) If we want to prove $A \Rightarrow B$, then we take A as a premise and construct a proof of B. This is called the conditional proof rule. It is denoted by CP.
(b) To prove a formula α, we construct a proof of $\neg \alpha \Rightarrow \mathbf{F}$. In particular, to prove $A \Rightarrow B$, we construct a proof of $A \wedge \neg B \Rightarrow \mathbf{F}$.

EXAMPLE 1.33

Test the validity of the following argument:

Babies are illogical.
Nobody is despised who can manage a crocodile.
Illogical persons are despised.
Therefore babies cannot manage crocodiles.

Solution

Let $B(x)$ denote 'x is a baby'.
Let $I(x)$ denote 'x is illogical'.
Let $D(x)$ denote 'x is despised'.
Let $C(x)$ denote 'x can manage crocodiles'.

Then the premises are:

(i) $\forall x\ (B(x) \Rightarrow I(x))$
(ii) $\forall x\ (C(x) \Rightarrow \neg D(x))$
(iii) $\forall x\ (I(x) \Rightarrow D(x))$

The conclusion is $\forall x\ (B(x) \Rightarrow \neg C(x))$.

1. $\forall x\ (B(x) \Rightarrow I(x))$	Premise (i)
2. $\forall x\ (C(x) \Rightarrow \neg D(x))$	Premise (ii)
3. $\forall x\ (I(x) \Rightarrow D(x))$	Premise (iii)
4. $B(x) \Rightarrow I(x)$	1, Universal instantiation
5. $C(x) \Rightarrow \neg D(x)$	2, Universal instantiation
6. $I(x) \Rightarrow D(x)$	3, Universal instantiation
7. $B(x)$	Premise of conclusion
8. $I(x)$	4,7 Modus pollens
9. $D(x)$	6,8 Modus pollens
10. $\neg C(x)$	5,9 Modus tollens
11. $B(x) \Rightarrow \neg C(x)$	7,10 Conditional proof
12. $\forall x\ (B(x) \Rightarrow \neg C(x))$	11, Universal generalization.

Hence the conclusion is valid.

EXAMPLE 1.34

Give an indirect proof of

$$(\neg Q,\ P \Rightarrow Q,\ P \vee S) \Rightarrow S$$

Solution

We have to prove S. So we include (iv) $\neg S$ as a premise.

1. $P \vee S$	Premise (iii)
2. $\neg S$	Premise (iv)
3. P	1,2, Disjunctive syllogism
4. $P \Rightarrow Q$	Premise (ii)
5. Q	3,4, Modus ponens
6. $\neg Q$	Premise (i)
7. $Q \wedge \neg Q$	5,6, Conjuction
8. $\mathbf{F}$	I_8

We get a contradiction. Hence $(\neg Q,\ P \Rightarrow Q,\ P \vee S) \Rightarrow S$.

EXAMPLE 1.35

Test the validity of the following argument:

All integers are irrational numbers.
Some integers are powers of 2.
Therefore, some irrational number is a power of 2.

Solution

Let $Z(x)$ denote 'x is an integer'.
Let $I(x)$ denote 'x is an irrational number'.
Let $P(x)$ denote 'x is a power of 2'.

The premises are:

(i) $\forall x\,(Z(x) \Rightarrow I(x))$
(ii) $\exists x\,(Z(x) \wedge P(x))$

The conclusion is $\exists x\,(I(x) \wedge P(x))$.

1. $\exists x\,(Z(x) \wedge P(x))$	Premise (ii)
2. $Z(b) \wedge P(b)$	1, Existential instantiation
3. $Z(b)$	2, Simplification
4. $P(b)$	2, Simplification
5. $\forall x\,(Z(x) \Rightarrow I(x))$	Premise (i)
6. $Z(b) \Rightarrow I(b)$	5, Universal instantiation
7. $I(b)$	3,6, Modus ponens
8. $I(b) \wedge P(b)$	7,4 Conjunction
9. $\exists x\,(I(x) \wedge P(x))$	8, Existential instantiation.

Hence the argument is valid.

SELF-TEST

Choose the correct answer to Questions 1–5:

1. The following sentence is not a proposition.
(a) George Bush is the President of India.
(b) $\sqrt{-1}$ is a real number.
(c) Mathematics is a difficult subject.
(d) I wish you all the best.

2. The following is a well-formed formula.
(a) $(P \wedge Q) \Rightarrow (P \vee Q)$
(b) $(P \wedge Q) \Rightarrow (P \vee Q) \wedge R)$
(c) $(P \wedge (Q \wedge R)) \Rightarrow (P \wedge Q))$
(d) $\neg (Q \wedge \neg (P \vee \neg Q)$

3. $\dfrac{P \wedge Q}{\therefore P}$ is called:
   (a) Addition
   (b) Conjunction
   (c) Simplification
   (d) Modus tollens

4. Modus ponens is
   (a) $\neg Q$

   $$\frac{P \Rightarrow Q}{\therefore \neg P}$$

   (b) $\neg P$

   $$\frac{P \vee Q}{\therefore Q}$$

   (c) P

   $$\frac{P \Rightarrow Q}{\therefore Q}$$

   (d) none of the above

5. $\neg P \wedge \neg Q \wedge R$ is a minterm of:
   (a) $P \vee Q$
   (b) $\neg P \wedge \neg Q \wedge R$
   (c) $P \wedge Q \wedge R \wedge S$
   (d) $P \wedge R$

6. Find the truth value of $P \Rightarrow Q$ if the truth values of P and Q are F and T respectively.

7. For what truth values of P, Q and R, the truth value of $(P \Rightarrow Q) \Rightarrow R$ is F?
   (P, Q, R have the truth values F, T, F or F, T, T)

8. If P, Q, R have the truth values F, T, F, respectively, find the truth value of $(P \Rightarrow Q) \vee (P \Rightarrow R)$.

9. State universal generalization.

10. State existential instantiation.

EXERCISES

1.1 Which of the following sentences are propositions?
   (a) A triangle has three sides.
   (b) 11111 is a prime number.
   (c) Every dog is an animal.

(d) Ram ran home.
(e) An even number is a prime number.
(f) 10 is a root of the equation $x^2 - 1002x + 10000 = 0$
(g) Go home and take rest.

1.2 Express the following sentence in symbolic form: For any two numbers a and b, only one of the following holds: $a < b$, $a = b$, and $a > b$.

1.3 The truth table of a connective called Exclusive OR (denoted by $\bar{\vee}$) is shown in Table 1.18.

TABLE 1.18 Truth Table for Exclusive OR

P	Q	$P \bar{\vee} Q$
T	T	F
T	F	T
F	T	T
F	F	F

Give an example of a sentence in English (i) in which Exclusive OR is used, (ii) in which OR is used. Show that $\bar{\vee}$ is associative, commutative and distributive over $\wedge$.

1.4 Find two connectives, using which any other connective can be described.

1.5 The connective NAND denoted by $\uparrow$ (also called the Sheffer stroke) is defined as follows: $P \uparrow Q = \neg (P \wedge Q)$. Show that every connective can be expressed in terms of NAND.

1.6 The connective NOR denoted by $\downarrow$ (also called the Peirce arrow) is defined as follows: $P \downarrow Q = \neg (P \vee Q)$. Show that every connective can be expressed in terms of NOR.

1.7 Construct the truth table for the following:
(a) $(P \vee Q) \Rightarrow ((P \vee R) \Rightarrow (R \vee Q))$
(b) $(P \vee (Q \Rightarrow R)) \Leftrightarrow ((P \vee \neg R) \Rightarrow Q)$

1.8 Prove the following equivalences:
(a) $(\neg P \Rightarrow (\neg P \Rightarrow (\neg P \wedge Q))) \equiv P \vee Q$
(b) $P \equiv (P \vee Q) \wedge (P \vee \neg Q)$
(c) $\neg (P \Leftrightarrow Q) \equiv (P \wedge \neg Q) \vee (\neg P \wedge Q)$

1.9 Prove the logical identities given in Table 1.11 using truth tables.

1.10 Show that $P \Rightarrow (Q \Rightarrow (R \Rightarrow (\neg P \Rightarrow (\neg Q \Rightarrow \neg R))))$ is a tautology.

1.11 Is $(P \Rightarrow \neg P) \Rightarrow \neg P$ (i) a tautology, (ii) a contradiction, (iii) neither a tautology nor a contradiction?

1.12 Is the implication $(P \wedge (P \Rightarrow \neg Q)) \vee (Q \Rightarrow \neg Q) \Rightarrow \neg Q$ a tautology?

1.13 Obtain the principal disjunctive normal form of the following:
(a) $P \Rightarrow (P \Rightarrow Q \wedge (\neg (\neg Q \vee \neg P)))$
(b) $(Q \wedge \neg R \wedge \neg S) \vee (R \wedge S)$.

1.14 Simplify the formula whose principal disjunctive normal form is $110 \vee 100 \vee 010 \vee 000$.

1.15 Test the validity of the following arguments:
(a) $P \Rightarrow Q$

$$\frac{R \Rightarrow \neg Q}{\therefore P \Rightarrow \neg R}$$

(b) $R \Rightarrow \neg Q$
$P \Rightarrow Q$

$$\frac{\neg R \Rightarrow S}{\therefore P \Rightarrow S}$$

(c) P
Q
$\neg Q \Rightarrow R$

$$\frac{Q \Rightarrow \neg R}{\therefore \neg R}$$

(d) $P \Rightarrow Q \wedge R$
$Q \vee S \Rightarrow T$

$$\frac{S \vee P}{\therefore T}$$

1.16 Test the validity of the following argument:
If Ram is clever then Prem is well-behaved.
If Joe is good then Sam is bad and Prem is not well-behaved.
If Lal is educated then Joe is good or Ram is clever.
Hence if Lal is educated and Prem is not well-behaved then Sam is bad.

1.17 A company called for applications from candidates, and stipulated the following conditions:
(a) The applicant should be a graduate.
(b) If he knows Java he should know C++.
(c) If he knows Visual Basic he should know Java.
(d) The applicant should know Visual Basic.

Can you simplify the above conditions?

1.18 For what universe of discourse the proposition $\forall x\,(x \geq 5)$ is true?

1.19 By constructing a suitable universe of discourse, show that

$$\exists x\,(P(x) \Rightarrow Q(x)) \Leftrightarrow (\exists x\,P(x) \Rightarrow \exists x\,Q(x))$$

is not valid.

1.20 Show that the following argument is valid:
All men are mortal.
Socrates is a man.
So Socrates is mortal.

1.21 Is the following sentence true? If philosophers are not money-minded and some money-minded persons are not clever, then there are some persons who are neither philosphers nor clever.

1.22 Test the validity of the following argument:
No person except the uneducated are proud of their wealth.
Some persons who are proud of their wealth do not help others.
Therefore, some uneducated persons cannot help others.

2 Mathematical Preliminaries

In this chapter we introduce the concepts of set theory and graph theory. Also, we define strings and discuss the properties of strings and operations on strings. In the final section we deal with the principle of induction, which will be used for proving many theorems throughout the book.

2.1 SETS, RELATIONS AND FUNCTIONS

2.1.1 SETS AND SUBSETS

A set is a well-defined collection of objects, for example, the set of all students in a college. Similarly, the collection of all books in a college library is also a set. The individual objects are called *members* or *elements* of the set.

We use the capital letters A, B, C, . . . for denoting sets. The small letters a, b, c, . . . are used to denote the elements of any set. When a is an element of the set A, we write $a \in A$. When a is not an element of A, we write $a \notin A$.

Various Ways of Describing a Set

(i) *By listing its elements.* We write all the elements of the set (without repetition) and enclose them within braces. We can write the elements in any order. For example, the set of all positive integers divisible by 15 and less than 100 can be written as {15, 30, 45, 60, 75, 90}.

(ii) *By describing the properties of the elements of the set.* For example, the set {15, 30, 45, 60, 75, 90} can be described as: $\{n \mid n$ is a positive integer divisible by 15 and less than 100$\}$. (The description of the property is called *predicate*. In this case the set is said to be implicitly specified.)

(iii) *By recursion.* We define the elements of the set by a computational rule for calculating the elements. For example, the set of all natural numbers leaving a remainder 1 when divided by 3 can be described as

$$\{a_n \mid a_o = 1,\ a_{n+1} = a_n + 3\}$$

When the computational rule is clear from the context, we simply specify the set by some initial elements. The previous set can be written as {1, 4, 7, 10, . . .}. The four elements given suggest that the computational rule is: $a_{n+1} = a_n + 3$.

Subsets and Operations on Sets

A set A is said to be a subset of B (written as $A \subseteq B$) if every element of A is also an element of B.

Two sets A and B are equal (we write $A = B$) if their members are the same. In practice, to prove that $A = B$, we prove $A \subseteq B$ and $B \subseteq A$.

A set with no element is called an empty set, also called a null set or a void set, and is denoted by $\emptyset$.

We define some operations on sets.

$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$, called the union of A and B.
$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$, called the intersection of A and B.
$A - B = \{x \mid x \in A \text{ and } x \notin B\}$, called the complement of B in A.

A^c denotes $U - A$, where U is the universal set, the set of all elements under consideration.

The set of all subsets of a set A is called the *power set* of A. It is denoted by 2^A.

Let A and B be two sets. Then $A \times B$ is defined as $\{(a, b) \mid a \in A \text{ and } b \in B\}$. ($(a, b)$ is called an ordered pair and is different from (b, a).)

Definition 2.1 Let S be a set. A collection $(A_1, A_2, \ldots, A_n)$ of subsets of S is called a partition if $A_i \cap A_j = \emptyset\ (i \neq j)$ and $S = \bigcup_{i=1}^{n} A_i$ (i.e. $A_1 \cup A_2 \cup \ldots \cup A_n$).

For example, if $S = \{1, 2, 3, \ldots, 10\}$, then $\{\{1, 3, 5, 7, 9\}, \{2, 4, 6, 8, 10\}\}$ is a partition of S.

2.1.2 Sets with One Binary Operation

A binary operation $*$ on a set S is a rule which assigns, to every ordered pair (a, b) of elements from S, a unique element denoted by $a * b$.

Addition, for example, is a binary operation on the set Z of all integers. (Throughout this book, Z denotes the set of all integers.)

Union is a binary operation on 2^A, where A is any nonempty set. We give below five postulates on binary operations.

Postulate 1: *Closure.* If a and b are in S, then $a * b$ is in S.

Postulate 2: *Associativity.* If a, b, c are in S, then $(a * b) * c = a * (b * c)$.

Postulate 3: *Identity element.* There exists a unique element (called the identity element) e in S such that for any element x in S, $x * e = e * x = x$.

Postulate 4: *Inverse.* For every element x in S there exists a unique element x' in S such that $x * x' = x' * x = e$. The element x' is called the inverse of x w.r.t. $*$.

Postulate 5: *Commutativity.* If $a, b \in S$, then $a * b = b * a$.

It may be noted that a binary operation may satisfy none of the above five postulates. For example, let $S = \{1, 2, 3, 4, \ldots\}$, and let the binary operation be subtraction (i.e. $a * b = a - b$). The closure postulate is not satisfied since $2 - 3 = -1 \notin S$. Also, $(2 - 3) - 4 \neq 2 - (3 - 4)$, and so associativity is not satisfied. As we cannot find a positive integer such that $x - e = e - x = x$, the postulates 3 and 4 are not satisfied. Obviously, $a - b \neq b - a$. Therefore, commutativity is not satisfied.

Our interest lies in sets with a binary operation satisfying the postulates.

Definitions (i) A set S with a binary operation $*$ is called a *semigroup* if the postulates 1 and 2 are satisfied.

(ii) A set S with a binary operation $*$ is called a *monoid* if the postulates 1–3 are satisfied.

(iii) A set S with $*$ is called a *group* if the postulates 1–4 are satisfied.

(iv) A semigroup (monoid or group) is called a *commutative* or an *abelian* semigroup (monoid or group) if the postulate 5 is satisfied.

Figure 2.1 gives the relationship between semigroups, monoids, groups, etc. where the numbers refer to the postulate number.

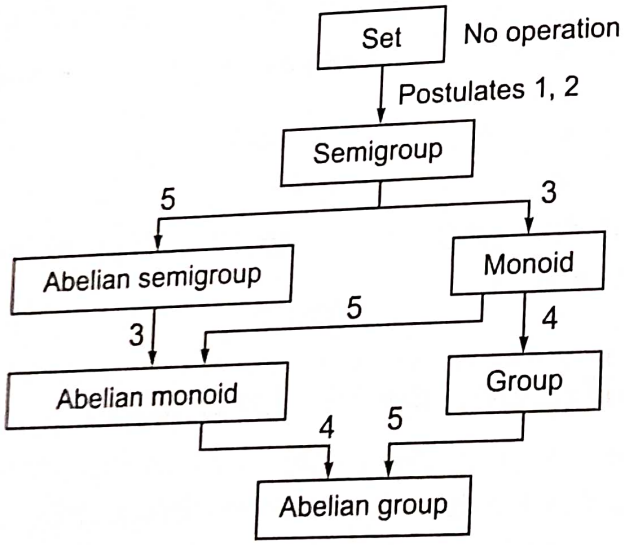

Fig. 2.1 Sets with one binary operation.

We interpret Fig. 2.1 as follows: A monoid satisfying postulate 4 is a group. A group satisfying postulate 5 is an abelian group, etc.

We give below a few examples of sets with one binary operation:

(i) Z with addition is an abelian group.

(ii) Z with multiplication is an abelian monoid. (It is not a group since it does not satisfy the postulate 4.)

(iii) $\{1, 2, 3, \ldots\}$ with addition is a commutative semigroup but not a monoid. (The identity element can be only 0, but 0 is not in the set.)

(iv) The power set 2^A of $A (A \neq \emptyset)$ with union is a commutative monoid. (The identity element is $\emptyset$.)

(v) The set of all 2×2 matrices under multiplication is a monoid but not an abelian monoid.

2.1.3 Sets with Two Binary Operations

Sometimes we come across sets with two binary operations defined on them (for example, in the case of numbers we have addition and multiplication). Let S be a set with two binary operations $*$ and o. We give below 11 postulates in the following way:

(i) Postulates 1–5 refer to $*$ postulates.

(ii) Postulates 6, 7, 8, 10 are simply the postulates 1, 2, 3, 5 for the binary operation o.

(iii) *Postulate* 9: If S under $*$ satisfies the postulates 1–5 then for every x in S, with $x \neq e$, there exists a unique element x' in S such that $x' \text{ o } x = x \text{ o } x' = e'$, where e' is the identity element corresponding to o.

(iv) *Postulate* 11: *Distributivity.* For a, b, c, in S

$$a \text{ o } (b * c) = (a \text{ o } b) * (a \text{ o } c)$$

A set with one or more binary operations is called an algebraic system. For example, groups, monoids, semigroups are algebraic systems with one binary operation.

We now define some algebraic systems with two binary operations.

Definitions (i) A set with two binary operations $*$ and o is called a *ring* if (a) it is an abelian group w.r.t. $*$, and (b) o satisfies the closure, associativity and distributivity postulates (i.e. postulates 6, 7 and 11).

(ii) A ring is called a commutative ring if the commutativity postulate is satisfied for o.

(iii) A commutative ring with unity is a commutative ring that satisfies the identity postulate (i.e. postulate 8) for o.

(iv) A *field* is a set with two binary operations $*$ and o if it satisfies the postulates 1–11.

We now give below a few examples of sets with two binary operations:

(i) Z with addition and multiplication (in place of $*$ and o) is a commutative ring with identity. (The identity element w.r.t. addition is 0, and the identity element w.r.t. multiplication is 1.)

(ii) The set of all rational numbers (i.e. fractions which are of the form a/b, where a is any integer and b is an integer different from zero) is a field. (The identity element w.r.t. multiplication is 1. The inverse of a/b, $a/b \neq 0$ is b/a.)

(iii) The set of all 2×2 matrices with matrix addition and matrix multiplication is a ring with identity, but not a field.

(iv) The power set 2^A ($A \neq \emptyset$) is also a set with two binary operations $\cup$ and $\cap$. The postulates satisfied by $\cup$ and $\cap$ are 1, 2, 3, 5, 6, 7, 8, 10 and 11. The power set 2^A is not a group or a ring or a field. But it is an abelian monoid w.r.t. both the operations $\cup$ and $\cap$.

Figure 2.2 illustrates the relation between the various algebraic systems we have introduced. The interpretation is as given in Fig. 2.1. The numbers refer to postulates. For example, an abelian group satisfying the postulates 6, 7 and 11 is a ring.

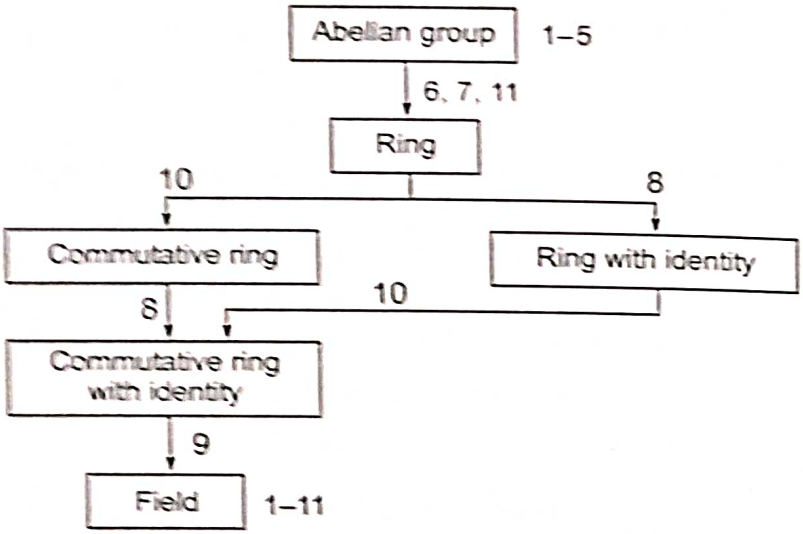

Fig. 2.2 Sets with two binary operations.

2.1.4 RELATIONS

The concept of a relation is a basic concept in computer science as well as in real life. This concept arises when we consider a pair of objects and compare one with the other. For example, 'being the father of' gives a relation between two persons. We can express the relation by ordered pairs (for instance, 'a is the father of b' can be represented by the ordered pair (a, b)).

While executing a program, comparisons are made, and based on the result, different tasks are performed. Thus in computer science the concept of relation arises just as in the case of data structures.

Definition 2.2 A relation R in a set S is a collection of ordered pairs of elements in S (i.e. a subset of $S \times S$). When (x, y) is in R, we write xRy. When (x, y) is not in R, we write $xR'y$.

EXAMPLE 2.1

A relation R in Z can be defined by xRy if $x > y$.

Properties of Relations

(i) A relation R in S is *reflexive* if xRx for every x in S.
(ii) A relation R in S is *symmetric* if for x, y in S, yRx whenever xRy.
(iii) A relation R in S is *transitive* if for x, y and z in S, xRz whenever xRy and yRz.

We note that the relation given in Example 2.1 is neither reflexive nor symmetric, but transitive.

EXAMPLE 2.2

A relation R in $\{1, 2, 3, 4, 5, 6\}$ is given by

$$\{(1, 2), (2, 3), (3, 4), (4, 4), (4, 5)\}$$

This relation is not reflexive as $1R'1$. It is not symmetric as $2R3$ but $3R'2$. It is also not transitive as $1R2$ and $2R3$ but $1R'3$.

EXAMPLE 2.3

Let us define a relation R in $\{1, 2, \ldots, 10\}$ by aRb if a divides b. R is reflexive and transitive but not symmetric ($3R6$ but $6R'3$).

EXAMPLE 2.4

If i, j, n are integers we say that i is congruent to j modulo n (written as $i \equiv j$ modulo n or $i \equiv j \bmod n$) if $i - j$ is divisible by n. The 'congruence modulo n' is a relation which is reflexive and symmetric (if $i - j$ is divisible by n, so is $j - i$). If $i \equiv j \bmod n$ and $j \equiv k \bmod n$, then we have $i - j = an$ for some a and $j - k = bn$ for some b. So,

$$i - k = i - j + j - k = an + bn$$

which means that $i \equiv k \bmod n$. Thus this relation is also transitive.

Definition 2.3 A relation R in a set S is called an equivalence relation if it is reflexive, symmetric and transitive.

Example 2.5 gives an equivalence relation in Z.

EXAMPLE 2.5

We can define an equivalence relation R on any set S by defining aRb if $a = b$. (Obviously, $a = a$ for every a. So, R is reflexive. If $a = b$ then $b = a$. So R is symmetric. Also, if $a = b$ and $b = c$, then $a = c$. So R is transitive.)

EXAMPLE 2.6

Define a relation R on the set of all persons in New Delhi by aRb if the persons a and b have the same date of birth. Then R is an equivalence relation.

Let us study this example more carefully. Corresponding to any day of the year (say, 4th February), we can associate the set of all persons born on that day. In this way the set of all persons in New Delhi can be partitioned into 366 subsets. In each of the 366 subsets, any two elements are related. This leads to one more property of equivalence relations.

Definition 2.4 Let R be an equivalence relation on a set S. Let $a \in S$. Then C_a is defined as

$$\{b \in S \mid aRb\}$$

The C_a is called an equivalence class containing a. In general, the C_a's are called equivalence classes.

EXAMPLE 2.7

For the congruence modulo 3 relation on $\{1, 2, \ldots, 7\}$,

$$C_2 = \{2, 5\}, \qquad C_1 = \{1, 4, 7\}, \qquad C_3 = \{3, 6\}$$

For the equivalence relation 'having the same birth day' (discussed in Example 2.6), the set of persons born on 4th February is an equivalence class, and the number of equivalence classes is 366. Also, we may note that the union of all the 366 equivalence classes is the set of all persons in Delhi. This is true for any equivalence relation because of the following theorem.

Theorem 2.1 Any equivalence relation R on a set S partitions S into disjoint equivalence classes.

Proof Let $\bigcup_{a \in S} C_a$ denote the union of distinct equivalence classes. We have to prove that:

(i) $S = \bigcup_{a \in S} C_a$,

(ii) $C_a \cap C_b = \emptyset$ if C_a and C_b are different, i.e. $C_a \neq C_b$.

Let $s \in S$. Then $s \in C_s$ (since sRs, R being reflexive). But $C_s \subseteq \bigcup_{a \in S} C_a$. So $S \subseteq \bigcup_{a \in S} C_a$. By definition of C_a, $C_a \subseteq S$ for every a in S. So $\bigcup_{a \in S} C_a \subseteq S$. Thus we have proved (i).

Before proving (ii), we may note the following:

$$C_a = C_b \quad \text{if } aRb. \tag{2.1}$$

As aRb, we have bRa because R is symmetric. Let $d \in C_a$. By definition of C_a, we have aRd. As bRa and aRd, by transitivity of R, we get bRd. This means $d \in C_b$. Thus we have proved $C_a \subseteq C_b$. In a similar way we can show that $C_b \subseteq C_a$. Therefore, (2.1) is proved.

Now we prove (ii) by the method of contradiction (refer to Section 2.5). We want to prove that $C_a \cap C_b = \emptyset$ if $C_a \neq C_b$. Suppose $C_a \cap C_b \neq \emptyset$. Then there exists some element d in S such that $d \in C_a$ and $d \in C_b$. As $d \in C_a$, we have aRd. Similarly, we have bRd. By symmetry of R, dRb. As aRd and dRb, by transitivity of R, we have aRb. Now we can use (2.1) to conclude that $C_a = C_b$. But this is a contradiction (as $C_a \neq C_b$). Therefore, $C_a \cap C_b = \emptyset$. Thus (ii) is proved. ∎

If we apply Theorem 2.1 to the equivalence relation congruence modulo 3 on $\{1, 2, 3, 4, 5, 6, 7\}$, we get

$$C_1 = C_4 = C_7 = \{1, 4, 7\}$$
$$C_2 = C_5 = \{2, 5\}$$
$$C_3 = C_6 = \{3, 6\}$$

and therefore,

$$\{1, 2, \ldots, 7\} = C_1 \cup C_2 \cup C_3$$

EXERCISE Let S denote the set of all students in a particular college. Define aRb if a and b study in the same class. What are the equivalence classes? In what way does R partition S?

2.1.5 Closure of Relations

A given relation R may not be reflexive or transitive. By adding more ordered pairs to R we can make it reflexive or transitive. For example, consider a relation $R = \{(1, 2), (2, 3), (1, 1), (2, 2)\}$ in $\{1, 2, 3\}$. R is not reflexive as $3R'3$. But by adding $(3, 3)$ to R, we get a reflexive relation. Also, R is not transitive as $1R2$ and $2R3$ but $1R'3$. By adding the pair $(1, 3)$, we get a relation $T = \{(1, 2), (2, 3), (1, 1), (2, 2), (1, 3)\}$ which is transitive. There are many transitive relations T containing R. But the smallest among them is interesting.

Definition 2.5 Let R be a relation in a set S. Then the transitive closure of R (denoted by R^+) is the smallest transitive relation containing R.

Note: We can define reflexive closure and symmetric closure in a similar way.

Definition 2.6 Let R be a relation in S. Then the reflexive-transitive closure of R (denoted by R^*) is the smallest reflexive and transitive relation containing R.

For constructing R^+ and R^*, we define the composite of two relations. Let R_1 and R_2 be the two relations in S. Then,

(i) $R_1 \circ R_2 = \{(a, c) \in S \times S \mid aR_1b \text{ and } bR_2c \text{ for some } b \in S\}$

(ii) $R_1^2 = R_1 \circ R_1$

(iii) $R_1^n = R_1^{n-1} \circ R_1$ for all $n \geq 2$

Note: For getting the elements of R_1 o R_2, we combine (a, b) in R_1 and (b, c) in R_2 to get (a, c) in R_1 o R_2.

Theorem 2.2 Let S be a finite set and R be a relation in S. Then the transitive closure R^+ of R exists and $R^+ = R \cup R^2 \cup R^3 \ldots$.

EXAMPLE 2.8

Let $R = \{(1, 2), (2, 3), (2, 4)\}$ be a relation in $\{1, 2, 3, 4\}$. Find R^+.

Solution

$$R = \{(1, 2), (2, 3), (2, 4)\}$$

$$R^2 = \{(1, 2), (2, 3), (2, 4)\} \text{ o } \{(1, 2), (2, 3), (2, 4)\}$$

$$= \{(1, 3), (1, 4)\}$$

(We combine (a, b) and (b, c) in R to get (a, c) in R^2.)

$$R^3 = R^2 \text{ o } R = \{(1, 3), (1, 4)\} \text{ o } \{(1, 2), (2, 3), (2, 4)\} = \emptyset$$

(Here no pair (a, b) in R^2 can be combined with any pair in R.)

$$R^4 = R^5 = \cdots = \emptyset$$

$$R^+ = R \cup R^2 = \{(1, 2), (2, 3), (2, 4), (1, 3), (1, 4)\}$$

EXAMPLE 2.9

Let $R = \{(a, b), (b, c), (c, a)\}$. Find R^+.

Solution

$$R = \{(a, b), (b, c), (c, a)\}$$

$$R \text{ o } R = \{(a, b), (b, c), (c, a)\} \text{ o } \{(a, b), (b, c), (c, a)\}$$

$$= \{(a, c), (b, a), (c, b)\}$$

(This is obtained by combining the pairs: (a, b) and (b, c), (b, c) and (c, a), and (c, a) and (a, b).)

$$R^3 = R^2 \text{ o } R = \{(a, c), (b, a), (c, b)\} \text{ o } \{(a, b), (b, c), (c, a)\}$$

$$= \{(a, a), (b, b), (c, c)\}$$

$$R^4 = R^3 \text{ o } R = \{(a, a), (b, b), (c, c)\} \text{ o } \{(a, b), (b, c), (c, a)\}$$

$$= \{(a, b), (b, c), (c, a)\} = R$$

So,

$$R^5 = R^4 \text{ o } R = R \text{ o } R = R^2, \qquad R^6 = R^5 \text{ o } R = R^2 \text{ o } R = R^3$$

$$R^7 = R^6 \text{ o } R = R^3 \text{ o } R = R^4 = R$$

Then any R^n is one of R, R^2 or R^3. Hence,

$$R^+ = R \cup R^2 \cup R^3$$

$$= \{(a, b), (b, c), (c, a), (a, c), (b, a), (c, b), (a, a), (b, b), (c, c)\}$$

Note: $R^* = R^+ \cup \{(a, a) \mid a \in S\}$.

EXAMPLE 2.10

If $R = \{(a, b), (b, c), (c, a)\}$ is a relation in $\{a, b, c\}$, find R^*.

Solution

From Example 2.9,

$$R^* = R^+ \cup \{(a, a), (b, b), (c, c)\}$$
$$= \{(a, b), (b, c), (c, a), (a, c), (b, a), (c, b), (a, a), (b, b), (c, c)\}$$

EXAMPLE 2.11

What is the symmetric closure of relation R in a set S?

Solution

Symmetric closure of $R = R \cup \{(b, a) \mid aRb\}$.

2.1.6 FUNCTIONS

The concept of a function arises when we want to associate a unique value (or result) with a given argument (or input).

Definition 2.7 A function or map f from a set X to a set Y is a rule which associates to every element x in X a unique element in Y, which is denoted by $f(x)$. The element $f(x)$ is called the image of x under f. The function is denoted by $f: X \to Y$.

Functions can be defined either (i) by giving the images of all elements of X, or (ii) by a computational rule which computes $f(x)$ once x is given.

EXAMPLES (a) f: $\{1, 2, 3, 4\} \to \{a, b, c\}$ can be defined by $f(1) = a$, $f(2) = c$, $f(3) = a$, $f(4) = b$.

(b) f: $R \to R$ can be defined by $f(x) = x^2 + 2x + 1$ for every x in R. (R denotes the set of all real numbers.)

Definition 2.8 $f : X \to Y$ is said to be one-to-one (or injective) if different elements in X have different images, i.e. $f(x_1) \neq f(x_2)$ when $x_1 \neq x_2$.

Note: To prove that f is one-to-one, we prove the following: Assume $f(x_1) = f(x_2)$ and show that $x_1 = x_2$.

Definition 2.9 $f : X \to Y$ is onto (surjective) if every element y in Y is the image of some element x in X.

Definition 2.10 $f : X \to Y$ is said to be a one-to-one correspondence or bijection if f is both one-to-one and onto.

EXAMPLE 2.12

$f : Z \to Z$ given by $f(n) = 2n$ is one-to-one but not onto.

Solution

Suppose $f(n_1) = f(n_2)$. Then $2n_1 = 2n_2$. So $n_1 = n_2$. Hence f is one-to-one. It is not onto since no odd integer can be the image of any element in Z (as any image is even).

The following theorem distinguishes a finite set from an infinite set.

Theorem 2.3 Let S be a finite set. Then $f : S \to S$ is one-to-one iff it is onto.

Note: The above result is not true for infinite sets as Example 2.12 gives a one-to-one function $f : Z \to Z$ which is not onto.

EXAMPLE 2.13

Show that $f : R \to R - \{1\}$ given by $f(x) = (x + 1)/(x - 1)$ is onto.

Solution

Let $y \in R$. Suppose $y = f(x) = (x + 1)/(x - 1)$. Then $y(x - 1) = x + 1$, i.e. $yx - x = 1 + y$. So, $x = (1 + y)/(y - 1)$. As $(1 + y)/(y - 1) \in R$ for all $y \neq 1$, y is the image of $(1 + y)/(y - 1)$ in $R - \{1\}$. Thus, f is onto.

The Pigeonhole Principle†

Suppose a postman distributes 51 letters in 50 mailboxes (pigeonholes). Then it is evident that some mailbox will contain at least two letters. This is enunciated as a mathematical principle called the pigeonhole principle.

If n objects are distributed over m places and $n > m$, then some place receives at least two objects.

EXAMPLE 2.14

If we select 11 natural numbers between 1 to 380, show that there exist at least two among these 11 numbers whose difference is at most 38.

Solution

Arrange the numbers 1, 2, 3, . . ., 380 in 10 boxes, the first box containing 1, 2, 3, . . ., 38, the second containing 39, 40, . . ., 76, etc. There are 11 numbers to be selected. Take these numbers from the boxes. By the pigeonhole principle, at least one box will contain two of these eleven numbers. These two numbers differ by 38 or less.

† The pigeonhole principle is also called the Dirichlet drawer principle, named after the French mathematician G. Lejeune Dirichlet (1805–1859).

2.2 GRAPHS AND TREES

The theory of graphs is widely applied in many areas of computer science—formal languages, compiler writing, artificial intelligence (AI), to mention only a few. Also, the problems in computer science can be phrased as problems in graphs. Our interest lies mainly in trees (special types of graphs) and their properties.

2.2.1 GRAPHS

Definition 2.11 A graph (or undirected graph) consists of (i) a nonempty set V called the set of vertices, (ii) a set E called the set of edges, and (iii) a map Φ which assigns to every edge a unique unordered pair of vertices.

Representation of a Graph

Usually a graph, namely the undirected graph, is represented by a diagram where the vertices are represented by points or small circles, and the edges by arcs joining the vertices of the associated pair (given by the map Φ).

Figure 2.3, for example, gives an undirected graph. Thus, the unordered pair $\{v_1, v_2\}$ is associated with the edge e_1; the pair (v_2, v_2) is associated with e_6. (e_6 is a self-loop. In general, an edge is called a self-loop if the vertices in its associated pair coincide.)

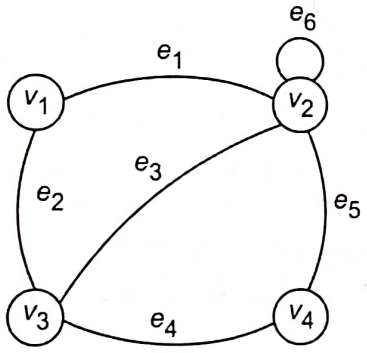

Fig. 2.3 An undirected graph.

Definition 2.12 A directed graph (or digraph) consists of (i) a nonempty set V called the set of vertices, (ii) a set E called the set of edges, and (iii) a map Φ which assigns to every edge a unique ordered pair of vertices.

Representation of a Digraph

The representation is as in the case of undirected graphs except that the edges are represented by directed arcs.

Figure 2.4, for example, gives a directed graph. The ordered pairs (v_2, v_3), (v_3, v_4), (v_1, v_3) are associated with the edges e_3, e_4, e_2, respectively.

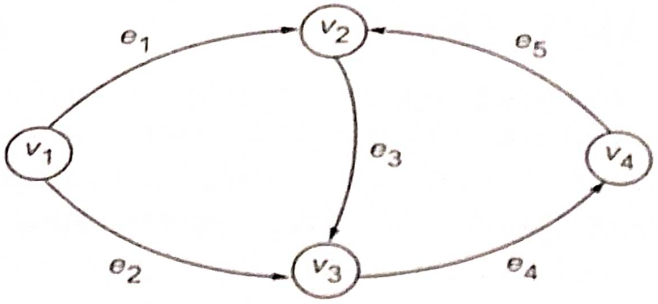

Fig. 2.4 A directed graph.

Definitions (i) If (v_i, v_j) is associated with an edge e, then v_i and v_j are called the end vertices of e; v_i is called a predecessor of v_j which is a successor of v_i.

In Fig. 2.3, v_2 and v_3 are the end vertices of e_3. In Fig. 2.4, v_2 is a predecessor of v_3 which is a successor of v_2. Also, v_4 is a predecessor of v_2 and successor of v_3.

(ii) If G is a digraph, the undirected graph corresponding to G is the undirected graph obtained by considering the edges and vertices of G, but ignoring the 'direction' of the edges. For example, the undirected graph corresponding to the digraph given in Fig. 2.4 is shown in Fig. 2.5.

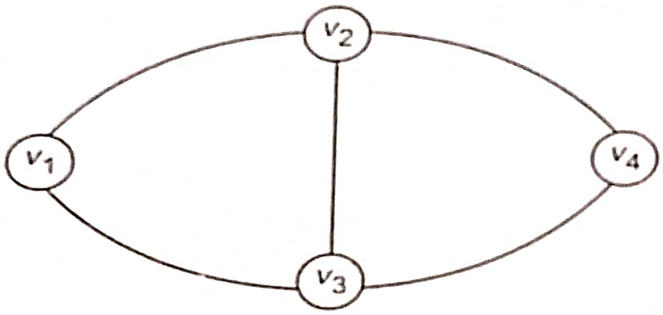

Fig. 2.5 A graph.

Definition 2.13 The degree of a vertex in a graph (directed or undirected) is the number of edges with v as an end vertex. (A self-loop is counted twice while calculating the degree.) In Fig. 2.3, $\deg(v_1) = 2$, $\deg(v_3) = 3$, $\deg(v_2) = 5$. In Fig. 2.4, $\deg(v_2) = 3$, $\deg(v_4) = 2$

We now mention the following theorem without proof.

Theorem 2.4 The number of vertices of odd degree in any graph (directed or undirected) is even.

Definition 2.14 A path in a graph (undirected or directed) is an alternating sequence of vertices and edges of the form $v_1e_1v_2e_2 \ldots v_{n-1}e_{n-1}v_n$ beginning and ending with vertices such that e_i has v_i and v_{i+1} as its end vertices and no edge or vertex is repeated in the sequence. The path is said to be a path from v_1 to v_n.

For example, $v_1e_2v_3e_3v_2$ is a path in Fig. 2.3. It is a path from v_1 to v_2. In Fig. 2.4, $v_1e_2v_3e_3v_2$ is a path from v_1 to v_2. $v_1e_1v_2$ is also a path from v_1 to v_2.

And $v_3e_4v_4e_5v_2$ is a path from v_3 to v_2. We call $v_3e_4v_4e_5v_2$ a directed path since the edges e_4 and e_5 have the forward direction. (But $v_1e_2v_3e_3v_2$ is not a directed path as e_2 is in the forward direction and e_3 is in the backward direction.)

Definition 2.15 A graph (directed or undirected) is connected if there is a path between every pair of vertices.

The graphs given by Figs. 2.3 and 2.4, for example, are connected.

Definition 2.16 A circuit in a graph is an alternating sequence $v_1e_1v_2e_2 \ldots e_{n-1}v_1$ of vertices and edges starting and ending in the same vertex such that e_i has v_i and v_{i+1} as the end vertices and no edge or vertex other than v_1 is repeated.

In Fig. 2.3, for example, $v_3e_3v_2e_5v_4e_4v_3$, $v_1e_2v_3e_4v_4e_5v_2e_1v_1$ are circuits. In Fig. 2.4, $v_1e_2v_3e_3v_2e_1v_1$ and $v_2e_3v_3e_4v_4e_5v_2$ are circuits.

2.2.2 TREES

Definition 2.17 A graph (directed or undirected) is called a tree if it is connected and has no circuits.

The graphs given in Figs. 2.6 and 2.7, for example, are trees. The graphs given in Figs. 2.3 and 2.4 are not trees.

Note: A directed graph G is a tree iff the corresponding undirected graph is a tree.

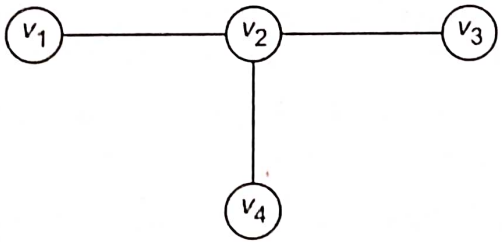

Fig. 2.6 A tree with four vertices.

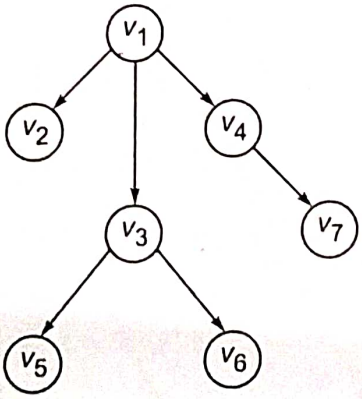

Fig. 2.7 A tree with seven vertices.

We now discuss some properties of trees (both directed and undirected) used in developing transition systems and studying grammar rules.

Property 1 A tree is a connected graph with no circuits or loops.

Property 2 In a tree there is one and only one path between every pair of vertices.

Property 3 If in a graph there is a unique (i.e. one and only one) path between every pair of vertices, then the graph is a tree.

Property 4 A tree with n vertices has $n - 1$ edges.

Property 5 If a connected graph with n vertices has $n - 1$ edges, then it is a tree.

Property 6 If a graph with no circuits has n vertices and $n - 1$ edges, then it is a tree.

A leaf in a tree can be defined as a vertex of degree one. The vertices other than leaves are called internal vertices.

In Fig. 2.6, for example, v_1, v_3, v_4 are leaves and v_2 is an internal vertex. In Fig. 2.7, v_2, v_5, v_6, v_7 are leaves and v_1, v_3, v_4 are internal vertices.

The following definition of ordered trees will be used for representing derivations in context-free grammars.

Definition 2.18 An ordered directed tree is a digraph satisfying the following conditions:

T_1: There is one vertex called the root of the tree which is distinguished from all the other vertices and the root has no predecessors.

T_2: There is a directed path from the root to every other vertex.

T_3: Every vertex except the root has exactly one predecessor.

T_4: The successors of each vertex are ordered 'from the left'.

Note: The condition T_4 of the definition becomes evident once we have the diagram of the graph.

Figure 2.7 is an ordered tree with v_1 as the root. Figure 2.8 also gives an ordered directed tree with v_1 as the root. In this figure the successors of v_1 are ordered as v_2v_3. The successors of v_3 are ordered as v_5v_6.

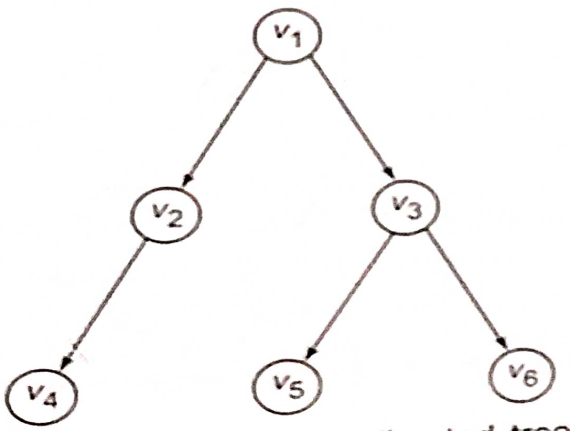

Fig. 2.8 An ordered directed tree.

By adopting the following convention, we can simplify Fig. 2.8. The root is at the top. The directed edges are represented by arrows pointing downwards. As all the arrows point downwards, the directed edges can be simply represented by lines sloping downwards, as illustrated in Fig. 2.9.

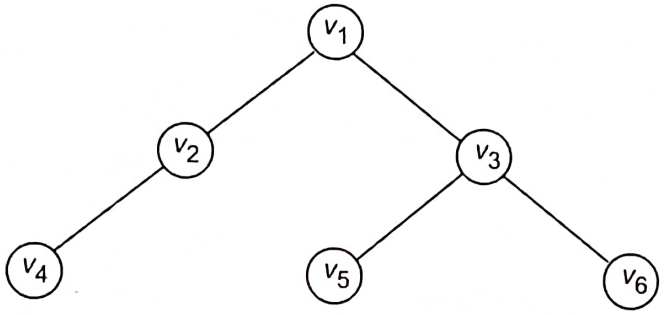

Fig. 2.9 Representation of an ordered directed tree.

Note: An ordered directed tree is connected (which follows from T_2). It has no circuits (because of T_3). Hence an ordered directed tree is a tree (see Definition 2.17).

As we use only the ordered directed trees in applications to grammars, we refer to ordered directed trees as simply trees.

Definition 2.19 A binary tree is a tree in which the degree of the root is 2 and the remaining vertices are of degree 1 or 3.

Note: In a binary tree any vertex has at most two successors. For example, the trees given by Figs. 2.11 and 2.12 are binary trees. The tree given by Fig. 2.9 is not a binary tree.

Theorem 2.5 The number of vertices in a binary tree is odd.

Proof Let n be the number of vertices. The root is of degree 2 and the remaining $n-1$ vertices are of odd degree (by Definition 2.19). By Theorem 2.4, $n-1$ is even and hence n is odd. ∎

We now introduce some more terminology regarding trees:

(i) A son of a vertex v is a successor of v.
(ii) The father of v is the predecessor of v.
(iii) If there is a directed path from v_1 to v_2, v_1 is called an ancestor of v_2, and v_2 is called a descendant of v_1. (*Convention:* v_1 is an ancestor of itself and also a descendant of itself.)
(iv) The number of edges in a path is called the length of the path.
(v) The height of a tree is the length of a longest path from the root. For example, for the tree given by Fig. 2.9, the height is 2. (Actually there are three longest paths, $v_1 \to v_2 \to v_4$, $v_1 \to v_3 \to v_5$, $v_1 \to v_2 \to v_6$. Each is of length 2.)
(vi) A vertex v in a tree is at level k if there is a path of length k from the root to the vertex v (the maximum possible level in a tree is the height of the tree).

Figure 2.10, for example, gives a tree where the levels of vertices are indicated.

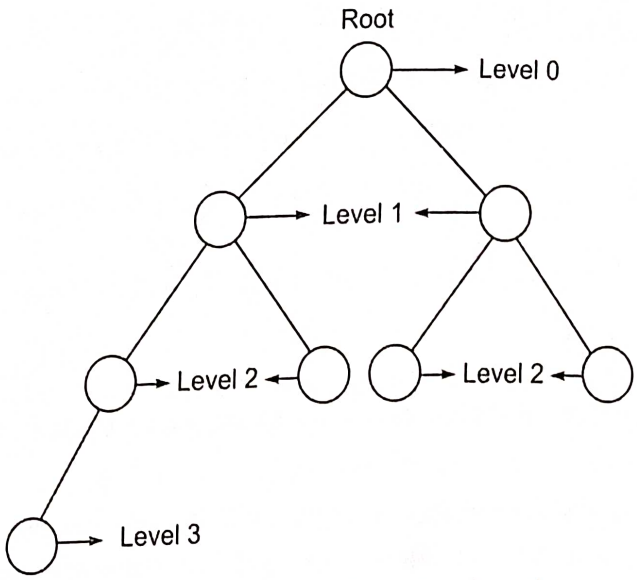

Fig. 2.10 Illustration of levels of vertices.

EXAMPLE 2.15

For a binary tree T with n vertices, show that the minimum possible height is $\lceil \log_2(n + 1) - 1 \rceil$, where $\lceil k \rceil$ is the smallest integer $\geq k$, and the maximum possible height is $(n - 1)/2$.

Solution

In a binary tree the root is at level 0. As every vertex can have at most two successors, we have at most two vertices at level 1, at most 4 vertices at level 2, etc. So the maximum number of vertices in a binary tree of height k is $1 + 2 + 2^2 + \cdots + 2^k$. As T has n vertices, $1 + 2 + 2^2 + \cdots + 2^k \geq n$, i.e. $(2^{k+1} - 1)/(2 - 1) \geq n$, so $k \geq \log_2(n + 1) - 1$. As k is an integer, the smallest possible value for k is $\lceil \log_2(n + 1) - 1 \rceil$. Thus the minimum possible height is $\lceil \log_2(n + 1) - 1 \rceil$.

To get the maximum possible height, we proceed in a similar way. In a binary tree we have the root at zero level and at least two vertices at level 1, 2, ... When T is of height k, we have at least $1 + 2 + \cdots + 2$ (2 repeated k times) vertices. So, $1 + 2k \leq n$, i.e. $k \leq (n - 1)/2$. But, n is odd by Theorem 2.4. So $(n - 1)/2$ is an integer. Hence the maximum possible value for k is $(n - 1)/2$.

EXAMPLE 2.16

When $n = 9$, the trees with minimum and maximum height are shown in Figs. 2.11 and 2.12 respectively. The height of the tree in Fig. 2.11 is $\lceil \log_2(9 + 1) - 1 \rceil = 3$. For the tree in Fig. 2.12, the height $= (9 - 1)/2 = 4$.

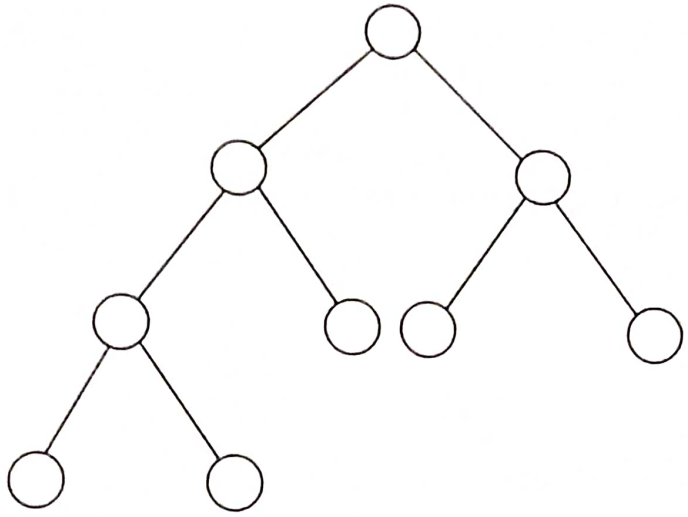

Fig. 2.11 Binary tree of minimum height with 9 vertices.

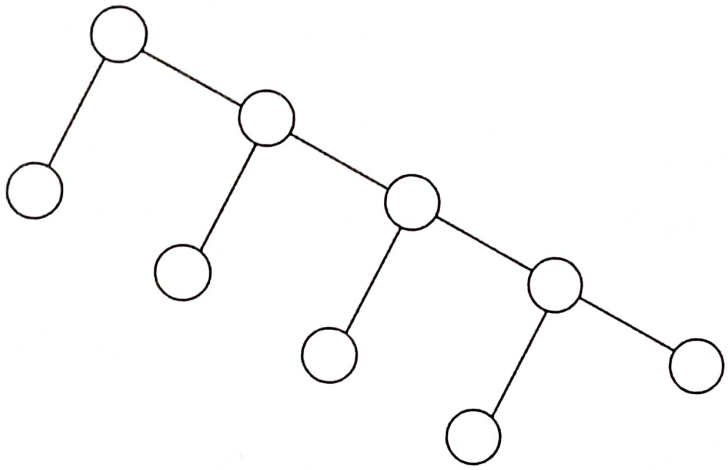

Fig. 2.12 Binary tree of maximum height with 9 vertices.

EXAMPLE 2.17

Prove that the number of leaves in a binary tree T is $(n + 1)/2$, where n is the number of vertices.

Solution

Let m be the number of leaves in a tree with n vertices. The root is of degree 2 and the remaining $n - m - 1$ vertices are of degree 3. As T has n vertices, it has $n - 1$ edges (by Property 4). As each edge is counted twice while calculating the degrees of its end vertices, $2(n - 1)$ = the sum of degrees of all vertices = $2 + m + 3(n - m - 1)$. Solving for m, we get $m = (n + 1)/2$.

EXAMPLE 2.18

For the tree shown in Fig. 2.13, answer the following questions:

(a) Which vertices are leaves and which internal vertices?

(b) Which vertices are the sons of 5?
(c) Which vertex is the father of 5?
(d) What is the length of the path from 1 to 9?
(e) What is the left-right order of leaves?
(f) What is the height of the tree?

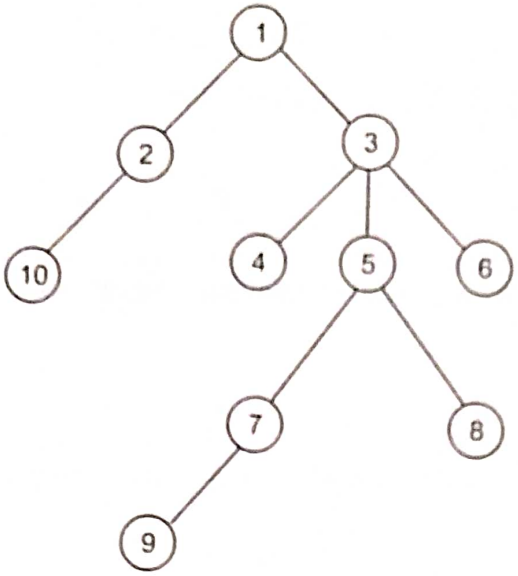

Fig. 2.13 The directed tree for Example 2.18.

Solutions

(a) 10, 4, 9, 8, 6 are leaves. 1, 2, 3, 5, 7 are internal vertices.
(b) 7 and 8 are the sons of 5.
(c) 3 is the father of 5.
(d) Four (the path is $1 \rightarrow 3 \rightarrow 5 \rightarrow 7 \rightarrow 9$).
(e) 10 – 4 – 9 – 8 – 6.
(f) Four ($1 \rightarrow 3 \rightarrow 5 \rightarrow 7 \rightarrow 9$ is the longest path).

2.3 STRINGS AND THEIR PROPERTIES

A string over an alphabet set Σ is a finite sequence of symbols from Σ.

NOTATION: Σ^* denotes the set of all strings (including Λ, the empty string) over the alphabet set Σ. That is, $\Sigma^+ = \Sigma^* - \{\Lambda\}$.

2.3.1 OPERATIONS ON STRINGS

The basic operation for strings is the binary concatenation operation. We define this operation as follows: Let x and y be two strings in Σ^*. Let us form a new string z by placing y after x, i.e. $z = xy$. The string z is said to be obtained by concatenation of x and y.

EXAMPLE 2.19

Find xy and yx, where

(a) $x = 010$, $y = 1$
(b) $x = a\Lambda$, $y = \text{ALGOL}$

Solution

(a) $xy = 0101$, $yx = 1010$.
(b) $xy = a\Lambda$ ALGOL
$yx =$ ALGOL $a\Lambda$.

We give below some basic properties of concatenation.

Property 1 Concatenation on a set Σ^* is associative since for each x, y, z in Σ^*, $x(yz) = (xy)z$.

Property 2 *Identity element.* The set Σ^* has an identity element Λ w.r.t. the binary operation of concatenation as

$$x\Lambda = \Lambda x = x \qquad \text{for every } x \text{ in } \Sigma^*$$

Property 3 Σ^* has left and right cancellations. For x, y, z in Σ^*,

$zx = zy$ implies $x = y$ (left cancellation)

$xz = yz$ implies $x = y$ (right cancellation)

Property 4 For x, y in Σ^*, we have

$$|xy| = |x| + |y|$$

where $|x|$, $|y|$, $|xy|$ denote the lengths of the strings x, y, xy, respectively.

We introduce below some more operations on strings.

Transpose Operation

We extend the concatenation operation to define the transpose operation as follows:

For any x in Σ^* and a in Σ,

$$(xa)^T = a(x)^T$$

For example, $(aaabab)^T$ is *babaaa*.

Palindrome. A palindrome is a string which is the same whether written forward or backward, e.g. Malayalam. A palindrome of even length can be obtained by concatenation of a string and its transpose.

Prefix and suffix of a string. A prefix of a string is a substring of leading symbols of that string. For example, w is a prefix of y if there exists y' in Σ^* such that $y = wy'$. Then we write $w < y$. For example, the string 123 has four prefixes, i.e. Λ, 1, 12, 123.

Similarly, a suffix of a string is a substring of trailing symbols of that string, i.e. w is a suffix of y if there exists $y' \in \Sigma^*$ such that $y = y'w$. For example, the string 123 has four suffixes, i.e. Λ, 3, 23, 123.

Theorem 2.6 (Levi's theorem) Let v, w, x and $y \in \Sigma^*$ and $vw = xy$. Then:

(i) there exists a unique string z in Σ^* such that $v = xz$ and $y = zw$ if $|v| > |x|$;

(ii) $v = x$, $y = w$, i.e. $z = \Lambda$ if $|v| = |x|$;

(iii) there exists a unique string z in Σ^* such that $x = vz$, and $w = zy$ if $|v| < |x|$.

Proof We shall give a very simple proof by representing the strings by a diagram (see Fig. 2.14). ∎

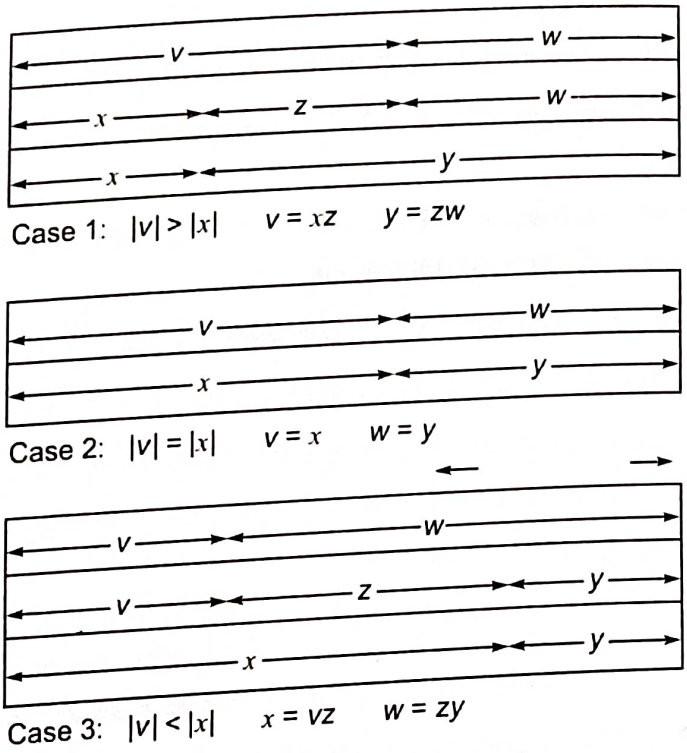

Fig. 2.14 Illustration of Levi's theorem.

2.3.2 TERMINAL AND NONTERMINAL SYMBOLS

The definitions in this section will be used in subsequent chapters.

A terminal symbol is a unique indivisible object used in the generation of strings.

A nonterminal symbol is a unique object but divisible, used in the generation of strings. A nonterminal symbol will be constructed from the terminal symbols; the number of terminal symbols in a nonterminal symbol may vary; it is also called a variable. In a natural language, e.g. English, the letters a, b, A, B, etc. are terminals and the words boy, cat, dog, go are nonterminal symbols. In programming languages, A, B, C, . . ., Z, :, =, begin, and, if, then, etc. are terminal symbols.

The following will be a variable in Pascal:

< For statement > → for < control variable > : =
< for list > do < statement >

2.4 PRINCIPLE OF INDUCTION

The process of reasoning from general observations to specific truths is called *induction*.

The following properties apply to the set N of natural numbers and the principle of induction.

Property 1 Zero is a natural number.

Property 2 The successor of any natural number is also a natural number.

Property 3 Zero is not the successor of any natural number.

Property 4 No two natural numbers have the same successor.

Property 5 Let a property $P(n)$ be defined for every natural number n. If (i) $P(0)$ is true, and (ii) P(successor of n) is true whenever $P(n)$ is true, then $P(n)$ is true for all n.

A proof by complete enumeration of all possible combinations is called *perfect induction*, e.g. *proof by truth table.*

The method of proof by induction can be used to prove a property $P(n)$ for all n.

2.4.1 METHOD OF PROOF BY INDUCTION

This method consists of three basic steps:

Step 1 Prove $P(n)$ for $n = 0/1$. This is called the *proof for the basis.*

Step 2 Assume the result/properties for $P(n)$. This is called the *induction hypothesis.*

Step 3 Prove $P(n + 1)$ using the induction hypothesis.

EXAMPLE 2.20

Prove that $1 + 3 + 5 + \cdots + r = n^2$, for all $n > 0$, where r is an odd integer and n is the number of terms in the sum. (*Note:* $r = 2n - 1$.)

Solution

(a) *Proof for the basis.* For n = I, L.H.S. = 1 and R.H.S. = $1^2 = 1$. Hence the result is true for $n = 1$.

(b) By induction hypothesis, we have $1 + 3 + 5 + \cdots + r = n^2$. As $r = 2n - 1$,

$$\text{L.H.S.} = 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(c) We have to prove that $1 + 3 + 5 + \cdots + r + r + 2 = (n + 1)^2$:

$$\text{L.H.S.} = (1 + 3 + 5 + \cdots + r + (r + 2))$$

$$= n^2 + r + 2 = n^2 + 2n - 1 + 2 = (n + 1)^2 = \text{R.H.S.}$$

EXAMPLE 2.21

Prove the following theorem by induction:

$$1 + 2 + 3 + \cdots + n = n(n + 1)/2$$

Solution

(a) *Proof for the basis.* For $n = 1$, L.H.S. $= 1$ and R.H.S. $= 1(1 + 1)/2 = 1$

(b) Assume $1 + 2 + 3 + \cdots + n = n(n + 1)/2$.

(c) We have to prove:

$$1 + 2 + 3 + \cdots + (n + 1) = (n + 1)(n + 2)/2$$

$$1 + 2 + 3 + \cdots + n + (n + 1)$$

$= n(n + 1)/2 + (n + 1)$ (by induction hypothesis)

$= (n + 1)(n + 2)/2$ (on simplification)

The proof by induction can be modified as explained in the following section.

2.4.2 Modified Method of Induction

Three steps are involved in the modified proof by induction.

Step 1 Proof for the basis ($n = 0/1$).

Step 2 Assume the result/properties for all positive integers $< n + 1$.

Step 3 Prove the result/properties using the induction hypothesis (i.e. step 2), for $n + 1$.

Example 2.22 below illustrates the modified method of induction. The method we shall apply will be clear once we mention the induction hypothesis.

EXAMPLE 2.22

Prove the following theorem by induction: A tree with n vertices has $(n - 1)$ edges.

Solution

For $n = 1, 2$, the following trees can be drawn (see Fig. 2.15). So the theorem is true for $n = 1, 2$. Thus, there is basis for induction.

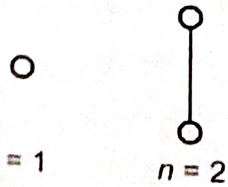

Fig. 2.15 Trees with one or two vertices.

Consider a tree T with $(n + 1)$ vertices as shown in Fig. 2.16. Let e be an edge connecting the vertices v_i and v_j. There is a unique path between v_i and v_j through the edge e. (Property of a tree: There is a unique path between every pair of vertices in a tree.) Thus, the deletion of e from the graph will divide the graph into two subtrees. Let n_1 and n_2 be the number of vertices in the subtrees. As $n_1 \leq n$ and $n_2 \leq n$, by induction hypothesis, the total number of edges in the subtrees is $n_1 - 1 + n_2 - 1$, i.e. $n - 2$. So, the number of edges in T is $n - 2 + 1 = n - 1$ (by including the deleted edge e). By induction, the result is true for all trees.

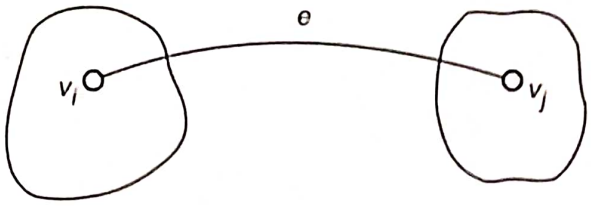

Fig. 2.16 Tree T with $(n + 1)$ vertices.

EXAMPLE 2.23

Two definitions of palindromes are given below. Prove by induction that the two definitions are equivalent.

Definition 1 A palindrome is a string that reads the same forward and backward.

Definition 2 (i) Λ is a palindrome.
(ii) If a is any symbol, the string a is a palindrome.
(iii) If a is any symbol and x is a palindrome, then axa is a palindrome.
(iv) Nothing is a palindrome unless it follows from (i)–(iii).

Solution

Let x be a string which satisfies the Definition 1, i.e. x reads the same forward and backward. By induction on the length of x we prove that x satisfies the Definition 2.

If $|x| \leq 1$, then $x = a$ or Λ. Since x is a palindrome by Definition 1, Λ and a are also palindromes (hence (i) and (ii)), i.e. there is basis for induction. If $|x| > 1$, then $x = awa$, where w, by Definition 1, is a palindrome; hence the rule (iii). Thus, if x satisfies the Definition 1, then it satisfies the Definition 2.

Let x be a string which is constructed using the Definition 2. We show by induction on $|x|$ that it satisfies the Definition 1. There is basis for induction by rule (ii). Assume the result for all strings with length $< n$. Let x be a string of length n. As x has to be constructed using the rule (iii), $x = aya$, where y is a palindrome. As y is a palindrome by Definition 2 and $|y| < n$, it satisfies the Definition 1. So, $x = aya$ also satisfies the Definition 1.

EXAMPLE 2.24

Prove the pigeonhole principle.

Proof We prove the theorem by induction on m. If $m = 1$ and $n > 1$, then all these n items must be placed in a single place. Hence the theorem is true for $m = 1$.

Assume the theorem for m. Consider the case of $m + 1$ places. We prove the theorem for $n = m + 2$. (If $n > m + 2$, already one of the $m + 1$ places will receive at least two objects from $m + 2$ objects, by what we are going to prove.) Consider a particular place, say, P.

Three cases arise:

(i) P contains at least two objects.
(ii) P contains one object
(iii) P contains no object.

In case (i), the theorem is proved for $n = m + 2$. Consider case (ii). As P contains one object, the remaining m places should receive $m + 1$ objects. By induction hypothesis, at least one place (not the same as P) contains at least two objects. In case (iii), $m + 2$ objects are distributed among m places. Once again, by induction hypothesis, one place (other than P) receives at least two objects. Hence, in all the cases, the theorem is true for $(m + 1)$ places. By the principle of induction, the theorem is true for all m.

2.4.3 SIMULTANEOUS INDUCTION

Sometimes we may have a pair of related identities. To prove these, we may apply two induction proofs simultaneously. Example 2.25 illustrates this method.

EXAMPLE 2.25

A sequence $F_0, F_1, F_2, \ldots$ called the sequence of Fibonacci numbers (named after the Italian mathematician Leonardo Fibonacci) is defined recursively as follows:

$$F_{n+1} = F_n + F_{n-1}, \qquad F_0 = 0, \qquad F_1 = 1$$

Prove that:

$$P_n : F_n^2 + F_{n-1}^2 = F_{2n-1} \tag{2.2}$$

$$Q_n : F_{n+1}F_n + F_nF_{n-1} = F_{2n} \tag{2.3}$$

Proof We prove the two identities (2.2) and (2.3) simultaneously by simultaneous induction. P_1 and Q_1 are $F_1^2 + F_0^2 = F_1$ and $F_2F_1 + F_1F_0 = F_2$

respectively. As $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, these are true. Hence there is basis for induction. Assume P_n and Q_n. So

$$F_n^2 + F_{n-1}^2 = F_{2n-1} \tag{2.2}$$

$$F_{n+1}F_n + F_nF_{n-1} = F_{2n} \tag{2.3}$$

Now,

$$\begin{aligned} F_{n+1}^2 + F_n^2 &= (F_{n-1} + F_n)^2 + F_n^2 \\ &= F_{n-1}^2 + F_n^2 + 2F_{n-1}F_n + F_n^2 \\ &= (F_{n-1}^2 + F_n^2) + F_{n-1}F_n + F_n^2 + F_{n-1}F_n \\ &= F_{n-1}^2 + F_n^2 + (F_{n-1} + F_n)F_n + F_nF_{n-1} \\ &= (F_{n-1}^2 + F_n^2) + F_{n+1}F_n + F_nF_{n-1} \\ &= F_{2n-1} + F_{2n} \qquad \text{(by (2.3))} \\ &= F_{2n+1} \end{aligned}$$

This proves P_{n+1}.

Also,

$$\begin{aligned} F_{n+2}F_{n+1} + F_{n+1}F_n &= (F_{n+1} + F_n)F_{n+1} + (F_n + F_{n-1})F_n \\ &= F_{n+1}^2 + F_{n+1}F_n + F_nF_{n-1} + F_n^2 \\ &= (F_{n+1}^2 + F_n^2) + (F_{n+1}F_n + F_nF_{n-1}) \\ &= F_{2n+1} + F_{2n} \qquad \text{(By } P_{n+1} \text{ and (2.3))} \\ &= F_{2n+2} \end{aligned}$$

This proves Q_{n+1}.

So, by induction (2.2) and (2.3) are true for all n.

We conclude this chapter with the method of proof by contradiction.

2.5 PROOF BY CONTRADICTION

Suppose we want to prove a property P under certain conditions. The method of proof by contradiction is as follows:

Assume that property P is not true. By logical reasoning get a conclusion which is either absurd or contradicts the given conditions.

The following example illustrates the use of proof by contradiction and proof by induction.

EXAMPLE 2.26

Prove that there is no string x in $\{a, b\}^*$ such that $ax = xb$. (For the definition of strings, refer to Section 2.3.)

Proof We prove the result by induction on the length of x. When $|x| = 1$, $x = a$ or $x = b$. In both cases $ax \neq xb$. So there is basis for induction. Assume the result for any string whose length is less than n. Let x be any string of length n. We prove that $ax \neq xb$ through proof by contradiction. Suppose $ax = xb$. As a is the first symbol on the L.H.S., the first symbol of x is a. As b is the last symbol on R.H.S., the last symbol of x is b. So, we can write x as ayb with $|y| = n - 2$. This means $aayb = aybb$ which implies $ay = yb$. This contradicts the induction hypothesis. Thus, $ax \neq xb$. By induction the result is true for all strings.

2.6 SUPPLEMENTARY EXAMPLES

EXAMPLE 2.27

In a survey of 600 people, it was found that:

250 read the *Week*
260 read the *Reader's Digest*
260 read the *Frontline*
90 read both *Week* and *Frontline*
110 read both *Week* and *Reader's Digest*
80 read both *Reader's Digest* and *Frontline*
30 read all the three magazines.

(a) Find the number of people who read at least one of the three magazines.
(b) Find the number of people who read none of these magazines.
(c) Find the number of people who read exactly one magazine.

Solution

Let W, R, F denote the set of people who read *Week*, *Reader's Digest* and *Frontline*, respectively. We use the Venn diagram to represent these sets (see Fig. 2.17).

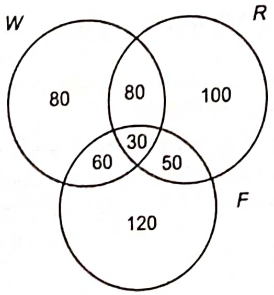

Fig. 2.17 Venn diagram for Example 2.27.

It is given that:

$|W| = 250, \quad |R| = 260, \quad |F| = 260, \quad |W \cap F| = 90,$
$|W \cap R| = 110, \quad |R \cap F| = 80, \quad |W \cap R \cap F| = 30$

$\therefore |W \cup R \cup F|$
$= |W| + |R| + |F| - |W \cap F| - |W \cap R| - |R \cap F| + |W \cap R \cap F|$
$= 250 + 260 + 260 - 90 - 110 - 80 + 30 = 520$

So the solution for (a) is 520.

(b) The number of people who read none of the magazines
$= 600 - 520 = 80$

Using the data, we fill up the various regions of the Venn diagram.

(c) The number of people who read only one magazine
$= 80 + 100 + 120 = 300$

EXAMPLE 2.28

Prove that $(A \cup B \cup C)' = (A \cup B)' \cap (A \cup C)'$

Solution

$(A \cup B \cup C) = (A \cup A) \cup B \cup C$
$= A \cup (A \cup B) \cup C = (A \cup B) \cup (A \cup C)$

Hence $(A \cup B \cup C)' = (A \cup B)' \cap (A \cup C)'$ (by DeMorgan's law)

EXAMPLE 2.29

Define aRb if $b = a^k$ for some positive integer k; $a, b \in z$. Show that R is a partial ordering. (A relation is a partial ordering if it is reflexive, antisymmetric and transitive.)

Solution

As $a = a^1$, we have aRa. To prove that R is antisymmetric, we have to prove that aRb and $bRa \Rightarrow a = b$. As aRb, we have $b = a^k$. As bRa, we have $a = b^l$. Hence $a = b^l = (a^k)^l = a^{kl}$. This is possible only when one of the following holds good:

(i) $a = 1$
(ii) $a = -1$
(iii) $kl = 1$

In case (i), $b = a^k = 1$. So $a = b$.

In case (ii), $a = -1$ and so kl is odd. This implies that both k and l are odd. So

$$b = a^k = (-1)^k = -1 = a$$

In case (iii), $kl = 1$. As k and l are positive integers, $k = l = 1$. So

$$b = a^k = a.$$

If aRb and bRc, then $b = a^k$ and $c = b^l$ for some k, l. Therefore, $c = a^{kl}$. Hence aRc.

EXAMPLE 2.30

Suppose $A = \{1, 2, \ldots, 9\}$ and $\sim$ relation on $A \times A$ is defined by $(m, n) \sim (p, q)$ if $m + q = n + p$, then prove that $\sim$ is an equivalence relation.

Solution

$(m, n) \sim (m, n)$ since $m + n = n + m$. So $\sim$ is reflexive. If $(m, n) \sim (p, q)$, then $m + q = n + p$; thus $p + n = q + m$. Hence $(p, q) \sim (m, n)$. So $\sim$ is symmetric.

If $(m, n) \sim (p, q)$ and $(p, q) \sim (r, s)$, then

$$m + q = n + p \qquad \text{and} \qquad p + s = q + r$$

Adding these,

$$m + q + p + s = n + p + q + r$$

That is,

$$m + s = n + r$$

which proves $(m, n) \sim (r, s)$.
Hence $\sim$ is an equivalence relation.

EXAMPLE 2.31

If $f : A \to B$ and $g : B \to C$ are one-to-one, prove that $g \circ f$ is one-to-one.

Solution

Let us assume that $g \circ f(a_1) = g \circ f(a_2)$. Then, $g(f(a_1)) = g(f(a_2))$. As g is one-to-one, $f(a_1) = f(a_2)$. As f is one-to-one, $a_1 = a_2$. Hence $g \circ f$ is one-to-one.

EXAMPLE 2.32

Show that a connected graph G with n vertices and $n - 1$ edges ($n \geq 3$) has at least one leaf.

Solution

G has n vertices and $n - 1$ edges. Every edge is counted twice while computing the degree of each of its end vertices. Hence

$$\Sigma \deg(v) = 2(n - 1)$$

where summation is taken over all vertices of G.

So, $\Sigma \deg(v)$ is the sum of n positive integers. If $\deg(v) \geq 2$ for every vertex v of G, then

$$2n \leq \Sigma \deg(v) = 2(n - 1)$$

which is not possible.

Hence $\deg(v) = 1$ for at least one vertex v of G and this vertex v is a leaf.

EXAMPLE 2.33

Prove Property 5 stated in Section 2.2.2.

Solution

We prove the result by induction on n. Obviously, there is basis for induction. Assume the result for connected graphs with $n - 1$ vertices. Let T be a connected graph with n vertices and $n - 1$ edges. By Example 2.32, T has at least one leaf v (say).

Drop the vertex v and the (single) edge incident with v. The resulting graph G' is still connected and has $n - 1$ vertices and $n - 2$ edges. By induction hypothesis, G' is a tree. So G' has no circuits and hence G also has no circuits. (Addition of the edge incident with v does not create a circuit in G.) Hence G is a tree. By the principle of induction, the property is true for all n.

EXAMPLE 2.34

A person climbs a staircase by climbing either (i) two steps in a single stride or (ii) only one step in a single stride. Find a formula for $S(n)$, where $S(n)$ denotes the number of ways of climbing n stairs.

Solution

When there is a single stair, there is only one way of climbing up. Hence $S(1) = 1$. For climbing two stairs, there are two ways, viz. two steps in a single stride or two single steps. So $S(2) = 2$. In reaching n steps, the person can climb either one step or two steps in his last stride. For these two choices, the number of ways are $S(n - 1)$ and $S(n - 2)$.

So,

$$S(n) = S(n - 1) + S(n - 2)$$

Thus, $S(n) = F(n)$, the nth Fibonacci number (refer to Exercise 2.20, at the end of this chapter).

EXAMPLE 2.35

How many subsets does the set $\{1, 2, \ldots, n\}$ have that contain no two consecutive integers?

Solution

Let S_n denote the number of subsets of $\{1, 2, \ldots, n\}$ having the desired property. If $n = 1$, $S_1 = |\{\emptyset, \{1\}\}| = 2$. If $n = 2$, then $S_2 = |\{\emptyset, \{1\}, \{2\}|| = 3$.

Consider a set A with n elements. If a subset having the desired property contains n, it cannot contain $n - 1$. So there are S_{n-2} such subsets. If it does not contain n, there are S_{n-1} such subsets. So $S_n = S_{n-1} + S_{n-2}$. As $S_1 = 2 = F_3$ and $S_2 = 3 = F_4$,

$$S_n = F_{n+2}$$

the $(n + 2)$th Fibonacci number.

EXAMPLE 2.36

If $n \geq 1$, show that

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1$$

Solution

We prove the result by induction on n. If $n = 1$, then $1 \cdot 1! = 1 = (1 + 1)! - 1$. So there is basis for induction.

Assume the result for n, i.e.

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1$$

Then,

$$\begin{aligned} &1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! + (n + 1) \cdot (n + 1)! \\ &= (n + 1)! - 1 + (n + 1) \cdot (n + 1)! \\ &= (n + 1)! \, (1 + n + 1) - 1 = (n + 2)! - 1 \end{aligned}$$

Hence the result is true for $n + 1$ and by the principle of induction, the result is true for all $n \geq 1$.

EXAMPLE 2.37

Using induction, prove that $2^n < n!$ for all $n \geq 4$.

Solution

For $n = 4$, $2^4 < 4!$. So there is basis for induction. Assume $2^n < n!$. Then,

$$2^{n+1} = 2^n \cdot 2 < n! \cdot 2 < (n + 1)n! = (n + 1)!$$

By induction, the result is true for all $n \geq 4$.

SELF-TEST

Choose the correct answer to Questions 1–10:

1. $(A \cup A) \cap (B \cap B)$ is
(a) A (b) $A \cap B$ (c) B (d) none of these

2. The reflexive–transitive closure of the relation $\{(1, 2), (2, 3)\}$ is
(a) $\{(1, 2), (2, 3), (1, 3)\}$
(b) $\{(1, 2), (2, 3), (1, 3), (3, 1)\}$
(c) $\{(1, 1), (2, 2), (3, 3), (1, 3), (1, 2), (2, 3)\}$
(d) $\{(1, 1), (2, 2), (3, 3), (1, 3)\}$

3. There exists a function

$$f : \{1, 2, \ldots, 10\} \to \{2, 3, 4, 5, 6, 7, 9, 10, 11, 12\}$$

which is
(a) one-to-one and onto
(b) one-to-one but not onto
(c) onto but not one-to-one
(d) none of these

4. A tree with 10 vertices has
(a) 10 edges (b) 9 edges (c) 8 edges (d) 7 edges.

5. The number of binary trees with 7 vertices is
(a) 7 (b) 6 (c) 2 (d) 1

6. Let $N = \{1, 2, 3, \ldots\}$. Then $f : N \to N$ defined by $f(n) = n + 1$
(a) onto but not one-to-one
(b) one-to-one but not onto
(c) both one-to-one and onto
(d) neither one-to-one nor onto

7. QST is a substring of
(a) $PQRST$
(b) $QRSTU$
(c) $QSPQSTUT$
(d) $QQSSTT$

8. If $x = 01$, $y = 101$ and $z = 011$, then $xyzy$ is
(a) 01011011
(b) 01101101011
(c) 01011101101
(d) 01101011101

9. A binary tree with seven vertices has
(a) one leaf
(b) two leaves
(c) three leaves
(d) four leaves

10. A binary operation o on $N = \{1, 2, 3, \ldots\}$ is defined by $a \circ b = a + 2b$. Then:
(a) o is commutative
(b) o is associative
(c) N has an identity element with respect to o
(d) none of these

EXERCISES

2.1 If $A = \{a, b\}$ and $B = \{b, c\}$, find:
(a) $(A \cup B)^*$
(b) $(A \cap B)^*$
(c) $A^* \cup B^*$

(d) $A^* \cap B^*$
(e) $(A - B)^*$
(f) $(B - A)^*$

2.2 Let $S = \{a, b\}^*$. For $x, y \in S$, define $x \circ y = xy$, i.e. $x \circ y$ is obtained by concatenating x and y.
(a) Is S closed under $\circ$?
(b) Is $\circ$ associative?
(c) Does S have the identity element with respect to $\circ$?
(d) Is $\circ$ commutative?

2.3 Let $S = 2^X$, where X is any nonempty set. For $A, B \subseteq X$, let $A \circ B = A \cup B$.
(a) Is $\circ$ commutative and associative?
(b) Does S have the identity element with respect to $\circ$?
(c) If $A \circ B = A \circ C$, does it imply that $B = C$?

2.4 Test whether the following statements are true or false. Justify your answer.
(a) The set of all odd integers is a monoid under multiplication.
(b) The set of all complex numbers is a group under multiplication.
(c) The set of all integers under the operation $\circ$ given by $a \circ b = a + b - ab$ is a monoid.
(d) 2^S under symmetric difference $\bar{\vee}$ defined by $A \bar{\vee} B = (A - B) \cup (B - A)$ is an abelian group.

2.5 Show that the following relations are equivalence relations:
(a) On a set S, aRb if $a = b$.
(b) On the set of all lines in the plane, $l_1 R l_2$ if l_1 is parallel to l_2.
(c) On $N = \{0, 1, 2, \ldots\}$, mRn if m differs from n by a multiple of 3.

2.6 Show that the following are not equivalence relations:
(a) On a set S, aRb if $a \neq b$.
(b) On the set of lines in the plane, $l_1 R l_2$ if l_1 is perpendicular to l_2.
(c) On $N = \{0, 1, 2, \ldots\}$, mRn if m divides n.
(d) On $S = \{1, 2, \ldots, 10\}$, aRb if $a + b = 10$.

2.7 For x, y in $\{a, b\}^*$, define a relation R by xRy if $|x| = |y|$. Show that R is an equivalence relation. What are the equivalence classes?

2.8 For x, y in $\{a, b\}^*$, define a relation R by xRy if x is a substring of y (x is a substring of y if $y = z_1 x z_2$ for some string z_1, z_2). Is R an equivalence relation?

2.9 Let $R = \{(1, 2), (2, 3), (1, 4), (4, 2), (3, 4)\}$. Find R^+, R^*.

2.10 Find R^* for the following relations:
(a) $R = \{(1, 1), (1, 2), (2, 1), (2, 3), (3, 2)\}$
(b) $R = \{(1, 1), (2, 3), (3, 4), (3, 2)\}$

(c) $R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$
(d) $R = \{(1, 2), (2, 3), (3, 1), (4, 4)\}$

2.11 If R is an equivalence relation on S, what can you say about R^+, R^*?

2.12 Let $f : \{a, b\}^* \to \{a, b\}^*$ be given by $f(x) = ax$ for every $x \in \{a, b\}^*$. Show that f is one-to-one but not onto.

2.13 Let $g : \{a, b\}^* \to \{a, b\}^*$ be given by $g(x) = x^T$. Show that g is one-to-one and onto.

2.14 Give an example of (a) a tree with six vertices and (b) a binary tree with seven vertices.

2.15 For the tree T given in Fig. 2.18, answer the following questions:
(a) Is T a binary tree?
(b) Which vertices are the leaves of T?
(c) How many internal vertices are in T?
(d) What is the height of T?
(e) What is the left-to-right ordering of leaves?
(f) Which vertex is the father of 5?
(g) Which vertices are the sons of 3?

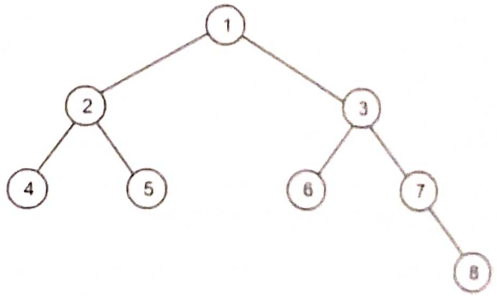

Fig. 2.18 The tree for Exercise 2.15

2.16 In a get-together, show that the number of persons who know an odd number of persons is even.
[*Hint:* Use a graph.]

2.17 If X is a finite set, show that $|2^X| = 2^{|X|}$.

2.18 Prove the following by the principle of induction:

(a) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

(b) $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{(n+1)}$

(c) $10^{2n} - 1$ is divisible by 11 for all $n > 1$.

2.19 Prove the following by the principle of induction:

(a) $1 + 4 + 7 + \cdots + (3n - 2) = \dfrac{n(3n - 1)}{2}$

(b) $2^n > n$ for all $n > 1$

(c) If $f(2) = 2$ and $f(2^k) = 2f(2^{k-1}) + 3$, then $f(2^k) = (5/2) \cdot 2^k - 3$.

2.20 The Fibonacci numbers are defined in the following way:

$$F(0) = 1, \qquad F(1) = 1, \qquad F(n + 1) = F(n) + F(n - 1)$$

Prove by induction that:

(a) $F(2n + 1) = \sum_{k=0}^{n} F(2k)$

(b) $F(2n + 2) = \sum_{k=1}^{n} F(2k + 1) + 1$

2.21 Show that the maximum number of edges in a simple graph (i.e. a graph having no self-loops or parallel edges) is $\dfrac{n(n - 1)}{2}$.

2.22 If $w \in \{a, b\}^*$ satisfies the relation $abw = wab$, show that $|w|$ is even.

2.23 Suppose there are an infinite number of envelopes arranged one after another and each envelope contains the instruction 'open the next envelope'. If a person opens an envelope, he has to then follow the instruction contained therein. Show that if a person opens the first envelope, he has to open all the envelopes.