Department of Mathematics, Government Arts College (Autonomous), Coimbatore-18

Year	Subject Title	Sem.	Sub Code
2018 -19 Onwards	DISCRETE MATHEMATICS FOR COMPUTER SCIENCE	II	18BCS24A

OBJECTIVES:

1. To understand the concepts of basic Discrete structures.
2. To get knowledge about applying the properties of Discrete Mathematical Structures.

UNIT: III

BASIC SET THEORY: Basic definitions – Venn diagrams and set operations – Laws of set theory – Principle of inclusion and exclusion – Relations – Properties of relations – Matrices of relations – Functions – Injective, surjective and bijective functions.

(Chapter II - Sections: 2.1, 2.3 and 2.4)

2-1 BASIC CONCEPTS OF SET THEORY

In this section first we introduce the notation used for specifying sets. The concepts of membership and inclusion are given. Certain special sets such as the universal set, empty set, and the power set of a given set are introduced. Next, various set operations are defined. Finally, some of the basic identities of set algebra are derived.

2-1.1 Notation

Rather than defining the term "set," here we give only an intuitive idea of what a set is. By a *set* we mean a collection of objects of any sort. The word "object" is used here in a very broad sense to include even abstract objects. The following examples will illustrate the concept of a set.

The *set* of all Canadians

A *pair* of shoes

A *bouquet* of flowers

The *set* of all ideas contained in a book

A *flock* of sheep

A *collection* of rocks

Note that we encounter many words which convey the same idea as that of a set. Some of these words, however, are used in a more restricted sense than the term "set," while the others are synonyms. We shall use the words "class," "aggregate," and "collection" as synonyms of the word "set," particularly to avoid using the same word repeatedly in a given sentence. For example, a set of sets may be called a collection of sets.

Generally speaking, we think of a set as a collection of objects which share some common property. For example, in mathematics it is common to consider a set of lines, a set of triangles, a set of real numbers, etc. However, this restriction is not necessary, and a set consisting of a horse, the letter A, a jacket, and Mr. Smith is an acceptable example of a set, although it may be uninteresting and not important.

A fundamental concept of set theory is that of membership or belonging to a set. Any object belonging to a set is called a *member* or an *element* of that set. A set is said to be *well defined* if it is possible to determine, by means of certain rules, whether any given object is a member of the set.

Capital letters, with or without subscripts, will be used throughout to denote sets, and lowercase letters will be used to denote the elements. Some exceptions to these rules will be made in order to conform to standard practice.

If an element p belongs to a set A, then we write

$$p \in A$$

which is read as "p is an element of the set A" or "p belongs to the set A," or "p is in A." If there exists an object q which does not belong to the set A, then we express this fact as

$$q \notin A$$

which is equivalent to the negation of the statement "q is in A," that is,

$$\neg(q \in A) \Leftrightarrow q \notin A$$

There are several ways in which a set can be specified. For example, a set consisting of the elements 1, 3, and a is generally written as

$$\{1, 3, a\}$$

The names of the elements are enclosed in braces and separated by commas. If we wish to denote this set as S, then we write

$$S = \{1, 3, a\}$$

where the equality sign is understood to mean that S is the set $\{1, 3, a\}$. Obviously,

$$1 \in S \qquad 3 \in S \qquad a \in S \qquad \text{and} \qquad 2 \notin S$$

This method of specifying a set is not convenient, and it is not always possible to use it. In general, a set can be defined or characterized by a predicate. Examples of such sets are

$$S_1 = \{x \mid x \text{ is an odd positive integer}\}$$
$$S_2 = \{x \mid x \text{ is a province of Canada}\}$$
$$S_3 = \{x \mid x \text{ is a river}\}$$
$$S_4 = \{x \mid x = a \text{ or } x = b\}$$

If we let $P(x)$ denote any predicate, then $\{x \mid P(x)\}$ defines a set. An element b belongs to this set if $P(b)$ is true; otherwise b does not belong to the set. This statement would be written symbolically as

$$(y)\,(P(y) \Leftrightarrow y \in \{x \mid P(x)\})$$

If we denote the set $\{x \mid P(x)\}$ by A, then $A = \{x \mid P(x)\}$ and

$$(y)\,(y \in A \Leftrightarrow y \in \{x \mid x \in A\})$$

Other sets which are specified by listing the elements can also be characterized by means of predicates. For example, the set $\{1, 3, a\}$ could be defined as

$$\{x \mid (x = 1) \lor (x = 3) \lor (x = a)\}$$

Although it is possible to characterize any set by a predicate, it is sometimes convenient to specify sets by yet another method, such as

$$S_5 = \{1, 3, 5, \ldots\}$$
$$S_6 = \{2, 4, 6, \ldots, 18\}$$
$$S_7 = \{a, a^2, a^3, \ldots\}$$

In this representation the missing elements can be determined from the elements present and from the context.

The number of distinct elements present in a set may be finite or infinite. We shall call a set *finite* if it contains a finite number of distinguishable elements; otherwise, a set is *infinite*. Precise definitions of a finite and an infinite set are given in Sec. 2-5.2.

Note that no restriction has been placed on the objects that can be members of a set. It is not unusual to have sets whose members are themselves sets, such as

$$S = \{a, \{1, 2\}, p, \{q\}\}$$

However, it is important to distinguish between the set $\{q\}$, which is an element of S, and the element q, which is a member of $\{q\}$ but not a member of S.

2-1.2 Inclusion and Equality of Sets

In Sec. 2-1.1, we discussed the notion of membership of an element in a set. Another basic concept in set theory is that of inclusion.

Definition 2-1.1 Let A and B be any two sets. If every element of A is an element of B, then A is called a *subset* of B, or A is said to be *included* in B, or B *includes* A. Symbolically, this relation is denoted by $A \subseteq B$, or equivalently by $B \supseteq A$. Alternatively,

$$A \subseteq B \Leftrightarrow (x)\,(x \in A \rightarrow x \in B) \Leftrightarrow B \supseteq A$$

It is important at this stage to distinguish between membership and inclusion. We illustrate the difference between these two. Let

$$A = \{1, 2, 3\} \qquad B = \{1, 2\} \qquad C = \{1, 3\} \qquad \text{and} \qquad D = \{3\}$$

then

$$B \subseteq A \qquad C \subseteq A \qquad \text{and} \qquad D \subseteq A$$

or

$$\{1, 2\} \subseteq \{1, 2, 3\} \qquad \{1, 3\} \subseteq \{1, 2, 3\} \qquad \{3\} \subseteq \{1, 2, 3\}$$

On the other hand, $1 \in \{1, 2, 3\}$, and 1 is not included in $\{1, 2, 3\}$, though $\{1\} \subseteq \{1, 2, 3\}$. Only a set can be included in or can be a subset of another set, while only elements can be members of a set. Of course, a set may sometimes have other sets as elements. For example, if $A = \{\{1\}, 2, 3\}$, then

$$\{1\} \in A \qquad \{\{1\}, 2\} \subseteq A \qquad \{\{1\}\} \subseteq A \qquad 2 \in A \qquad \{2, 3\} \subseteq A$$

The following are some of the important properties of set inclusion. For any sets A, B, and C

$$A \subseteq A \qquad \text{(reflexive)} \tag{1}$$

$$(A \subseteq B) \wedge (B \subseteq C) \Rightarrow (A \subseteq C) \qquad \text{(transitive)} \tag{2}$$

It is enough to note at this stage that set inclusion is reflexive and transitive. These terms are explained in Sec. 2-3.2. The proof of Statement (1) is obvious, while Statement (2) can be proved by using the implication

$$(x)(x \in A \to x \in B) \wedge (x)(x \in B \to x \in C) \Rightarrow (x)(x \in A \to x \in C)$$

(see Example 2, Sec. 1-6.4). For two sets A and B, note that $A \subseteq B$ does not necessarily imply $B \subseteq A$ except for the following case.

Definition 2-1.2 Two sets A and B are said to be *equal* (extensionally equal) iff $A \subseteq B$ and $B \subseteq A$, or symbolically,

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$$

From the equivalence

$$(x)((P(x) \to Q(x)) \wedge (Q(x) \to P(x))) \Leftrightarrow (x)(P(x) \rightleftarrows Q(x))$$

we can alternatively define the equality of two sets as

$$A = B \Leftrightarrow (x)(x \in A \rightleftarrows x \in B)$$

We now give some examples of sets that are equal and sets that are not equal.

$\{1, 2, 4\} = \{1, 2, 2, 4\}$.

$\{1, 4, 2\} = \{1, 2, 4\}$.

If $P = \{\{1, 2\}, 4\}$ and $Q = \{1, 2, 4\}$, then $P \neq Q$.

$\{\{1\}\} \neq \{1\}$ because $\{1\} \in \{\{1\}\}$ while $1 \in \{1\}$.

If $A = \{x \mid x(x - 1) = 0\}$ and $B = \{0, 1\}$, then $A = B$.

$\{1, 3, 5, \ldots\} = \{x \mid x \text{ is an odd positive integer}\}$.

From the definition of equality of sets it is clear that

$$A = B \Leftrightarrow B = A$$

The equality of sets is reflexive, symmetric, and transitive.

Definition 2-1.3 A set A is called a *proper subset* of a set B if $A \subseteq B$ and $A \neq B$. Symbolically it is written as $A \subset B$, so that

$$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$$

$A \subset B$ is also called a proper inclusion.

A proper inclusion is not reflexive; however, it is transitive, i.e.,

$$(A \subset B) \wedge (B \subset C) \Rightarrow (A \subset C)$$

We shall now introduce two special sets, of which one includes every set under discussion while the other is included in every set under discussion.

Definition 2-1.4 A set is called a *universal set* if it includes every set under discussion. A universal set will be denoted by E.

It follows from the definition that for any set A, we have $A \subseteq E$. Thus every element $x \in E$, that is, $(x)(x \in E)$ is identically true. One could specify E in a variety of ways, e.g.,

$$E = \{x \mid P(x) \lor \neg P(x)\}$$

where $P(x)$ is any predicate. It is easy to show that all such sets are equal to the set E. The introduction of the universal set makes the notion of $b \notin A$ more definite in the sense that b is assumed to be in E. The universal set is the same as the universe of discourse given in Sec. 1-5.5.

Definition 2-1.5 A set which does not contain any element is called an *empty set* or a *null set*. An empty set will be denoted by $\varnothing$.

It follows from the definition that for an empty set $\varnothing$ and any x, $x \in \varnothing$ is a contradiction, that is, $(x)(x \in \varnothing)$ is a contradiction. Thus for any set A, $\varnothing \subseteq A$, because $(x)(x \in \varnothing \Rightarrow x \in A)$. One could specify $\varnothing$ in a variety of ways, e.g.,

$$\varnothing = \{x \mid P(x) \land \neg P(x)\}$$

where $P(x)$ is any predicate. It is easy to show that all such sets are identical to the set $\varnothing$.

2-1.3 The Power Set

Given any set A, we know that the null set $\varnothing$ and the set A are both subsets of A. Also for any element $a \in A$, the set $\{a\}$ is a subset of A. Similarly, we can consider other subsets of A. Rather than finding individual subsets of A, we would like to say something about the set of all subsets of A.

Definition 2-1.6 For a set A, a collection or family of all subsets of A is called the *power set* of A. The power set of A is denoted by $\rho(A)$ or 2^A, so that

$$\rho(A) = 2^A = \{x \mid x \subseteq A\}$$

Let us consider some finite sets and their power sets. The power set of the null set $\varnothing$ has only the element $\varnothing$; hence $\rho(\varnothing) = \{\varnothing\}$. For a set $S_1 = \{a\}$, the power set $\rho(S_1) = \{\varnothing, \{a\}\} = \{\varnothing, S_1\}$. For $S_2 = \{a, b\}$, $\rho(S_2) = \{\varnothing, \{a\}, \{b\}, S_2\}$, and for $S_3 = \{a, b, c\}$, $\rho(S_3) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, S_3\}$.

We now introduce a notation by which one can designate every subset of a finite set in a unique manner. Before we describe this notation, it would be useful to assume that the elements of the given set are ordered in some way, so that a particular element may be called the first element, the next element the second, and so on. No such ordering of the elements of a set is implied in the definition of a set. However, for the purpose of representing a set on a computer it is generally necessary to prescribe some arbitrary order; i.e., to each element is attached a label which describes the position of the element with respect to other elements of the set. As an example, let us assume that in the set S_2 given earlier we let a be the first element and b be the second element. Now, in any subset of a given set, some elements of the set are present while the remaining ones are absent. We shall use this idea, together with the ordering prescribed on the elements of a given set, to designate the subsets. For example, the subsets of S_2 may be designated as

$$\varnothing = B_{00} \qquad \{a\} = B_{10} \qquad \{b\} = B_{01} \qquad \text{and} \qquad \{a, b\} = B_{11}$$

where the subscripts of B contain 1 or 0 in the first position on the left depending on whether the first element, viz., a, is present (or not). Similarly, the subscript has 1 or 0 in the second position from the left depending on whether b, the second member, is present (or not). As there are only two elements in S_2, we need only the subscripts 00, 01, 10, and 11. Conversely, given any one of these $2^2 = 4$ subscripts, we can determine the elements of the corresponding subset. For example, $B_{01} = \{b\}$. Note that it is only the subscript that determines the elements of the subset. The use of the letter B in naming the subsets is incidental. A similar technique has been used earlier in assigning names to maxterms and minterms. This method will also be used in the representation of data on a computer.

Consider the set $J = \{00, 01, 10, 11\}$ or $J = \{i \mid i \text{ is a binary integer}, 00 \leq i \leq 11\}$; then $\rho(S_2) = \{B_i \mid i \in J\}$. Similarly,

$$\rho(S_3) = \{B_i \mid i \in J\}$$

where $J = \{i \mid i \text{ is a binary integer}, 000 \leq i \leq 111\}$. From $S_3 = \{a, b, c\}$ we have $B_{001} = \{c\}$, $B_{101} = \{a, c\}$, and $B_{011} = \{b, c\}$.

The above notation can be generalized to designate the subsets of a set having n distinct elements. Obviously, there are 2^n such subsets. The subscripts designating the subsets range over the binary representations of the decimal integers 0 to $2^n - 1$. Care must be taken to insert as many zeros on the left of this binary integer as necessary in order to have exactly n digits in all. One can use decimal integers from 0 to $2^n - 1$ and convert them only at the time when the elements of the corresponding subsets are to be determined. As an illustration, let $S_6 = \{a_1, a_2, \ldots, a_6\}$. Obviously, there are 2^6 subsets of S_6, which we shall designate by $B_0, B_1, \ldots B_{2^6-1}$. The following examples illustrate the method to determine the elements of any subset.

$$B_7 = B_{111} = B_{000111} = \{a_4, a_5, a_6\}$$

$$B_{12} = B_{1100} = B_{001100} = \{a_3, a_4\}$$

The method of employing subscripts to designate the elements of a family of sets is used very often. Here we have used it to designate the members of a power set. It is convenient to introduce the concept of an indexed set at this stage.

Definition 2-1.7 Let $J = \{s_1, s_2, s_3, \ldots\}$ and A be a family of sets $A = \{A_{s_1}, A_{s_2}, A_{s_3}, \ldots\}$ such that for any $s_i \in J$ there corresponds a set $A_{s_i} \in A$, and also $A_{s_i} = A_{s_j}$ iff $s_i = s_j$, then A is called an *indexed set*, J the *index set*, and any subscript such as s_i in A_{s_i} is called an *index*.

An indexed family of sets can also be written as

$$A = \{A_i\}_{i \in J}$$

In particular, if $J = \mathbf{I} = \{1, 2, 3, \ldots\}$, then $A = \{A_1, A_2, A_3, \ldots\}$. Also, if $J = \mathbf{I}_n = \{1, 2, \ldots, n\}$, then $A = \{A_1, A_2, \ldots, A_n\} = \{A_i\}_{i \in I_n}$. For a set S containing n elements, the power set $\rho(S)$ is written as the indexed set

$$\rho(S) = \{B_i\}_{i \in J} \qquad J = \{0, 1, 2, \ldots, 2^n - 1\}$$

EXERCISES 2-1.3

1 Give another description of the following sets and indicate those which are infinite sets.
(*a*) $\{x \mid x$ is an integer and $5 \le x \le 12\}$.
(*b*) $\{2, 4, 8, \ldots\}$.
(*c*) All the countries of the world.

2 Given $S = \{2, a, \{3\}, 4\}$ and $R = \{\{a\}, 3, 4, 1\}$, indicate whether the following are true or false.
(*a*) $\{a\} \in S$
(*b*) $\{a\} \in R$
(*c*) $\{a, 4, \{3\}\} \subseteq S$
(*d*) $\{\{a\}, 1, 3, 4\} \subset R$
(*e*) $R = S$
(*f*) $\{a\} \subseteq S$
(*g*) $\{a\} \subseteq R$
(*h*) $\varnothing \subset R$
(*i*) $\varnothing \subseteq \{\{a\}\} \subseteq R \subseteq E$
(*j*) $\{\varnothing\} \subseteq S$
(*k*) $\varnothing \in R$
(*l*) $\varnothing \subseteq \{\{3\}, 4\}$

3 Show that

$$(R \subseteq S) \land (S \subset Q) \Rightarrow R \subset Q$$

Is it correct to replace $R \subset Q$ by $R \subseteq Q$? Explain your answer.

4 Give the power sets of the following.
(*a*) $\{a, \{b\}\}$
(*b*) $\{1, \varnothing\}$
(*c*) $\{X, Y, Z\}$

5 Given $S = \{a_1, a_2, \ldots, a_8\}$, what subsets are represented by B_{17} and B_{31}? Also, how will you designate the subsets $\{a_2, a_6, a_7\}$ and $\{a_1, a_8\}$?

2-1.4 Some Operations on Sets

In this section we introduce certain basic operations on sets. Using these operations, one can construct new sets by combining the elements of given sets. While the term "operation" and its properties are discussed in Sec. 2-4.4, it suffices to say here that operations on one or more sets produce other sets according to certain rules.

Definition 2-1.8 The *intersection* of any two sets A and B, written as $A \cap B$, is the set consisting of all the elements which belong to both A and B. Symbolically,

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$$

From the definition of intersection it follows that for any sets A and B,

$$A \cap B = B \cap A \qquad A \cap A = A \qquad \text{and } A \cap \varnothing = \varnothing \tag{1}$$

The first of these equalities shows that the intersection is commutative. The importance of the other two will be discussed later. The commutativity of intersection can be proved in the following manner. For any x,

$$\begin{aligned} x \in A \cap B &\Leftrightarrow x \in \{x \mid (x \in A) \wedge (x \in B)\} \\ &\Leftrightarrow (x \in A) \wedge (x \in B) \\ &\Leftrightarrow (x \in B) \wedge (x \in A) \\ &\Leftrightarrow x \in \{x \mid (x \in B) \wedge (x \in A)\} \\ &\Leftrightarrow x \in B \cap A \end{aligned}$$

The other two equalities in Eq. (1) can be proved in a similar manner.

Since $A \cap B$ is a set, we can consider its intersection with another set C, so that

$$(A \cap B) \cap C = \{x \mid x \in A \cap B \wedge x \in C\}$$

Using $(x \in A \wedge x \in B) \wedge x \in C \Leftrightarrow x \in A \wedge (x \in B \wedge x \in C)$, we can easily show that

$$(A \cap B) \cap C = A \cap (B \cap C) \qquad \text{(associative)} \tag{2}$$

In view of Eq. (2), we can write $(A \cap B) \cap C$ as $A \cap B \cap C$.

For an indexed set $A = \{A_1, A_2, \ldots, A_n\} = \{A_i\}_{i \in I_n}$ where $\mathbf{I}_n = \{1, 2, \ldots, n\}$, we write

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \bigcap_{i \in I_n} A_i$$

In general, for any index set J,

$$\bigcap_{i \in J} A_i = \{x \mid x \in A_i \text{ for all } i \in J\}$$

Definition 2-1.9 Two sets A and B are called *disjoint* iff $A \cap B = \varnothing$, that is, A and B have no element in common.

Definition 2-1.10 A collection of sets is called a *disjoint collection* if, for every pair of sets in the collection, the two sets are disjoint. The elements of a disjoint collection are said to be *mutually disjoint*.

Let A be an indexed set $A = \{A_i\}_{i \in J}$. The set A is a disjoint collection iff $A_i \cap A_j = \varnothing$ for all $i, j \in J$, $i \neq j$.

EXAMPLE 1 If $A_1 = \{\{1, 2\}, \{3\}\}$, $A_2 = \{\{1\}, \{2, 3\}\}$, and $A_3 = \{\{1, 2, 3\}\}$, then show that A_1, A_2, and A_3 are mutually disjoint.

SOLUTION Note that $A_1 \cap A_2 = \varnothing$, $A_1 \cap A_3 = \varnothing$ and $A_2 \cap A_3 = \varnothing$. ////

EXAMPLE 2 Show that $A \subseteq B \Leftrightarrow A \cap B = A$.

SOLUTION Note that for any x,

$$x \in A \rightarrow x \in B \Leftrightarrow (x \in A \wedge x \in B) \rightleftarrows x \in A$$

which follows from $P \rightarrow Q \Leftrightarrow ((P \wedge Q) \rightleftarrows P)$. Now

$$A \subseteq B \Leftrightarrow (x)(x \in A \rightarrow x \in B)$$

while

$$A \cap B = A \Leftrightarrow (x)(x \in A \wedge x \in B \rightleftarrows x \in A) \qquad ////$$

Definition 2-1.11 For any two sets A and B, the *union* of A and B, written as $A \cup B$, is the set of all elements which are members of the set A or the set B or both. Symbolically, it is written as

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

From the definition, it follows that

$$A \cup B = B \cup A \quad \text{(commutative)} \qquad A \cup \varnothing = A \qquad A \cup A = A$$
$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{(associative)} \tag{3}$$

The last equality in Eq. (3) suggests that we can write $(A \cup B) \cup C$ as $A \cup B \cup C$. Note that

$$A \cup B \cup C = \{x \mid x \in A \vee x \in B \vee x \in C\}$$

We shall now prove one of the equalities in Eq. (3), viz., $A \cup A = A$. The proofs of the other equalities are similar. For any x,

$$\begin{aligned} x \in A \cup A &\Leftrightarrow x \in \{x \mid x \in A \vee x \in A\} \\ &\Leftrightarrow x \in A \vee x \in A \\ &\Leftrightarrow x \in A \\ &\Leftrightarrow x \in \{x \mid x \in A\} \\ &\Leftrightarrow x \in A \end{aligned}$$

For any indexed set $A = \{A_i\}_{i \in J}$,

$$\bigcup_{i \in J} A_i = \{x \mid x \in A_i \text{ for at least one } i \in J\}$$

For $J = \mathbf{I}_n = \{1, 2, \ldots, n\}$, we may write

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

EXAMPLE 3 What are $S \cup Q$ and $S \cap Q$ if $S = \{a, b, p, q\}$ and $Q = \{a, p, t\}$?

SOLUTION

$$S \cup Q = \{a, b, p, q, t\} \qquad S \cap Q = \{a, p\} \qquad ////$$

EXAMPLE 4 If $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, and $A_3 = \{1, 2, 3, 6\}$, what are $\bigcup_{i=1}^{3} A_i$ and $\bigcap_{i=1}^{3} A_i$?

SOLUTION

$$\bigcup_{i=1}^{3} A_i = \{1, 2, 3, 6\} \qquad \bigcap_{i=1}^{3} A_i = \{2\} \qquad ////$$

Definition 2-1.12 Let A and B be any two sets. The *relative complement* of B in A (or of B with respect to A), written as $A - B$, is the set consisting of all elements of A which are not elements of B, that is,

$$A - B = \{x \mid x \in A \land x \notin B\} = \{x \mid x \in A \land \neg(x \in B)\}$$

The relative complement of B in A is also called the *difference* of A and B.

Definition 2-1.13 Let E be the universal set. For any set A, the relative complement of A with respect to E, that is, $E - A$, is called the *absolute complement* of A. The absolute complement of a set A is often called the *complement* of A and is denoted by $\sim A$. Symbolically,

$$\sim A = E - A = \{x \mid x \in E \land x \notin A\} = \{x \mid x \notin A\} = \{x \mid \neg(x \in A)\}$$

The following equalities follow from the definition of the complement.

$$\sim(\sim A) = \sim\sim A = A \quad \sim\varnothing = E \quad \sim E = \varnothing \quad A \cup \sim A = E \quad A \cap \sim A = \varnothing \tag{4}$$

We now prove one of these equalities, viz., that $A \cup \sim A = E$:

$$(A \cup \sim A) = \{x \mid x \in A \lor x \notin A\} = E$$

EXAMPLE 5 Given $A = \{2, 5, 6\}$, $B = \{3, 4, 2\}$, $C = \{1, 3, 4\}$, find $A - B$ and $B - A$. Show that $A - B \neq B - A$ and $A - C = A$.

SOLUTION $A - B = \{5, 6\}$, $B - A = \{3, 4\}$, and $A - C = \{2, 5, 6\}$ ////

EXAMPLE 6 Show that (*a*) $A - B = A \cap \sim B$ and (*b*) $A \subseteq B \Leftrightarrow \sim B \subseteq \sim A$.

SOLUTION

(*a*) For any x,

$$\begin{aligned} x \in A - B &\Leftrightarrow x \in \{x \mid x \in A \land x \notin B\} \\ &\Leftrightarrow x \in (A \cap \sim B) \end{aligned}$$

(b)
$$A \subseteq B \Leftrightarrow (x)(x \in A \rightarrow x \in B)$$
$$\Leftrightarrow (x)(\neg(x \in B) \rightarrow \neg(x \in A))$$
$$\Leftrightarrow (x)(x \notin B) \rightarrow x \notin A)$$
$$\Leftrightarrow \sim B \subseteq \sim A$$
////

EXAMPLE 7 Show that for any two sets A and B

$$A - (A \cap B) = A - B$$

SOLUTION For any x,

$$x \in A - (A \cap B) \Leftrightarrow x \in \{x \mid x \in A \wedge x \notin (A \cap B)\}$$
$$\Leftrightarrow x \in A \wedge \sim(x \in A \wedge x \in B)$$
$$\Leftrightarrow x \in A \wedge (x \notin A \vee x \notin B)$$
$$\Leftrightarrow (x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B)$$
$$\Leftrightarrow x \in A \wedge x \notin B$$
$$\Leftrightarrow x \in \{x \mid x \in A \wedge x \notin B\}$$

Definition 2-1.14 Let A and B be any two sets. The *symmetric difference* (or *Boolean sum*) of A and B is the set $A + B$ defined by

$A + B = (A - B) \cup (B - A)$ or $x \in A + B \Leftrightarrow x \in \{x \mid x \in A \,\overline{\vee}\, x \in B\}$

where $\overline{\vee}$ is the exclusive disjunction.

The following equalities are interesting and easy to prove.

$$A + B = B + A \qquad (A + B) + C = A + (B + C) \qquad A + \varnothing = A$$
$$A + A = \varnothing \qquad \text{and} \qquad A + B = (A \cap \sim B) \cup (B \cap \sim A) \tag{5}$$

We shall now prove one of these, viz., $A + \varnothing = A$. For any x,

$$x \in A + \varnothing \Leftrightarrow x \in \{x \mid (x \in A \wedge x \notin \varnothing) \vee (x \in \varnothing \wedge x \notin A)\}$$
$$\Leftrightarrow (x \in A \wedge x \notin \varnothing) \vee (x \in \varnothing \wedge x \notin A)$$
$$\Leftrightarrow (x \in A) \vee \mathbf{F}$$
$$\Leftrightarrow x \in A$$
$$\Leftrightarrow x \in \{x \mid x \in A\}$$
$$\Leftrightarrow x \in A$$

The programming of these set operations is discussed in Sec. 2-2.

EXERCISES 2-1.4

1 Prove the equalities in Eqs. (1).
2 Given $A = \{x \mid x$ is an integer and $1 \le x \le 5\}$, $B = \{3, 4, 5, 17\}$, and $C = \{1, 2, 3, \ldots\}$, find $A \cap B$, $A \cap C$, $A \cup B$, and $A \cup C$.
3 Show that $A \subseteq A \cup B$ and $A \cap B \subseteq A$.

4 Show that $A \subseteq B \Leftrightarrow A \cup B = B$.

5 If $S = \{a, b, c\}$, find nonempty disjoint sets A_1 and A_2 such that $A_1 \cup A_2 = S$. Find other solutions to this problem.

6 Prove the equalities in Eqs. (4) and (5).

7 Given $A = \{2, 3, 4\}$, $B = \{1, 2\}$, and $C = \{4, 5, 6\}$, find $A + B$, $B + C$, $A + B + C$, and $(A + B) + (B + C)$.

2-1.5 Venn Diagrams

Introduction of the universal set permits the use of a pictorial device to study the connection between the subsets of a universal set and their intersection, union, difference, and other operations. The diagrams used are called Venn diagrams. A *Venn diagram* is a schematic representation of a set by a set of points. The universal set E is represented by a set of points in a rectangle (or any other figure), and a subset, say A, of E is represented by the interior of a circle or some other simple closed curve inside the rectangle. In Fig. 2-1.1 the shaded areas represent the sets indicated below each figure. The Venn diagram for $A \subseteq B$ and $A \cap B = \varnothing$ are also given. From some of the Venn diagrams it is

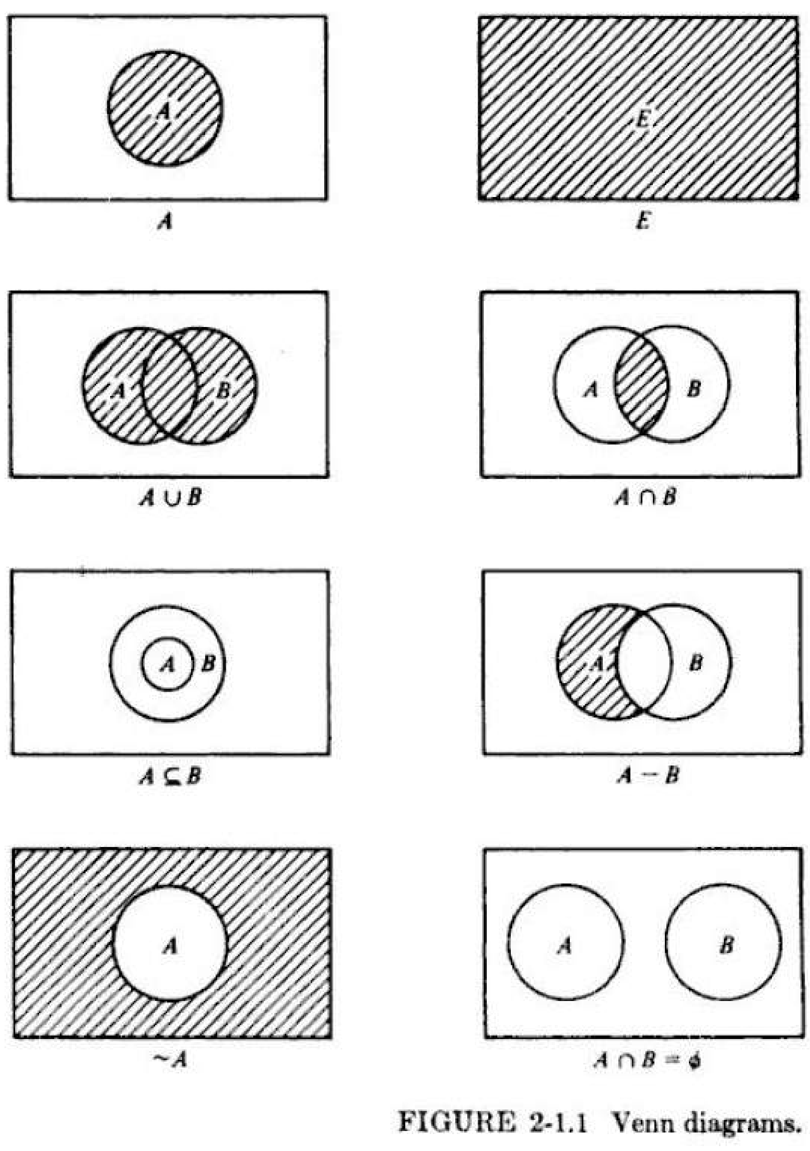


FIGURE 2-1.1 Venn diagrams.

easy to see that the following hold:

$$A \cup B = B \cup A \qquad A \cap B = B \cap A \qquad \sim(\sim A) = A$$

Furthermore, if $A \subseteq B$, then

$$A - B = \varnothing \qquad A \cap B = A \qquad \text{and} \qquad A \cup B = B$$

It should be emphasized that the above relations between the subsets are only suggested by the Venn diagram. Venn diagrams do not provide proofs that such relations are true in general for all subsets of E. We shall demonstrate this point by a particular example.

Consider the Venn diagrams given in Fig. 2-1.2. From the first two Venn diagrams it appears that

$$A \cup B = (A \cap \sim B) \cup (B \cap \sim A) \cup (A \cap B) \tag{1}$$

From the third Venn diagram it appears that

$$A \cup B = (A \cap \sim B) \cup (B \cap \sim A)$$

This equality is not true in general, although it happens to be true for the two disjoint sets A and B.

A formal proof of Eq. (1) will now be outlined. For any x,

$$x \in A \cup B \Leftrightarrow x \in \{x \mid x \in A \vee x \in B\}$$

$$\begin{aligned}
x \in\ & (A \cap \sim B) \cup (B \cap \sim A) \cup (A \cap B) \\
&\Leftrightarrow x \in \{x \mid x \in (A \cap \sim B) \vee x \in (B \cap \sim A) \vee x \in (A \cap B)\} \\
&\Leftrightarrow x \in (A \cap \sim B) \vee x \in (B \cap \sim A) \vee x \in (A \cap B) \\
&\Leftrightarrow (x \in A \wedge x \in \sim B) \vee (x \in B \wedge x \in \sim A) \vee (x \in A \wedge x \in B) \\
&\Leftrightarrow (x \in A \wedge (x \in \sim B \vee x \in B)) \vee (x \in B \wedge x \in \sim A) \\
&\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in \sim A) \\
&\Leftrightarrow (x \in A \vee x \in B) \\
&\Leftrightarrow x \in \{x \mid x \in A \vee x \in B\} \\
&\Leftrightarrow x \in A \cup B
\end{aligned}$$

Consider the Venn diagrams in Fig. 2-1.3. From the third and fifth Venn diagrams it appears that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{2}$$

Similarly, one can show that for any three sets A, B, and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{3}$$

Equations (2) and (3) are known as the *distributive laws of union and intersection.*

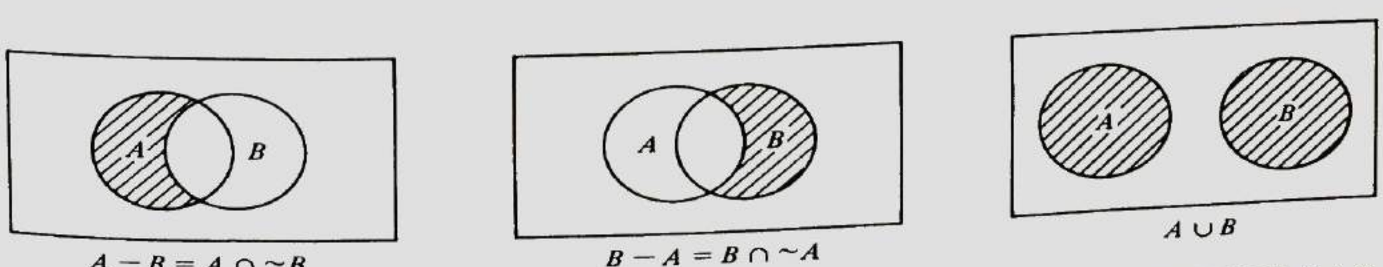


FIGURE 2-1.2

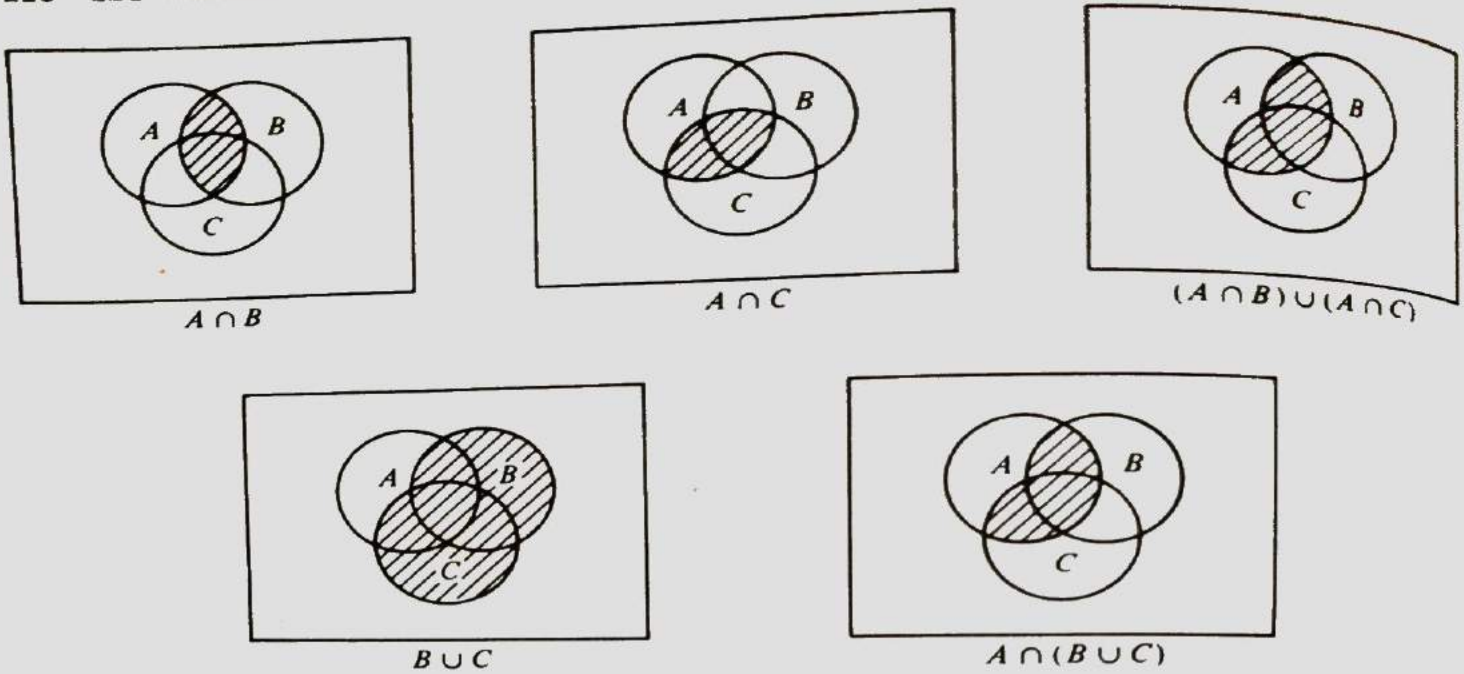


FIGURE 2-1.3

We shall now prove Eq. (3). For any x,

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in \{x \mid x \in A \vee x \in (B \cap C)\} \\ &\Leftrightarrow x \in \{x \mid x \in A \vee (x \in B \wedge x \in C)\} \\ &\Leftrightarrow x \in \{x \mid (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\} \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

EXERCISES 2-1.5

1 Prove Eq. (2).

2 Draw a Venn diagram to illustrate Eq. (3).

2-1.6 Some Basic Set Identities

Set operations such as union, intersection, complementation, etc., have been defined. With the help of these operations one can construct new sets from given sets. Capital letters have been used to denote definite sets. These letters have also been used as set variables. This practice is similar to the one employed in the statement calculus. Capital letters such as A, B, C, . . . are used as set variables; they are not exactly sets, but *set formulas*. The operations on sets can also be extended to set formulas, so that $A \cup B$, $A \cap B$, $\sim A$, etc., are all set formulas. Any well-formed string involving set variables, the operations $\cap$, $\cup$, $\sim$, and parentheses is a set formula which will also be called a set for the sake of brevity.

In fact, one obtains a set from a set formula by replacing the variables by definite sets. Two set formulas are said to be equal if they are equal as sets whenever the set variables appearing in both the formulas are replaced by any sets. It is assumed that any particular variable is replaced by the same set throughout both formulas. Since the equality of set formulas does not depend upon the sets which replace the variables, these equalities are called set *identities*. Some of the basic identities describe certain properties of the operations involved and are given special names. These properties describe an algebra called set algebra. We shall see in Chap. 4 that both the statement algebra and the set algebra are particular cases of an abstract algebra called a Boolean algebra. This fact also explains why one could see similarities between the operators in the statement calculus and the operations of set theory. For all the identities listed in this section, we have also listed the corresponding equivalences from the statement calculus. Similar equivalences hold for the predicate calculus.

Not all the identities listed here are independent. Some of the identities can be proved by assuming certain other identities. However, we have listed these identities in order to include all those identities which exhibit some basic and useful properties. Most of these identities have been proved earlier in this section, and the others can be proved either by using the same technique or by using the identities already known to be true.

In our discussion here we assume that all the sets involved are subsets of a universal set E. Although such an assumption is not necessary for many of the identities, there is no loss of generality. Furthermore, some of the identities do require such an assumption, particularly those involving complementation.

Set Algebra	*Statement Algebra*	
	Idempotent laws	
$A \cup A = A$	$P \vee P \Leftrightarrow P$	(1)
$A \cap A = A$	$P \wedge P \Leftrightarrow P$	
	Associative laws	
$(A \cup B) \cup C = A \cup (B \cup C)$	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	(2)
$(A \cap B) \cap C = A \cap (B \cap C)$	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	
	Commutative laws	
$A \cup B = B \cup A$	$P \vee Q \Leftrightarrow Q \vee P$	(3)
$A \cap B = B \cap A$	$P \wedge Q \Leftrightarrow Q \wedge P$	
	Distributive laws	
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (Q \vee R)$	(4)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	
$A \cup \varnothing = A$	$P \vee \mathbf{F} \Leftrightarrow P$	(5)
$A \cap E = A$	$P \wedge \mathbf{T} \Leftrightarrow P$	
$A \cup E = E$	$P \vee \mathbf{T} \Leftrightarrow \mathbf{T}$	(6)
$A \cap \varnothing = \varnothing$	$P \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	
$A \cup \sim A = E$	$P \vee \neg P \Leftrightarrow \mathbf{T}$	(7)
$A \cap \sim A = \varnothing$	$P \wedge \neg P \Leftrightarrow \mathbf{F}$	
	Absorption laws	
$A \cup (A \cap B) = A$	$P \vee (P \wedge Q) \Leftrightarrow P$	(8)
$A \cap (A \cup B) = A$	$P \wedge (P \vee Q) \Leftrightarrow P$	
	De Morgan's laws	
$\sim(A \cup B) = \sim A \cap \sim B$	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	(9)
$\sim(A \cap B) = \sim A \cup \sim B$	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	
$\sim \varnothing = E$	$\neg \mathbf{F} \Leftrightarrow \mathbf{T}$	(10)
$\sim E = \varnothing$	$\neg \mathbf{T} \Leftrightarrow \mathbf{F}$	
$\sim(\sim A) = A$	$\neg \neg P \Leftrightarrow P$	(11)

All the identities just given are presented in pairs except for the identity (11). This pairing is done because a principle of duality similar to the one given for statement algebra (see Sec. 1-2.10) also holds in the case of set algebra. In fact, the principle of duality holds for any Boolean algebra. At present it is sufficient to note that given any identity of the set algebra, one can obtain another identity by interchanging $\cup$ with $\cap$ and E with $\varnothing$.

Assuming identities (4) to (6), we shall prove the absorption laws. First note that

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

from the distributive and idempotent laws. Now

$$\begin{aligned} A \cup (A \cap B) &= (A \cap E) \cup (A \cap B) && \text{from (5)} \\ &= A \cap (E \cup B) && \text{from (4)} \\ &= A \cap E && \text{from (6)} \\ &= A && \text{from (5)} \end{aligned}$$

Alternatively one can prove it as follows. For any x,

$$\begin{aligned} x \in A \cup (A \cap B) &\Leftrightarrow x \in \{x \mid (x \in A) \vee ((x \in A) \wedge (x \in B))\} \\ &\Leftrightarrow x \in \{x \mid x \in A\} \\ &\Leftrightarrow x \in A \end{aligned}$$

using the absorption laws of predicate calculus.

In order to complete our discussion, we list some implications and certain set inclusions

$$(A \cup B \neq \varnothing) \Rightarrow (A \neq \varnothing) \vee (B \neq \varnothing) \qquad (12)$$

$$(A \cap B \neq \varnothing) \Rightarrow (A \neq \varnothing) \wedge (B \neq \varnothing) \qquad (13)$$

To prove the implication (12), let us assume that $A \neq \varnothing \vee B \neq \varnothing$ is *false*. This requires that $A \neq \varnothing$ is *false* and also that $B \neq \varnothing$ is *false*, that is, $A = B = \varnothing$. But then $A \cup B = \varnothing$, so that $A \cup B \neq \varnothing$ is also *false*. Hence the implication is proved. One could also have proved (12) by assuming that $A \cup B \neq \varnothing$ is *true* and showing that this assumption requires $A \neq \varnothing \vee B \neq \varnothing$ to be *true*. Implication (13) can be proved in a similar manner.

The following inclusions follow from the definition and have been proved earlier in this section.

$$A \cap B \subseteq A \qquad A \cap B \subseteq B \qquad A \subseteq A \cup B \qquad A - B \subseteq A \qquad (14)$$

Let A be a family of indexed sets over an index set I such that $A = \{A_1, A_2, \ldots\} = \{A_i\}_{i \in \mathbf{I}}$. Then

$$\bigcup_{i \in \mathbf{I}} A_i = \{x \mid x \in A_i \text{ for some } i \in \mathbf{I}\} \qquad (15)$$

$$\bigcap_{i \in \mathbf{I}} A_i = \{x \mid x \in A_i \text{ for every } i \in \mathbf{I}\} \qquad (16)$$

The associative laws and the distributive laws can be generalized in the following manner.

$$B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i) \tag{17}$$

$$B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$$

The identities (17) can be proved using mathematical induction discussed later in Sec. 2-5.1. We now give some examples illustrating the above operations.

EXAMPLE 1 Verify the identities (17) for

$$A_1 = \{1, 5\} \qquad A_2 = \{1, 2, 4, 6\} \qquad A_3 = \{3, 4, 7\}$$

$$B = \{2, 4\} \qquad \text{and} \qquad I = \{1, 2, 3\}$$

SOLUTION

$$\bigcup_{i \in I} A_i = \{1, 2, 3, 4, 5, 6, 7\}$$

$$\bigcap_{i \in I} A_i = \varnothing$$

$$B \cup (\bigcap_{i \in I} A_i) = \{2, 4\}$$

$$\bigcap_{i \in I} (B \cup A_i) = \{1, 2, 4, 5\} \cap \{1, 2, 4, 6\} \cap \{2, 3, 4, 7\} = \{2, 4\}$$

$$B \cap (\bigcup_{i \in I} A_i) = \{2, 4\}$$

$$\bigcup_{i \in I} (B \cap A_i) = \varnothing \cup \{2, 4\} \cup \{4\} = \{2, 4\}$$ ////

2-1.7 The Principle of Specification

The idea of a set was discussed in the beginning of this chapter, although we had used the notion earlier in Chap. 1 while discussing the universe of discourse or the domain of the object variable (see Sec. 1-5.5). The universe of discourse was defined as the set of all objects under consideration, and this set is the same as the universal set defined in Sec. 2-1.2.

A set is usually defined by means of a predicate. The connection between a predicate and a set defined by it is known as the *principle of specification*, which states that every predicate specifies a set which is a subset of a universal set. The subset specified by a predicate is called an *extension* of the predicate in the universal set. This method has been used extensively in defining sets. For example, if $P(x)$ is a predicate, then a set A is called an extension of $P(x)$ if

$$A = \{x \mid P(x)\}$$

A predicate can be considered as a condition, and any object of the universal set satisfying the condition is then an element of the set which is an extension of the predicate. Obviously, if two predicates are equivalent, then they have the same extension, and the two sets specified by equivalent predicates are equal. In other words, if $P(x) \Leftrightarrow Q(x)$, then $A = B$ where A and B are the extensions of $P(x)$ and $Q(x)$, respectively. We now have an analogy between the equality of sets and the equivalence of predicates. A similar analogy exists between set inclusion and implication. If $P(x) \Rightarrow Q(x)$, then $A \subseteq B$ where, again, A and B are extensions of $P(x)$ and $Q(x)$ respectively.

If $P(x)$ is identically *true* for all x in E, then the extension of $P(x)$ in the universal set is the universal set itself. Similarly, if $P(x)$ is identically *false* for all x in E, then the extension of $P(x)$ in E is the null set. Recall that the universal set and the null set were defined as extensions of $P(x) \vee \neg P(x)$ and $P(x) \wedge \neg P(x)$ respectively. However, any other identically *true* (valid) and *false* predicates could have been used to define them.

If A and B are extensions of the predicates $P(x)$ and $Q(x)$, respectively, in a universal set E, then it is easy to see that $A \cup B$ and $A \cap B$ are the extensions of $P(x) \vee Q(x)$ and $P(x) \wedge Q(x)$ respectively. Similarly $\sim A$ is the extension of $\neg P(x)$. The extension of $P(x) \rightarrow Q(x)$ is the set $\sim A \cup B$, and that of $P(x) \rightleftarrows Q(x)$ is the set $(\sim A \cup B) \cap (A \cup \sim B)$. Thus the new sets formed from the sets A and B can be interpreted in terms of extensions of formulas containing $P(x)$ and $Q(x)$.

From the above discussion it is clear that all the identities of set theory given in the previous section should follow from the corresponding equivalence of predicate formulas. Similarly, the inclusions of sets should follow from the corresponding implications of predicates. If we replace the predicates by their extensions—$\wedge$ by $\cap$, $\vee$ by $\cup$, and $\neg$ by $\sim$—in any predicate formula, then we obtain the corresponding formula of set theory. Also, the equivalences and implications are replaced by equality and inclusions of sets. In fact, this technique has often been used in proving the identities and other relations of set theory so far. For example, let us consider

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

If A and B denote the extensions of $P(x)$ and $Q(x)$ respectively, then we can write

$$\sim(A \cup B) = \sim A \cap \sim B$$

Similarly, from

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

we get

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad [C \text{ is the extension of } R(x)]$$

2-1.8 Ordered Pairs and n-tuples

So far we have been solely concerned with sets, their equality, and operations on sets to form new sets. We now introduce the notion of an ordered pair. Although it is possible to define ordered pairs rigorously, we shall give an intuitive definition.

An *ordered pair* consists of two objects in a given fixed order. Note that an ordered pair is not a set consisting of two elements. The ordering of the two objects is important. The two objects need not be distinct. We shall denote an ordered pair by $\langle x, y \rangle$. A familiar example of an ordered pair is the representation of a point in a two-dimensional plane in cartesian coordinates. Accordingly, the ordered pairs $\langle 1, 3\rangle$, $\langle 2, 4\rangle$, $\langle 1, 2\rangle$, and $\langle 2, 1\rangle$ represent different points in a plane.

The *equality* of two ordered pairs $\langle x, y\rangle$ and $\langle u, v\rangle$ is defined by

$$\langle x, y\rangle = \langle u, v\rangle \Leftrightarrow ((x = u) \wedge (y = v)) \tag{1}$$

so that $\langle 1, 2\rangle \neq \langle 2, 1\rangle$ and $\langle 1, 1\rangle \neq \langle 2, 2\rangle$. A distinction between ordered pairs and sets containing two elements will be clear from the following examples:

$$\{a, b\} = \{b, a\} = \{a, a, b\} \qquad \{a, a\} = \{a\} \qquad \langle a, b\rangle \neq \langle b, a\rangle \qquad \langle a, a\rangle \neq \{a\}$$

The idea of an ordered pair can be extended to define an ordered triple, and, more generally, an n-tuple.

An *ordered triple* is an ordered pair whose first member is itself an ordered pair. Thus an ordered triple can be written as $\langle\langle x, y\rangle, z\rangle$. From the definition of the equality of an ordered pair, we can arrive at the equality of ordered triples $\langle\langle x, y\rangle, z\rangle$ and $\langle\langle u, v\rangle, w\rangle$:

$$\langle\langle x, y\rangle, z\rangle = \langle\langle u, v\rangle, w\rangle \qquad \text{iff} \qquad \langle x, y\rangle = \langle u, v\rangle \wedge z = w$$

But, $\langle x, y\rangle = \langle u, v\rangle$ if $(x = u \wedge y = v)$. Therefore

$$\langle\langle x, y\rangle, z\rangle = \langle\langle u, v\rangle, w\rangle \Leftrightarrow ((x = u) \wedge (y = v) \wedge (z = w)) \tag{2}$$

From the above definition of equality of an ordered triple, we may write an ordered triple as $\langle x, y, z\rangle$ with an understanding that $\langle x, y, z\rangle$ stands for $\langle\langle x, y\rangle, z\rangle$. Note that

$$\langle x, y, z\rangle \neq \langle y, x, z\rangle \neq \langle x, z, y\rangle$$

An ordered quadruple can be defined as an ordered pair whose first member is an ordered triple. Thus, an ordered quadruple is written as $\langle\langle x, y, z\rangle, u\rangle$ which is actually $\langle\langle\langle x, y\rangle, z\rangle, u\rangle$. It is easy to show that two ordered quadruples $\langle\langle x, y, z\rangle, u\rangle$ and $\langle\langle p, q, r\rangle, s\rangle$ are equal provided that

$$(x = p) \wedge (y = q) \wedge (z = r) \wedge (u = s) \tag{3}$$

In view of this fact, we shall write an ordered quadruple as $\langle x, y, z, u\rangle$.

Continuing this process, an ordered n-tuple is defined to be an ordered pair whose first member is an ordered $(n - 1)$-tuple. We write an ordered n-tuple as $\langle\langle x_1, x_2, \ldots, x_{n-1}\rangle, x_n\rangle$. Further, given two ordered n-tuples $\langle\langle x_1, x_2, \ldots, x_{n-1}\rangle, x_n\rangle$ and $\langle\langle u_1, u_2, \ldots, u_{n-1}\rangle, u_n\rangle$, we have

$$\langle\langle x_1, x_2, \ldots, x_{n-1}\rangle, x_n\rangle = \langle\langle u_1, u_2, \ldots, u_{n-1}\rangle, u_n\rangle$$
$$\Leftrightarrow ((x_1 = u_1) \wedge (x_2 = u_2) \wedge \cdots \wedge (x_n = u_n))$$

Therefore, an ordered n-tuple will be written as $\langle x_1, x_2, \ldots, x_n\rangle$.

2-1.9 Cartesian Products

Definition 2-1.15 Let A and B be any two sets. The set of all ordered pairs such that the first member of the ordered pair is an element of A and the second member is an element of B is called the *cartesian product* of A

and B and is written as $A \times B$. Accordingly,

$$A \times B = \{\langle x, y\rangle \mid (x \in A) \wedge (y \in B)\}$$

EXAMPLE 1 If $A = \{\alpha, \beta\}$ and $B = \{1, 2, 3\}$, what are $A \times B$, $B \times A$, $A \times A$, $B \times B$, and $(A \times B) \cap (B \times A)$?

SOLUTION

$$\begin{aligned}
A \times B &= \{\langle \alpha, 1\rangle, \langle \alpha, 2\rangle, \langle \alpha, 3\rangle, \langle \beta, 1\rangle, \langle \beta, 2\rangle, \langle \beta, 3\rangle\} \\
B \times A &= \{\langle 1, \alpha\rangle, \langle 2, \alpha\rangle, \langle 3, \alpha\rangle, \langle 1, \beta\rangle, \langle 2, \beta\rangle, \langle 3, \beta\rangle\} \\
A \times A &= \{\langle \alpha, \alpha\rangle, \langle \alpha, \beta\rangle, \langle \beta, \alpha\rangle, \langle \beta, \beta\rangle\} \\
B \times B &= \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \\
&\qquad \langle 3, 2\rangle, \langle 3. 3\rangle\}
\end{aligned}$$

$(A \times B) \cap (B \times A) = \varnothing$ ////

EXAMPLE 2 If $A = \varnothing$ and $B = \{1, 2, 3\}$ what are $A \times B$ and $B \times A$?

SOLUTION

$$A \times B = \varnothing = B \times A \qquad ////$$

Before we consider the cartesian product of more than two sets let us consider the expressions $(A \times B) \times C$ and $A \times (B \times C)$. From the definition it follows that

$$\begin{aligned}
(A \times B) \times C &= \{\langle\langle a, b\rangle, c\rangle \mid (\langle a, b\rangle \in A \times B) \wedge (c \in C)\} \\
&= \{\langle a, b, c\rangle \mid (a \in A) \wedge (b \in B) \wedge (c \in C)\} \qquad (1)
\end{aligned}$$

The last step follows from our definition of the ordered triple given in Sec. 2-1.8. Next,

$$A \times (B \times C) = \{\langle a, \langle b, c\rangle\rangle \mid (a \in A) \wedge (\langle b, c\rangle \in B \times C)\}$$

Here $\langle a, \langle b, c\rangle\rangle$ is not an ordered triple. If we consider $(A \times B) \times C$ as an ordered pair, then the first member is an ordered pair and the second member is an element of C. On the other hand, $A \times (B \times C)$ is an ordered pair in which the first member is an element of A while the second member is an ordered pair. This fact shows that

$$(A \times B) \times C \neq A \times (B \times C)$$

Before defining the cartesian product of any finite number of sets, we shall show that the cartesian product satisfies the following distributive properties.

For any three sets A, B, and C

$$\begin{aligned}
A \times (B \cup C) &= (A \times B) \cup (A \times C) \\
A \times (B \cap C) &= (A \times B) \cap (A \times C) \qquad (2)
\end{aligned}$$

We now prove the first of these two identities.

$$
\begin{aligned}
A \times (B \cup C) &= \{\langle x\ y\rangle \mid (x \in A) \wedge (y \in B \cup C)\}\\
&= \{\langle x, y\rangle \mid (x \in A) \wedge ((y \in B) \vee (y \in C))\}\\
&= \{\langle x, y\rangle \mid ((x \in A) \wedge (y \in B)) \vee ((x \in A) \wedge (y \in C))\}\\
&= (A \times B) \cup (A \times C)
\end{aligned}
$$

The second equality in Eq. (2) can be proved in a similar manner.

Let $A = \{A_i\}_{i \in \mathbf{I}_n}$ be an indexed set and $\mathbf{I}_n = \{1, 2, \ldots, n\}$. We denote the cartesian product of the sets $A_1, A_2, \ldots, A_n$ by

$$\mathop{\times}_{i \in \mathbf{I}_n} A_i = A_1 \times A_2 \times \cdots \times A_n$$

which is defined by

$$\mathop{\times}_{i \in \mathbf{I}_1} A_i = A_1 \qquad \text{and} \qquad \mathop{\times}_{i \in \mathbf{I}_m} A_i = (\mathop{\times}_{i \in \mathbf{I}_{m-1}} A_i) \times A_m \qquad \text{for } m = 2, 3, \ldots, n$$

According to the above definition,

$$A_1 \times A_2 \times A_3 = (A_1 \times A_2) \times A_3$$

and

$$
\begin{aligned}
A_1 \times A_2 \times A_3 \times A_4 &= (A_1 \times A_2 \times A_3) \times A_4\\
&= ((A_1 \times A_2) \times A_3) \times A_4
\end{aligned}
$$

Our definition of cartesian product of n sets is related to the definition of n-tuples in the sense that

$$
\begin{aligned}
A_1 \times A_2 \times \ldots \times A_n = \{\langle x_1, x_2, \ldots, x_n\rangle \mid (x_1 \in A_1)\\
\wedge (x_2 \in A_2) \wedge \cdots \wedge (x_n \in A_n)\}
\end{aligned}
$$

The cartesian product $A \times A$ is also written as A^2, and similarly $A \times A \times A$ as A^3, and so on.

EXERCISES 2-1

1 Give examples of sets A, B, C such that $A \cup B = A \cup C$, but $B \neq C$.

2 Write the sets

$$\varnothing \cap \{\varnothing\} \qquad \{\varnothing\} \cap \{\varnothing\} \qquad \{\varnothing, \{\varnothing\}\} - \varnothing$$

3 Write the members of $\{a, b\} \times \{1, 2, 3\}$.

4 Write $A \times B \times C$, B^2, A^3, $B^2 \times A$, and $A \times B$ where $A = \{1\}$, $B = \{a, b\}$, and $C = \{2, 3\}$.

5 Show by means of an example that $A \times B \neq B \times A$ and $(A \times B) \times C \neq A \times (B \times C)$.

6 Show that for any two sets A and B

$$
\begin{aligned}
\rho(A) \cup \rho(B) &\subseteq \rho(A \cup B)\\
\rho(A) \cap \rho(B) &= \rho(A \cap B)
\end{aligned}
$$

Show by means of an example that

$$\rho(A) \cup \rho(B) \neq \rho(A \cup B)$$

7 Prove the identities

$$A \cap A = A \qquad A \cap \varnothing = \varnothing \qquad A \cap E = A \qquad \text{and } A \cup E = E$$

8 Show that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

9 Prove that

$$(A \cap B) \cup (A \cap \sim B) = A$$

and

$$A \cap (\sim A \cup B) = A \cap B$$

10 Show that $A \times B = B \times A \Leftrightarrow (A = \varnothing) \vee (B = \varnothing) \vee (A = B)$.

11 Show that $(A \cap B) \cup C = A \cap (B \cup C)$ iff $C \subseteq A$.

12 Draw Venn diagrams showing

$$A \cup B \subset A \cup C \quad \text{but} \quad B \not\subseteq C$$
$$A \cap B \subset A \cap C \quad \text{but} \quad B \not\subseteq C$$
$$A \cup B = A \cup C \quad \text{but} \quad B \neq C$$
$$A \cap B = A \cap C \quad \text{but} \quad B \neq C$$

13 Draw Venn diagrams and show the sets

$$\sim B \qquad \sim(A \cup B) \qquad B - (\sim A) \qquad \sim A \cup B \qquad \sim A \cap B$$

where $A \cap B \neq \varnothing$.

14 Show that $(A + B) + C = A + (B + C)$.

15 Prove that $A + A = \varnothing$ and $A + \varnothing = A$.

16 Show that $(A - B) - C = (A - C) - (B - C)$.

17 Prove that $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

2-3 RELATIONS AND ORDERING

The concept of a relation is a basic concept in everyday life as well as in mathematics. We have already used various relations. Associated with a relation is the act of comparing objects which are related to one another. The ability of a computer to perform different tasks based upon the result of a comparison is one of its most important attributes which is used several times during the execution of a typical program. In this section we first formalize the concept of a relation and then discuss methods of representing a relation by using a matrix or its graph. The relation matrix is useful in determining the properties of a relation and also in representing a relation on a computer. Various basic properties of relations are given, and certain important classes of relations are introduced. Among these, the compatibility relation and the equivalence relation have useful applications in the design of digital computers and other sequential machines. Partial ordering and its associated terminology are introduced next. The material in Chap. 4 is based upon these notions. Several relations given as examples in this section are used throughout the book. Algorithms to determine certain properties of relations are also given.

2-3.1 Relations

The word "relation" suggests some familiar examples of relations such as the relation of father to son, mother to son, brother to sister, etc. Familiar examples in arithmetic are relations such as "greater than," "less than," or that of equality between two real numbers. We also know the relation between the area of a circle and its radius and between the area of a square and its side. These examples suggest relationships between two objects. The relation between parents and child, the coincidence of three lines, and that of a point lying between two points are examples of relations among three objects. Similar examples exist for relations among four or more objects.

Here, we shall only consider relations, called binary relations, between a pair of objects. Before we give a set-theoretic definition of a relation, we note that a relation between two objects can be defined by listing the two objects as an ordered pair. A set of all such ordered pairs, in each of which the first member has some definite relationship to the second, describes a particular relationship. Of course, we have been motivated by relationships which are familiar and could be given a name. However, this is an undue restriction which will not appear in our definition of a relation.

Definition 2-3.1 Any set of ordered pairs defines a *binary relation.*

We shall call a binary relation simply a relation. It is sometimes convenient to express the fact that a particular ordered pair, say $\langle x, y \rangle \in R$, where R is a relation, by writing $x \; R \; y$ which may be read as "x is in relation R to y."

In mathematics, relations are often denoted by special symbols rather than by capital letters. A familiar example is the relation "greater than" for real numbers. This relation is denoted by $>$. In fact, $>$ should be considered as the name of a set whose elements are ordered pairs. Each member of any of the ordered pairs in the set is a real number, and if a and b are two real numbers such that $a > b$, then we say that $\langle a, b \rangle \in \, >$, or $a > b$. More precisely the relation $>$ is

$$> \; = \{ \langle x, y \rangle \mid x, y \text{ are real numbers and } x > y \} \tag{1}$$

The relation of father to his child can be described by a set, say F, of ordered pairs in which the first member is the name of the father and the second the name of his child. That is,

$$F = \{ \langle x, y \rangle \mid x \text{ is the father of } y \} \tag{2}$$

The definition of relation permits any set of ordered pairs to define a relation. For example, the set S given by

$$S = \{ \langle 2, 4 \rangle, \langle 1, 3 \rangle, \langle \lambda, 6 \rangle, \langle \text{Joan}, \mu \rangle \} \tag{3}$$

can be considered as a relation. Of course, such a relation may not be familiar or interesting.

Let $\mathbf{R}$ denote the set of real numbers. Then

$$Q = \{\langle x^2, x\rangle \mid x \in \mathbf{R}\} \tag{4}$$

defines the relation of the square of a real number.

Definition 2-3.2 Let S be a binary relation. The set $D(S)$ of all objects x such that for some y, $\langle x, y\rangle \in S$ is called the *domain* of S, that is,

$$D(S) = \{x \mid (\exists y)(\langle x, y\rangle \in S)\}$$

Similarly, the set $R(S)$ of all objects y such that for some x, $\langle x, y\rangle \in S$ is called the *range* of S, that is,

$$R(S) = \{y \mid (\exists x)(\langle x, y\rangle \in S)\}$$

For the relation S described in Eq. (3) we have

$$D(S) = \{2, 1, \lambda, \text{Joan}\} \quad \text{and} \quad R(S) = \{4, 3, 6, \mu\}$$

Let X and Y be any two sets. A subset of the cartesian product $X \times Y$ defines a relation, say C. For any such relation C, we have $D(C) \subseteq X$ and $R(C) \subseteq Y$, and the relation C is said to be from X to Y. If $Y = X$, then C is said to be a relation from X to X. In such a case, C is called a relation in X. Thus any relation in X is a subset of $X \times X$. The set $X \times X$ itself defines a relation in X and is called a *universal relation* in X, while the empty set which is also a subset of $X \times X$ is called a *void relation* in X.

The relations given in Eqs. (1) and (4) are in the set $\mathbf{R}$ of real numbers. The relation in Eq. (2) is in the set of all human beings. It could also be considered as a relation from the set of all males to the set of human beings. The relation S in Eq. (3) can be considered from a set X to a set Y where $\{2, 1, \lambda, \text{Joan}\} \subseteq X$ and $\{4, 3, 6, \mu\} \subseteq Y$. In fact any relation from a set X to a set Y can also be considered as a relation in $X \cup Y$.

If $\mathbf{R}$ is the set of real numbers, then the elements of $\mathbf{R} \times \mathbf{R}$ can be represented by points in a plane, as shown in Sec. 2-1.8. Some of the subsets of $\mathbf{R} \times \mathbf{R}$ define familiar relations which can be shown graphically. For example, consider the relations in which $x * y$ means xy

$$\begin{aligned} R_1 &= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge x * y \geq 1\} \\ R_2 &= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge x^2 + y^2 \leq 9\} \\ R_3 &= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge y^2 < x\} \end{aligned} \tag{5}$$

R_1 can be represented by points on one side of a hyperbola, R_2 by points inside or on a circle of radius 3, and R_3 by points on one side of a parabola. These relations are displayed in Fig. 2-3.1.

A relation has been defined as a set of ordered pairs. It is therefore possible to apply the usual operations of sets to relations as well. The resulting sets will also be ordered pairs and will define some relation. If R and S denote two relations, then $R \cap S$ defines a relation such that

$$x\,(R \cap S)\,y \Leftrightarrow x\,R\,y \wedge x\,S\,y$$

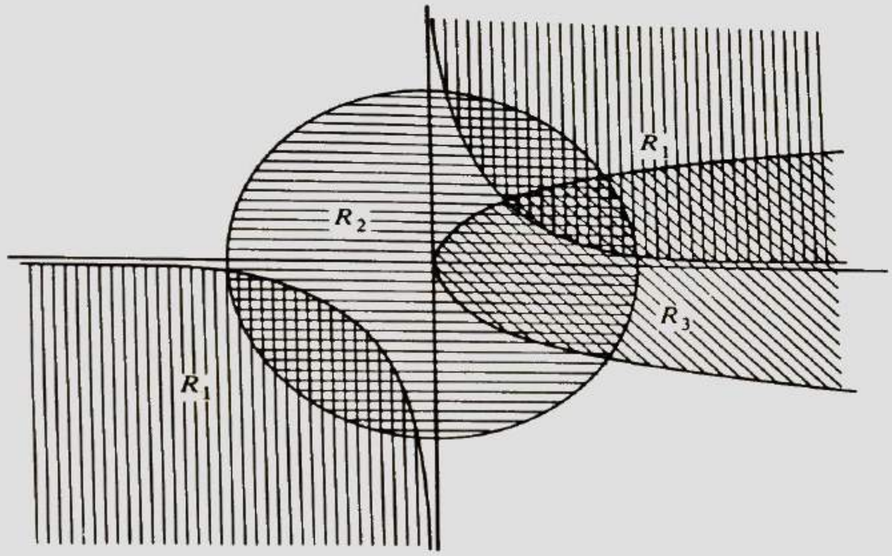


FIGURE 2-3.1

Similarly, $R \cup S$ is a relation such that

$$x\ (R \cup S)\ y \Leftrightarrow x\ R\ y \vee x\ S\ y$$

Also

$$x\ (R - S)\ y \Leftrightarrow x\ R\ y \wedge x \not S\ y$$

and

$$x\ (\sim R)\ y \Leftrightarrow x \not R\ y$$

EXAMPLE 1 (*a*) Let $X = \{1, 2, 3, 4\}$. If

$R = \{\langle x, y\rangle \mid x \in X \wedge y \in X \wedge ((x - y)$ is an integral nonzero multiple of 2)$\}$
$= \{\langle 1, 3\rangle, \langle 3, 1\rangle, \langle 2, 4\rangle, \langle 4, 2\rangle\}$

$S = \{\langle x, y\rangle \mid x \in X \wedge y \in X \wedge ((x - y)$ is an integral nonzero multiple of 3)$\}$
$= \{\langle 1, 4\rangle, \langle 4, 1\rangle\}$

Find $R \cup S$ and $R \cap S$.

(*b*) If $X = \{1, 2, 3, \ldots\}$, what is $R \cap S$ for R and S as defined in (*a*)?

SOLUTION

(*a*) $R \cup S = \{\langle 1, 3\rangle, \langle 3, 1\rangle, \langle 2, 4\rangle, \langle 4, 2\rangle, \langle 1, 4\rangle, \langle 4, 1\rangle\}$ and $R \cap S = \varnothing$.
(*b*) $R \cap S = \{\langle x, y\rangle \mid x \in X \wedge y \in X \wedge ((x - y)$ is a nonzero multiple of 6)$\}$.
////

Let us return to the relations R_1, R_2, R_3 given in Eq. (5). The predicates P_1, P_2, and P_3 defined by

$$P_1\colon x * y \geq 1 \qquad P_2\colon x^2 + y^2 \leq 9 \qquad P_3\colon y^2 < x$$

describe the relations R_1, R_2, and R_3 respectively. Recall from Sec. 2-1.7 that associated with each predicate is an extension set. A more complex predicate such as $P_1 \wedge P_2 \wedge P_3$ having an extension set $R_1 \cap R_2 \cap R_3$ can be written. Given the coordinates of a point $\langle x, y\rangle$, it is instructive to determine whether $\langle x, y\rangle$ is a member of each of the following sets:

$$R_4 = R_1 \cap R_2 \cap R_3$$

$$= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge x * y \geq 1 \wedge x^2 + y^2 \leq 9 \wedge y^2 < x\}$$

$$R_5 = R_2 \cap (R_1 \cup R_3) \cap \sim(R_1 \cap R_3)$$

$$= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge x^2 + y^2 \leq 9 \wedge (x * y \geq 1 \vee y^2 < x)$$
$$\wedge \sim(x * y \geq 1 \wedge y^2 < x)\}$$

$$R_6 = R_1 \cap \sim R_2 \cap R_3.$$

$$= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge x * y \geq 1 \wedge \sim(x^2 + y^2 \leq 9) \wedge y^2 < x\}$$

$$R_7 = \sim(R_1 \cup R_3) \cap R_2$$

$$= \{\langle x, y\rangle \mid \langle x, y\rangle \in \mathbf{R} \times \mathbf{R} \wedge \sim(x * y \geq 1 \vee y^2 < x) \wedge x^2 + y^2 \leq 9\}$$

R_4 includes all points lying within the circle and the parabola and above the hyperbola of the first quadrant. R_5 includes all points within the circle which lie either within the parabola or above the hyperbola of the first quadrant, but not both, and all points within the circle and below the hyperbola in the third quadrant. R_6 includes all points lying above the hyperbola and within the parabola in the first quadrant. R_7 includes all points lying within the circle and between the hyperbolic curves but not within the parabola.

These newly defined sets can pictorially be represented as shown in Fig. 2-3.2. The program given in Fig. 2-3.3 reads a number of coordinate points and determines whether these points lie in the sets R_4 to R_7. Note that the relations R_4 to R_7 are written as predicates P_4 to P_7 in the program.

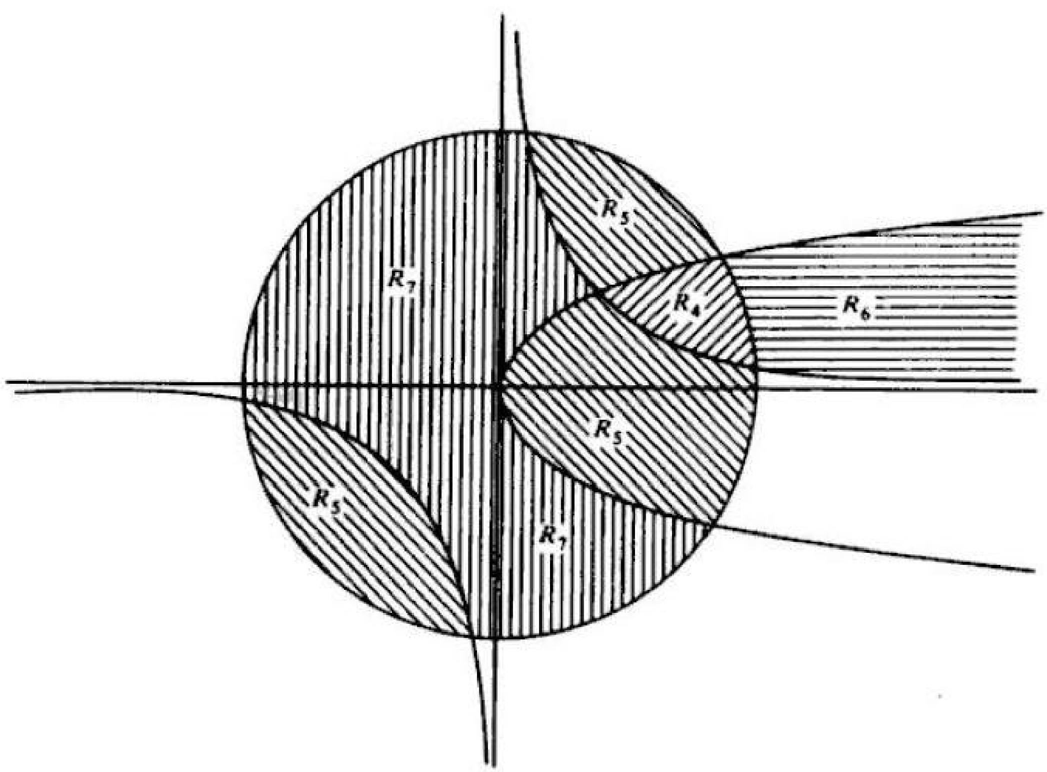


FIGURE 2-3.2

Find $P \cup Q$, $P \cap Q$, $D(P)$, $D(Q)$, $D(P \cup Q)$, $R(P)$, $R(Q)$, and $R(P \cap Q)$. Show that

$$D(P \cup Q) = D(P) \cup D(Q)$$

and

$$R(P \cap Q) \subseteq R(P) \cap R(Q)$$

2 What are the ranges of the relations

$$S = \{\langle x, x^2 \rangle \mid x \in \mathbf{N}\} \quad \text{and} \quad T = \{\langle x, 2x \rangle \mid x \in \mathbf{N}\}$$

where $\mathbf{N} = \{0, 1, 2, \ldots\}$? Find $R \cup S$ and $R \cap S$.

3 Let L denote the relation "less than or equal to" and D denote the relation "divides," where $x\,D\,y$ means "x divides y." Both L and D are defined on the set $\{1, 2, 3, 6\}$. Write L and D as sets, and find $L \cap D$.

2-3.2 Properties of Binary Relations in a Set

Definition 2-3.3 A binary relation R in a set X is *reflexive* if, for every $x \in X$, $x\,R\,x$, that is, $\langle x, x \rangle \in R$, or

$$R \text{ is reflexive in } X \Leftrightarrow (x)(x \in X \rightarrow x\,R\,x)$$

The relation $\leq$ is reflexive in the set of real numbers since, for any x, we have $x \leq x$. Similarly, the relation of inclusion is reflexive in the family of all subsets of a universal set. The relation of equality of sets is also reflexive. However, the relation $<$ is not reflexive in the set of real numbers, and the relation of proper inclusion is not reflexive in the family of subsets of a universal set.

Definition 2-3.4 A relation R in a set X is *symmetric* if, for every x and y in X, whenever $x\,R\,y$, then $y\,R\,x$. That is,

$$R \text{ is symmetric in } X \Leftrightarrow (x)(y)(x \in X \wedge y \in X \wedge x\,R\,y \rightarrow y\,R\,x)$$

The relations $\leq$ and $<$ are not symmetric in the set of real numbers, while the relation of equality is. The relation of similarity in the set of triangles in a plane is both reflexive and symmetric. The relation of being a brother is not symmetric in the set of all people. However, in the set of all males it is symmetric.

Definition 2-3.5 A relation R in a set X is *transitive* if, for every x, y, and z in X, whenever $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$. That is,

$$R \text{ is transitive in } X \Leftrightarrow (x)(y)(z)(x \in X \wedge y \in X \wedge z \in X \wedge x\,R\,y \wedge y\,R\,z \rightarrow x\,R\,z)$$

The relations $\leq$, $<$, and $=$ are transitive in the set of real numbers. The relations $\subseteq$, $\subset$, and equality are also transitive in the family of subsets of a universal set. The relation of similarity of triangles in a plane is transitive, while the relation of being a mother is not.

Definition 2-3.6 A relation R in a set X is *irreflexive* if, for every $x \in X$, $\langle x, x \rangle \notin R$.

Note that any relation which is not reflexive is not necessarily irreflexive, and vice versa. The relation $<$ in the set of real numbers is irreflexive because for no x do we have $x < x$. Similarly, the relation of proper inclusion in the set of all nonempty subsets of a universal set is irreflexive. The following is a simple example of a relation in $\{1, 2, 3\}$ which is not reflexive and not irreflexive:

$$S = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 3, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$$

Definition 2-3.7 A relation R in a set X is *antisymmetric* if, for every x and y in X, whenever $x \mathrel{R} y$ and $y \mathrel{R} x$, then $x = y$. Symbolically, R is antisymmetric in x iff

$$(x)(y)(x \in X \wedge y \in X \wedge x \mathrel{R} y \wedge y \mathrel{R} x \rightarrow x = y)$$

Note that it is possible to have a relation which is both symmetric and antisymmetric. This is obviously the case when each element is either related to itself or not related to any element.

Some known relations and their properties are now given.

Let **R** be the set of real numbers. The relations $>$ (greater than) and $<$ (less than) in **R** are both irreflexive and transitive. Also the relation $=$ (equality) in **R** is reflexive, symmetric, and transitive.

Let X be the set of all courses offered at a university, and for $x \in X$ and $y \in X$, $x \mathrel{R} y$ if x is a prerequisite for y. The relation of being a prerequisite is irreflexive and transitive.

Let X be the set of all male Canadians and let $x \mathrel{R} y$, where $x \in X$ and $y \in X$, denote the relation "x is a brother of y." The relation R is irreflexive and symmetric but not transitive. In general, any relation which is irreflexive and symmetric cannot be transitive because $x \mathrel{R} y \wedge y \mathrel{R} x \Rightarrow x \mathrel{R} x$, which is not true.

Let X be the collection of the subsets of a universal set. The relation of inclusion in X is reflexive, antisymmetric, and transitive. Also, the relation of proper inclusion in X is irreflexive, antisymmetric, and transitive.

Several important classes of relations having one or more of the properties given here will be discussed later in this section.

EXERCISES 2-3.2

1 Give an example of a relation which is neither reflexive nor irreflexive.

2 Give an example of a relation which is both symmetric and antisymmetric.

3 If relations R and S are both reflexive, show that $R \cup S$ and $R \cap S$ are also reflexive.

4 If relations R and S are reflexive, symmetric, and transitive, show that $R \cap S$ is also reflexive, symmetric, and transitive.

5 Show whether the following relations are transitive:

$$R_1 = \{\langle 1, 1\rangle\} \qquad R_2 = \{\langle 1, 2\rangle, \langle 2, 2\rangle\}$$
$$R_3 = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle\}$$

6 Given $S = \{1, 2, 3, 4\}$ and a relation R on S defined by

$$R = \{\langle 1, 2\rangle, \langle 4, 3\rangle, \langle 2, 2\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle\}$$

show that R is not transitive. Find a relation $R_1 \supseteq R$ such that R_1 is transitive. Can you find another relation $R_2 \supseteq R$ which is also transitive?

7 Given $S = \{1, 2, \ldots, 10\}$ and a relation R on S where

$$R = \{\langle x, y\rangle \mid x + y = 10\}$$

what are the properties of the relation R?

8 Let R be a relation on the set of positive real numbers so that its graphical representation consists of points in the first quadrant of the cartesian plane. What can we expect if R is (*a*) reflexive, (*b*) symmetric, and (*c*) transitive?

9 Show that the relations L and D given in Problem 3 of Exercises 2-3.1 are both reflexive, antisymmetric, and transitive. Give another example of such a relation. Draw the graphs of these relations as defined in Sec. 2-3.3.

2-3.3 Relation Matrix and the Graph of a Relation

A relation R from a finite set X to a finite set Y can also be represented by a matrix called the *relation matrix* of R.

Let $X = \{x_1, x_2, \ldots, x_m\}$, $Y = \{y_1, y_2, \ldots, y_n\}$, and R be a relation from X to Y. The relation matrix of R can be obtained by first constructing a table whose columns are preceded by a column consisting of successive elements of X and whose rows are headed by a row consisting of the successive elements of Y. If $x_i \, R \, y_j$, then we enter a 1 in the ith row and jth column. If $x_k \not R \, x_l$, then we enter a zero in the kth row and lth column. As a special case, consider $m = 3$, $n = 2$, and R given by

$$R = \{\langle x_1, y_1\rangle, \langle x_2, y_1\rangle, \langle x_3, y_2\rangle, \langle x_2, y_2\rangle\} \tag{1}$$

The required table for R is Table 2-3.1.

If we assume that the elements of X and Y appear in a certain order, then the relation R can be represented by a matrix whose elements are 1s and 0s. This matrix can be written down from the table constructed or can be defined in the following manner.

$$r_{ij} = \begin{cases} 1 & \text{if } x_i \, R \, y_j \\ 0 & \text{if } x_i \not R \, y_j \end{cases}$$

where r_{ij} is the element in the ith row and jth column. The matrix obtained in this way is called the relation matrix. If X has m elements and Y has n elements, then the relation matrix is an $m \times n$ matrix. For the relation R given in Eq. (1), the relation matrix is

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Table 2-3.1

	y_1	y_2
x_1	1	0
x_2	1	1
x_3	0	1

One can not only write a relation matrix when a relation R is given but also obtain the relation if the relation matrix is given.

Throughout the remainder of this subsection we shall assume that the relations are defined in a set, say X. A relation matrix reflects some of the properties of a relation in a set. If a relation is reflexive, then all the diagonal entries must be 1. If a relation is symmetric, then the relation matrix is symmetric. If a relation is antisymmetric, then its matrix is such that if $r_{ij} = 1$, then $r_{ji} = 0$ for $i \neq j$.

A relation can also be represented pictorially by drawing its *graph*. Although we shall introduce some of the concepts of graph theory which are discussed in Chap. 5, here we shall use graphs only as a tool to represent relations. Let R be a relation in a set $X = \{x_1, \ldots, x_m\}$. The elements of X are represented by points or circles called *nodes*. The nodes corresponding to x_i and x_j are labeled x_i and x_j respectively. These nodes may also be called vertices. If $x_i \, R \, x_j$, that is, if $\langle x_i, x_j \rangle \in R$, then we connect nodes x_i and x_j by means of an arc and put an arrow on the arc in the direction from x_i to x_j. When all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, we get a graph (directed graph) of the relation R. If $x_i \, R \, x_j$ and $x_j \, R \, x_i$, then we draw two arcs between x_i and x_j. For the sake of simplicity, we may replace the two arcs by one arc with arrows pointing in both directions. If $x_i \, R \, x_i$, we get an arc which starts from node x_i and returns to node x_i. Such an arc is called a *loop*. In Fig. 2-3.4 we show some arcs.

From the graph of a relation it is possible to observe some of its properties. If a relation is reflexive, then there must be a loop at each node. On the other hand, if the relation is irreflexive, then there is no loop at any node. If a relation is symmetric and if one node is connected to another, then there must be a return arc from the second node to the first. For antisymmetric relations no such direct return path should exist (see Fig. 2-3.5). If a relation is transitive, the situation is not so simple. In any case, its graph must have loops of the type shown in Fig. 2-3.6.

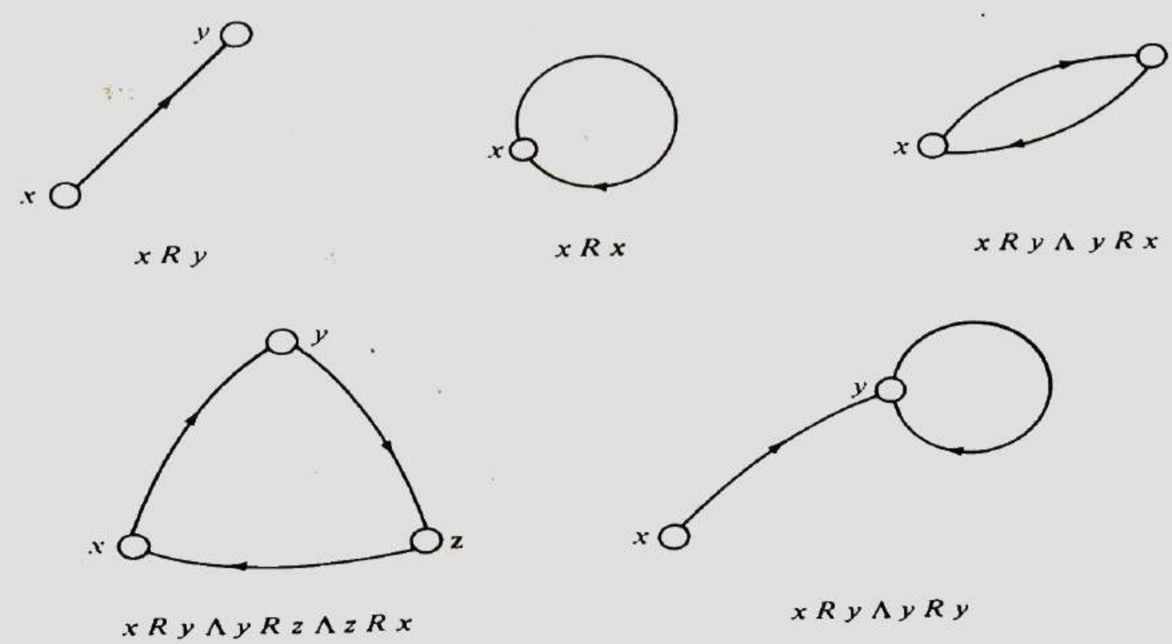


FIGURE 2-3.4 Graphs of relations.

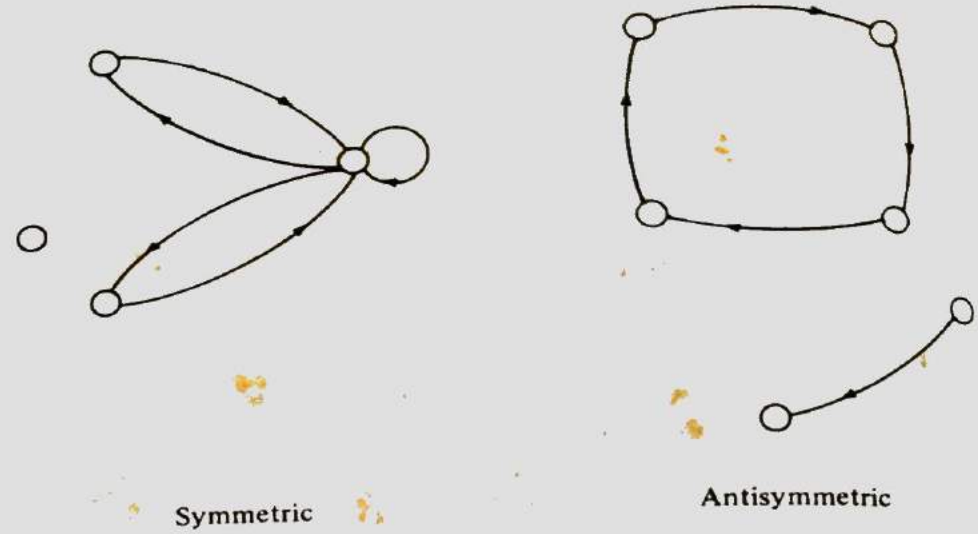


FIGURE 2-3.5 Symmetric and antisymmetric relations.

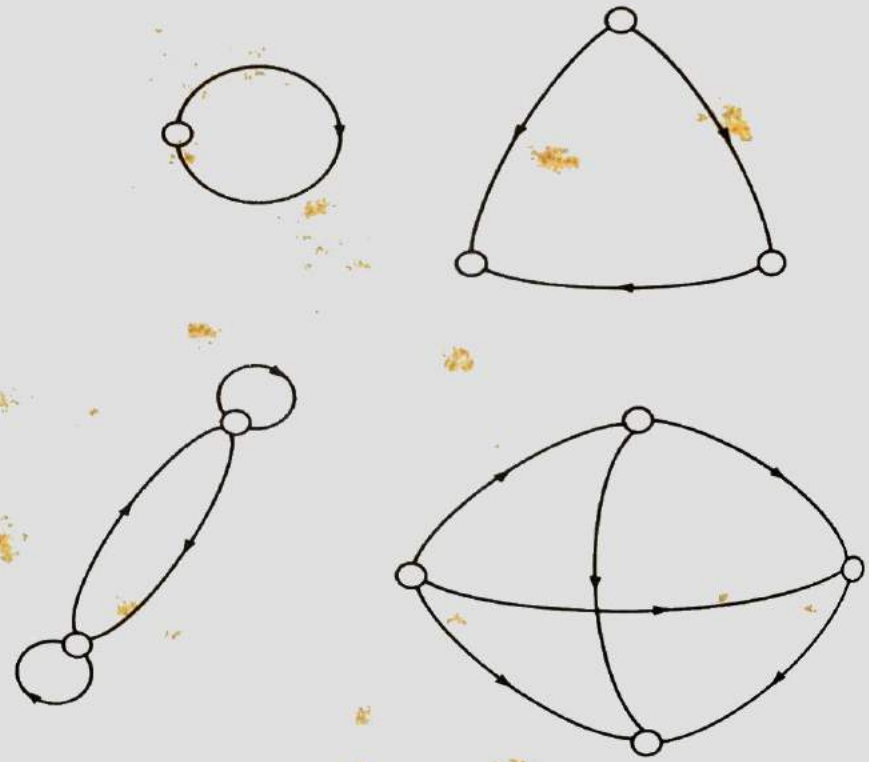
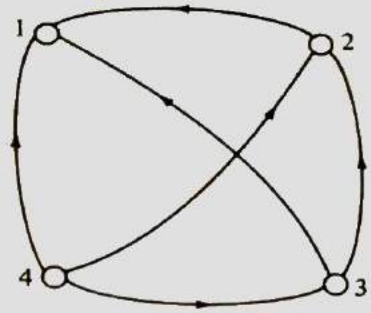


FIGURE 2-3.6 Transitive relations.

EXAMPLE 1 Let $X = \{1, 2, 3, 4\}$ and $R = \{\langle x, y\rangle \mid x > y\}$. Draw the graph of R and also give its matrix.

SOLUTION The graph and the corresponding relation matrix for the relation $R = \{\langle 4, 1\rangle, \langle 4, 2\rangle, \langle 4, 3\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle, \langle 2, 1\rangle\}$ is given in Fig. 2-3.7. ////

EXAMPLE 2 Let $A = \{a, b, c\}$ and denote the subsets of A by $B_0, \ldots, B_7$ according to the convention given in Sec. 2-1.3. Thus $B_0 = \varnothing$, $B_1 = \{c\}$, $B_2 = \{b\}$, $B_3 = \{b, c\}$, $B_4 = \{a\}$, $B_5 = \{a, c\}$, $B_6 = \{a, b\}$, and $B_7 = \{a, b, c\}$. If R is the relation of *proper inclusion* on the subsets $B_0, \ldots, B_7$, then give the matrix of the relation.



$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

FIGURE 2-3.7

SOLUTION

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The relations given in Examples 1 and 2 are both transitive, antisymmetric, and irreflexive. This class of relations will be discussed in Sec. 2-3.8.

EXAMPLE 3 Determine the properties of the relations given by the graphs shown in Fig. 2-3.8, and also write the corresponding relation matrices.

SOLUTION The relation given by the graph in (a) is antisymmetric, in (b) is reflexive, in (c) it is reflexive and symmetric, while in (d) it is transitive. The required matrices are

$$(a)\ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (b)\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (c)\ \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad (d)\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

////

When the number of elements in a set X over which a relation R is defined is large (say greater than or equal to 5 or 6), both the graphical and the matrix

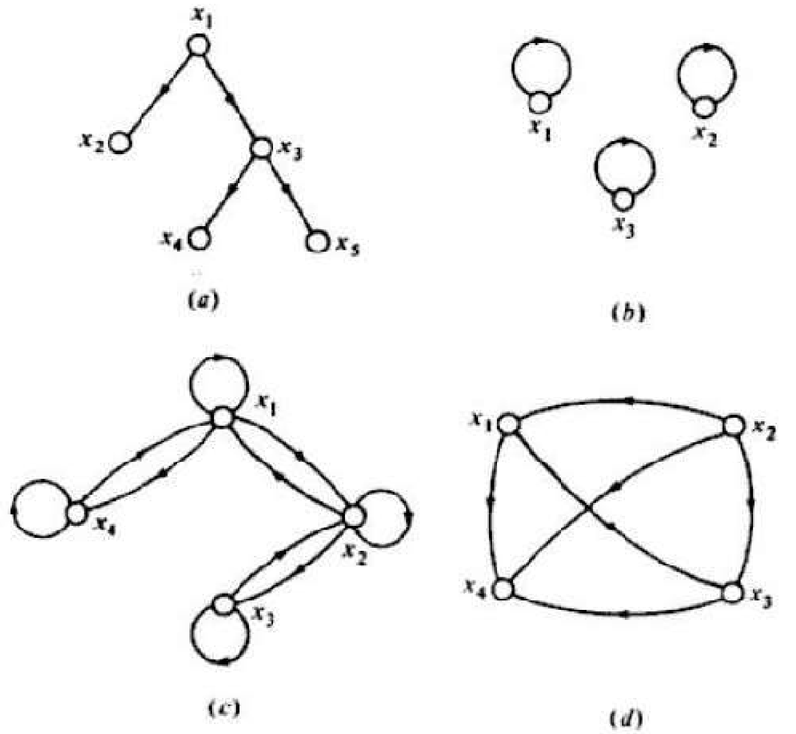


FIGURE 2-3.8

representations of the relation become unwieldy. In these cases, however, the matrix representation can be easily represented on a computer. When a relation matrix is available, it is easy to determine whether a given relation is reflexive or symmetric. It is not always easy to determine from the matrix whether the relation is transitive. We now present two algorithms. The first determines from a relation matrix whether the relation is reflexive and symmetric. The second algorithm then determines whether the relation is also transitive. Relations which are reflexive, symmetric, and transitive are called *equivalence relations*. Equivalence relations are discussed in Sec. 2-3.5.

The entries of the relation matrix are denoted by T and F instead of 1 and 0 in order to conserve storage. Note that in FORTRAN only 1 byte is needed for each logical entry, but at least 2 bytes are required for an integer entry.

Algorithm *REFSYM* Given a relation matrix R representing a relation in the set of positive integers from 1 to n inclusive, it is required to determine if the relation represented by R is symmetric and reflexive. If it is, the variable *FLAG* which is initially *false* is given the truth value *true*; otherwise *FLAG* remains *false*.

1 [Scan each row.] Repeat steps 2 and 3 for $i = 1, 2, \ldots, n$.
2 [Reflexive?] If $R[i, i] = F$ then Exit.
3 [Symmetric?] Repeat for $j = i + 1, i + 2, \ldots, n$:
If $R[i, j] \rightleftarrows R[j, i] = F$ then Exit.
4 [Successful test.] Set $FLAG \leftarrow T$ and Exit.

This algorithm scans each row of the matrix from the diagonal element to the right. If a diagonal element has the truth value F, then the algorithm is terminated in step 2 with *FLAG* remaining *false*. Step 3 scans each row in the

Then the set A is called a *covering* of S, and the sets $A_1, A_2, \ldots, A_m$ are said to *cover* S. If, in addition, the elements of A, which are subsets of S, are mutually disjoint, then A is called a *partition* of S, and the sets $A_1, A_2, \ldots, A_m$ are called the *blocks* of the partition.

For example, let $S = \{a, b, c\}$ and consider the following collections of subsets of S.

$$A = \{\{a, b\}, \{b, c\}\} \qquad B = \{\{a\}, \{a, c\}\} \qquad C = \{\{a\}, \{b, c\}\}$$
$$D = \{\{a, b, c\}\} \qquad E = \{\{a\}, \{b\}, \{c\}\} \qquad F = \{\{a\}, \{a, b\}, \{a, c\}\}$$

The sets A and F are coverings of S while C, D, and E are partitions of S. Of course, every partition is also a covering. The set B is neither a partition nor a covering of S. The partition D has only one block while E has three. In the case of the given set S, we cannot have more than three blocks in any partition. In fact, for any finite set, the smallest partition consists of the set itself as a block while the largest partition consists of blocks containing only single elements.

Two partitions are said to be equal if they are equal as sets. For a finite set, every partition is a finite partition, i.e., every partition contains only a finite number of blocks.

It will be shown in Sec. 2-3.5 that an equivalence relation on a set partitions the set. Another relation on a set known as a compatibility relation as described in Sec. 2-3.6 defines certain coverings of the set.

Now we discuss some partitions of the universal set E which are generated by the subsets of E. Let us first consider a subset A of E. The subsets A and $\sim A$ generate a partition of E (see Fig. 2-3.11a) since

$$E = A \cup \sim A$$

Next let A and B be any two subsets of E, and consider the sets

$$I_0 = \sim A \cap \sim B \qquad I_1 = \sim A \cap B \qquad I_2 = A \cap \sim B \qquad \text{and} \qquad I_3 = A \cap B$$

The sets I_0, I_1, I_2, and I_3 are called the complete intersections or the *minterms* generated by the subsets A and B. It is easy to see that I_0, I_1, I_2, and I_3 are mutually disjoint and

$$E = I_0 \cup I_1 \cup I_2 \cup I_3 = \bigcup_{j=0}^{3} I_j$$

The complete intersections or the minterms are the blocks of a partition of E generated by A and B (see Fig. 2-3.11b).

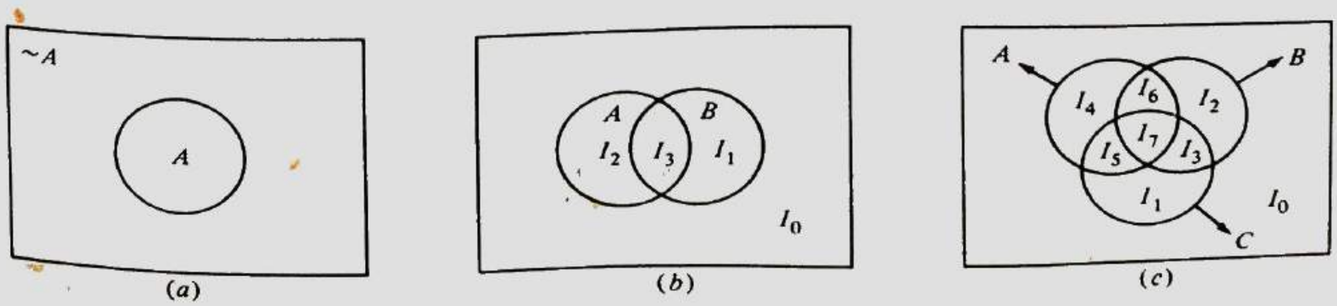


FIGURE 2-3.11 Complete intersections.

Let A, B, and C be three subsets of E and let the 2^3 minterms, denoted by $I_0, I_1, \ldots, I_7$ (see Fig. 2-3.11c), be as follows:

$$I_0 = \sim A \cap \sim B \cap \sim C \qquad I_1 = \sim A \cap \sim B \cap C$$
$$I_2 = \sim A \cap B \cap \sim C \qquad I_3 = \sim A \cap B \cap C$$
$$I_4 = A \cap \sim B \cap \sim C \qquad I_5 = A \cap \sim B \cap C$$
$$I_6 = A \cap B \cap \sim C \qquad I_7 = A \cap B \cap C$$

The subscript of I shows indirectly the minterm under consideration. In order to obtain the minterm, first we write the subscript as a binary integer containing three digits (since there are three subsets under consideration). The appearance of 1 or 0 in the first position on the left indicates the presence of A or $\sim A$, respectively. This relation also holds for the second and third positions. The notation is similar to the one used in Secs. 1-3.5 and 2-1.3. For example, $I_5 = A \cap \sim B \cap C$ since 5 written as a binary integer is 101.

In general, if $A_1, A_2, \ldots, A_n$ are any n subsets of the universal set E, then the complete intersections or minterms generated by these n subsets are denoted by $I_0, I_1, \ldots, I_{2^n-1}$ (see Sec. 2-1.3). These are mutually disjoint and are such that

$$E = \bigcup_{j=0}^{2^n-1} I_j$$

One can recognize a similarity between the minterms defined here and those given in the statement calculus. We shall return to a general discussion of this in Chap. 4.

EXERCISES 2-3.4

1 Define a well-formed formula of set theory in the same manner as in the definition given in Sec. 1-2.7, using the operators $\cap$, $\cup$, and $\sim$ only.

2 Show that for any formula in set theory involving set variables A and B and the operations $\cap$, $\cup$, and $\sim$, one can obtain another formula which is equal to the given formula and which contains the union of minterms only.

3 Show that the set of operations $\{\cup, \sim\}$ is functionally complete for formulas in set theory (*Hint*: Follow the same procedure used in Sec. 1-2.13).

4 Write the duals of minterms and discuss some of their important properties.

2-3.5 Equivalence Relations

Definition 2-3.9 A relation R in a set X is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

If R is an equivalence relation in a set X, then $D(R)$, the domain of R, is X itself. Therefore R will be called a relation on X. The following are some examples of equivalence relations.

1 Equality of numbers on a set of real numbers

2 Equality of subsets of a universal set

3 Similarity of triangles on the set of triangles
4 Relation of lines being parallel on a set of lines in a plane
5 Relation of living in the same town on the set of persons living in Canada
6 Relation of statements being equivalent in the set of statements

EXAMPLE 1 Let $X = \{1, 2, 3, 4\}$ and

$$R = \{\langle 1, 1\rangle, \langle 1, 4\rangle, \langle 4, 1\rangle, \langle 4, 4\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$$

Write the matrix of R and sketch its graph.

SOLUTION The matrix and the graph of R are given in Fig. 2-3.12. It is clear that R is an equivalence relation. ////

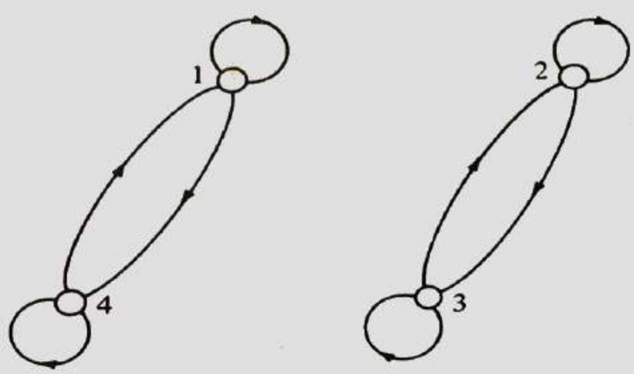
EXAMPLE 2 Let $X = \{1, 2, \ldots, 7\}$ and

$$R = \{\langle x, y\rangle \mid x - y \text{ is divisible by } 3\}$$

Show that R is an equivalence relation. Draw the graph of R.

SOLUTION See Fig. 2-3.13. One can see from the figure that R is an equivalence relation. It is possible to prove this statement without using the graph of the relation in the following manner:

1 For any $a \in X$, $a - a$ is divisible by 3; hence $a\ R\ a$, or R is reflexive.
2 For any $a, b \in X$, if $a - b$ is divisible by 3, then $b - a$ is also divisible by 3; that is, $a\ R\ b \Rightarrow b\ R\ a$. Thus R is symmetric.



$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

FIGURE 2-3.12 An equivalence relation

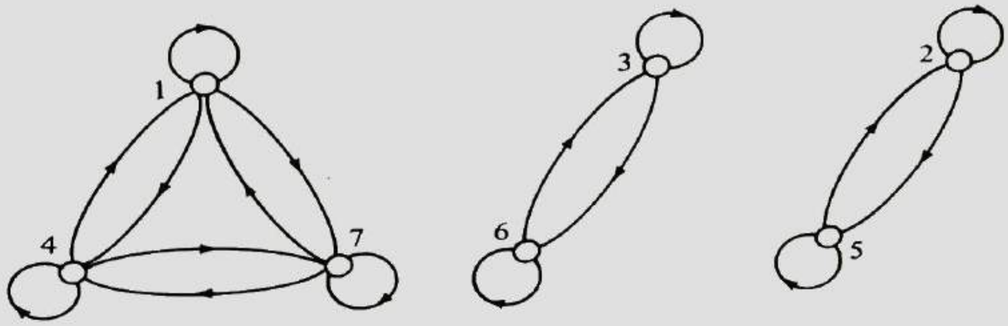


FIGURE 2-3.13

3 For $a, b, c \in X$, if $a\,R\,b$ and $b\,R\,c$, then both $a - b$ and $b - c$ are divisible by 3, so that $a - c = (a - b) + (b - c)$ is also divisible by 3, and hence $a\,R\,c$. Thus R is transitive. ////

Example 2 is a special case of a more general relation of equality in the modular number system. Let I denote the set of all positive integers, and let m be a positive integer. For $x \in I$ and $y \in I$, define R as

$$R = \{\langle x, y\rangle \mid x - y \text{ is divisible by } m\}$$

Note that "$x - y$ is divisible by m" is equivalent to the statement that both x and y have the same remainder when each is divided by m. It is customary to denote R by $\equiv$ and to write $x\,R\,y$ as $x \equiv y\ (m)$ or $x \equiv y \pmod{m}$, which is read as "x equals y modulo m." The relation $\equiv$ is also called a *congruence relation*. We define congruence relations in Sec. 3-1.2.

Definition 2-3.10 Let R be an equivalence relation on a set X. For any $x \in X$, the set $[x]_R \subseteq X$ given by

$$[x]_R = \{y \mid y \in X \wedge x\,R\,y\}$$

is called an *R-equivalence class* generated by $x \in X$.

Accordingly, the set $[x]_R$ consists of all the R-relatives of x in the set X. Sometimes $[x]_R$ is also written as x/R. We shall now study some properties of the equivalence classes generated by the elements of X.

1 For any element $x \in X$, we have $x\,R\,x$ because R is reflexive; therefore $x \in [x]_R$.

2 Let $y \in X$ be any other element such that $x\,R\,y$, so that $y \in [x]_R$. Because of the symmetry of R, $y\,R\,x$ and $x \in [y]_R$. Now, if there is an element $z \in [y]_R$, then z must be in $[x]_R$ because $y\,R\,z$, along with $x\,R\,y$, implies $x\,R\,z$. Thus $[y]_R \subseteq [x]_R$. By symmetry we must also have $[x]_R \subseteq [y]_R$. Finally, from $[y]_R \subseteq [x]_R$ and $[x]_R \subseteq [y]_R$, we have $[x]_R = [y]_R$.

3 In step 2 it is shown that if $x\,R\,y$, then $[x]_R = [y]_R$. We now show that if $x \not R\, y$, then $[x]_R$ and $[y]_R$ must be disjoint. This demonstration can be done by assuming that there is at least one element $z \in [x]_R$ and also $z \in [y]_R$; that is, $x\,R\,z$ and $y\,R\,z$, but this would imply $z\,R\,y$, and then from transitivity, $x\,R\,y$, which is a contradiction.

The above result shows that the R-equivalence class generated by any element $y \in X$ is equal to the R-equivalence class generated by $x \in X$ provided that $y \in [x]_R$. Otherwise the R-equivalence classes generated by x and y are disjoint. Further, each element of X generates an R-equivalence class which is nonempty. Therefore the R-equivalence classes generated by the elements of X cover X, that is, their union is the set X. Since the R-equivalence classes generated by any two elements are either equal or disjoint, we can say that the family of R-equivalence classes generated by the elements of X defines a partition of X. Such a partition is unique because an R-equivalence class of any element of X is unique. We now formulate this idea as a theorem.

Theorem 2-3.1 Every equivalence relation on a set generates a unique partition of the set. The blocks of this partition correspond to the R-equivalence classes.

As we have denoted the R-equivalence class generated by an element $x \in X$ by $[x]_R$, or x/R, we shall denote the family of equivalence classes by X/R, which is also written as X modulo R, or in short as X mod R. X/R is called the *quotient set* of X by R. Note that the elements of X/R are the equivalence classes which are themselves sets. They are, in fact, subsets of X or elements of the power set $\rho(X)$.

We consider now two special equivalence relations on a set X. The first such relation is $R_1 = X \times X$, and every element of X is in R_1-relation to all the elements of X. In this case the quotient set of X by R_1 is the set $\{X\}$. The other relation R_2 is such that every element of X is related to itself and to no other element. Such a relation is called an *identity relation*. An identity relation is an equivalence relation, and the quotient set of X by R_2 consists of sets which each contain a single element. Thus R_2 generates the largest partition of X.

EXAMPLE 3 Let $\mathbf{Z}$ be the set of integers and let R be the relation called "congruence modulo 3" defined by

$$R = \{\langle x, y\rangle \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z} \wedge (x - y) \text{ is divisible by } 3\}$$

Determine the equivalence classes generated by the elements of $\mathbf{Z}$.

SOLUTION The equivalence classes are

$$[0]_R = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1]_R = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2]_R = \{\ldots, -4, -1, 2, 5, 8 \ \ldots\}$$
$$\mathbf{Z}/R = \{[0]_R, [1]_R, [2]_R\}$$

////

In a similar manner one can find the equivalence classes generated by a relation "congruence modulo m" for any integer m.

EXAMPLE 4 Let S be the set of all statement functions in n variables and let R be the relation given by

$$R = \{\langle x \ \ y\rangle \mid x \in S \wedge y \in S \wedge x \Leftrightarrow y\}$$

Discuss the equivalence classes generated by the elements of S.

SOLUTION The number of possible distinct truth tables for statement functions which depend upon n statement variables is 2^{2^n} (see Sec. 1-2.12). Thus there are 2^{2^n} R-equivalence classes generated by the elements of S. ////

So far we have considered the partition of a set generated by an equivalence relation. Now we shall show that the converse of Theorem 2-3.1 also holds, i.e., if we start with a definite partition, say C, of a given set X, then we can define an equivalence relation which corresponds to this partition. For any $x \in X$, there is a set $C_1 \in C$ such that $x \in C_1$; also x does not belong to any other element of C. We now take all the elements of $C_1 \times C_1$ as members of a relation R. Thus every element of X that is in C_1 is an R-relative of every other member of C_1. Furthermore, no other member of X which is not in C_1 is related to the elements of C_1. Similarly, for every other member of the partition C, we form members of the relation R. If $C = \{C_1, C_2, C_3, \ldots, C_m\}$, then $R = (C_1 \times C_1) \cup (C_2 \times C_2) \cup \cdots \cup (C_m \times C_m)$. It is easy to see that R is an equivalence relation. Thus for every partition C we can define an equivalence relation.

EXAMPLE 5 Let $X = \{a, b, c, d, e\}$ and let $C = \{\{a, b\}, \{c\}, \{d, e\}\}$. Show that the partition C defines an equivalence relation on X.

SOLUTION

$R = \{\langle a, a\rangle, \langle b, b\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle c, c\rangle, \langle d, d\rangle, \langle e, e\rangle, \langle d, e\rangle, \langle e, d\rangle\}$ ////

It has been shown that an equivalence relation on a set generates a partition of the set, and conversely. It may happen that two relations, which may have been defined in different ways, generate the same partition. Since a relation is a set, any two relations consisting of equal sets are indistinguishable for our purpose. This statement will be true of every partition of the set as well. The following serves as an illustration.

Let $X = \{1, 2, \ldots, 9\}$ and $R_1 = \{\langle x, y\rangle \mid x \in X \wedge y \in X \wedge (x - y)$ is divisible by $3\}$. Further, let

$R_2 = \{\langle x, y\rangle \mid x \in X \wedge y \in X$ and x, y are in same column of matrix A$\}$

where

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Although R_1 and R_2 have been defined differently, $R_1 = R_2$.

In Sec. 2-3.3 we have already given algorithms to determine whether a given relation R on a set is an equivalence relation. Once it is determined, our next task is to obtain the equivalence classes. Before giving an algorithm for this purpose, let us discuss the technique that will be used for the representation of the equivalence classes in the algorithm.

Given a set $\{1, 2, \ldots, n\}$ and an equivalence relation R on it, the equivalence classes can be represented by means of two vectors, each having n elements. These vectors are called *FIRST* and *MEMBER*. The ith component of *FIRST* for $1 \leq i \leq n$ contains the number which is the first element in the equivalence class to which i belongs. The ith component of *MEMBER* contains the number which follows i in the equivalence class, unless i is the last element, in which case $MEMBER[i]$ is equal to zero.

As an example, let the set be $\{1, 2, 3, 4, 5, 6\}$ and the equivalence classes be $\{1, 3, 6\}$, $\{2\}$, and $\{4, 5\}$. The vectors *FIRST* and *MEMBER* representing these equivalence classes are shown in Fig. 2-3.14.

RELATION MATRIX

	1	2	3	4	5	6	7	8	9	10
1	T	T	F	F	F	F	F	T	F	F
2	T	T	F	F	F	F	F	T	F	F
3	F	F	T	F	F	F	F	F	F	F
4	F	F	F	T	F	T	T	F	F	F
5	F	F	F	F	T	F	F	F	F	F
6	F	F	F	T	F	T	T	F	F	F
7	F	F	F	T	F	T	T	F	F	F
8	T	T	F	F	F	F	F	T	F	F
9	F	F	F	F	F	F	F	F	T	F
10	F	F	F	F	F	F	F	F	F	T

THE RELATION IS AN EQUIVALENCE RELATION.

EQUIVALENCE CLASSES

1 2 8

3

4 6 7

5

9

10

FIRST	1	1	3	4	5	4	4	1	9	10
MEMBER	2	8	0	6	0	7	0	0	0	0

FIGURE 2-3.16*b*.

Then R is a compatibility relation, and x, y are called compatible if $x\ R\ y$. A compatibility relation is sometimes denoted by $\approx$. Note that ball $\approx$ bed, bed $\approx$ egg, but ball $\not\approx$ egg. Thus $\approx$ is not transitive. Denoting "ball" by x_1, "bed" by x_2, "dog" by x_3, "let" by x_4, and "egg" by x_5, the graph of $\approx$ is given in Fig. 2-3.17*a*.

Since $\approx$ is a compatibility relation, it is not necessary to draw the loops at each element nor is it necessary to draw both $x\ R\ y$ and $y\ R\ x$. Thus we can simplify the graph of $\approx$, as shown in Fig. 2-3.17*b*. Note that the elements in each of the sets $\{x_1, x_2, x_4\}$ and $\{x_2, x_3, x_5\}$ are related to each other, i.e., the elements are mutually compatible. Further, these two sets define a covering of X. The set $\{x_2, x_4, x_5\}$ also has elements compatible to each other.

The relation matrix of a compatibility relation is symmetric and has its diagonal elements unity. It is, therefore, sufficient to give only the elements of the lower triangular part of the relation matrix in such a case. For the compatibility relation we have been discussing, the relation matrix can be obtained from Table 2-3.2.

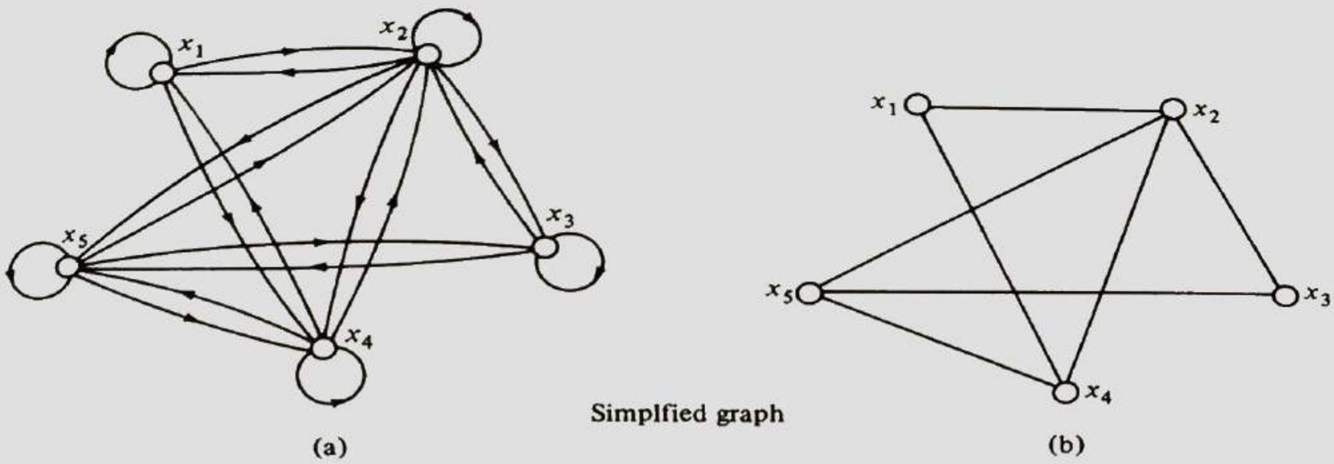


FIGURE 2-3.17 Graphs of compatibility relation $\approx$.

Although an equivalence relation on a set defines a partition of the set into equivalence classes, a compatibility relation does not necessarily define a partition. However, a compatibility relation does define a covering of the set.

Definition 2-3.12 Let X be a set and $\approx$ a compatibility relation on X. A subset $A \subseteq X$ is called a *maximal compatibility block* if any element of A is compatible to every other element of A and no element of $X - A$ is compatible to all the elements of A.

It is clear from Fig. 2-3.17b that the subset $\{x_1, x_2, x_4\}$ is a maximal compatibility block; so, too, are the subsets $\{x_2, x_3, x_5\}$ and $\{x_2, x_4, x_5\}$. These sets are not mutually disjoint, and therefore they only define a covering of X.

To find the maximal compatibility blocks corresponding to a compatibility relation on a set X, first we draw a simplified graph of the compatibility relation and pick from this graph the largest complete polygons. By a "largest complete polygon" we mean a polygon in which any vertex is connected to every other vertex. For example, a triangle is always a complete polygon, but for a quadrilateral to be a complete polygon we must have the two diagonals present. In addition to these examples, any element of the set which is related only to itself forms a maximal compatibility block. Similarly, any two elements which are compatible to one another but to no other elements also form a maximal compatibility block. We now give some graphs of compatibility relations, the corresponding relation matrices, and the maximal compatibility blocks.

The maximal compatibility blocks of the relations shown in Figs. 2-3.18

Table 2-3.2

x_2	1			
x_3	0	1		
x_4	1	1	0	
x_5	0	1	1	1
	x_1	x_2	x_3	x_4

2	0			
3	1	1		
4	1	0	1	
5	0	1	0	1
	1	2	3	4

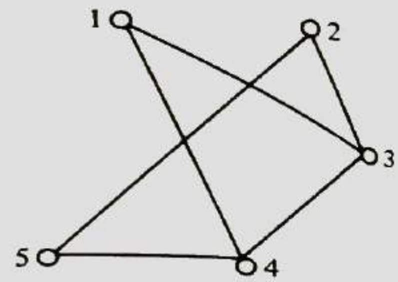


FIGURE 2-3.18

2	1				
3	1	1			
4	1	1	1		
5	0	1	0	0	
6	0	0	1	0	1
	1	2	3	4	5

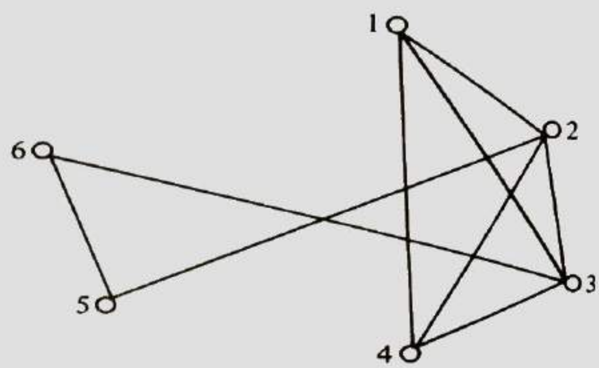


FIGURE 2-3.19

2	1			
3	1	1		
5	0	0	1	
6	1	0	1	1
	1	2	3	5

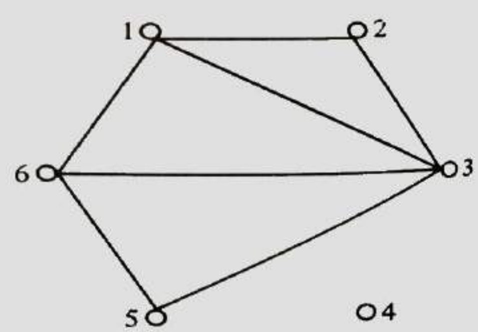


FIGURE 2-3.20

to 2-3.20 are given by

$\{1, 3, 4\} \quad \{2, 3\} \quad \{4, 5\} \quad \{2, 5\}$

$\{1, 2, 3, 4\} \quad \{2, 5\} \quad \{3, 6\} \quad \{5, 6\}$

and

$\{1, 2, 3\} \quad \{1, 3, 6\} \quad \{3, 5, 6\} \quad \{4\}$

respectively. For the compatibility relation of the example discussed earlier and given in Fig. 2-3.17, the maximal compatibility blocks are $\{x_1, x_2, x_4\}$, $\{x_2, x_3, x_5\}$, and $\{x_2, x_4, x_5\}$.

Another procedure for finding the maximal compatibility blocks from the table of the relation matrix can be described in the following manner. It is assumed that first a simplified table is obtained in which those elements which are only compatible to themselves are deleted, because they are in a maximal compatibility block by themselves and are in no other compatibility block. Such blocks are included in the list at the end (see Fig. 2-3.20).

1 Start in the rightmost column of the table and proceed to the left until a column containing at least one nonzero entry is encountered. List all the compatible pairs represented by the entries in that column.

2 Proceed left to the next column that contains at least one nonzero entry. If any element is compatible to all the members of some previously defined compatibility class, then add this element to that class. If a member is compatible to only some members of a previously defined class, then form a new class which includes all the members that are compatible. Next, list all the compatible pairs not included in any previously defined class.

3 Repeat step 2 until all the columns are considered.

The final sets of compatibility classes including those which are isolated elements constitute the maximal compatibility classes.

Compatibility relations are useful in solving certain minimization problems of switching theory, particularly for incompletely specified minimization problems.

EXERCISES 2-3.6

1 Let R denote a relation on the set of ordered pairs of positive integers such that $\langle x, y\rangle \; R \; \langle u, v\rangle$ iff $xv = yu$. Show that R is an equivalence relation.

2 Given a set $S = \{1, 2, 3, 4, 5\}$, find the equivalence relation on S which generates the partition $\{\overline{1, 2}, \overline{3}, \overline{4, 5}\}$. Draw the graph of the relation.

3 Prove that the relation "congruence modulo m" given by

$$\equiv \; = \{\langle x, y\rangle \mid x - y \text{ is divisible by } m\}$$

over the set of positive integers is an equivalence relation. Show also that if $x_1 \equiv y_1$ and $x_2 \equiv y_2$, then $(x_1 + x_2) \equiv (y_1 + y_2)$.

4 Given a covering of the set $S = \{A_1, A_2, \ldots, A_n\}$, show how we can write a compatibility relation which defines this covering.

5 Let the compatibility relation on a set $\{x_1, x_2, \ldots, x_6\}$ be given by the matrix

x_2	1				
x_3	1	1			
x_4	0	0	1		
x_5	0	0	1	1	
x_6	1	0	1	0	1
	x_1	x_2	x_3	x_4	x_5

Draw the graph and find the maximal compatibility blocks of the relation.

2-3.7 Composition of Binary Relations

Since a binary relation is a set of ordered pairs, the usual operations such as union, intersection, etc., on these sets produce other relations. This topic was discussed in Sec. 2-3.1. We shall now consider another operation on relations—relations which are formed in two or more stages. Familiar examples of such relations are the relation of being a nephew or a brother's or sister's son, the relation of an uncle or a father's or mother's brother, and the relation of being a grandfather which is a father's or mother's father. These relations can be produced in the following manner.

> **Definition 2-3.13** Let R be a relation from X to Y and S be a relation from Y to Z. Then a relation written as $R \circ S$ is called a *composite relation* of R and S where
>
> $$R \circ S = \{\langle x, z\rangle \mid x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge \langle x, y\rangle \in R \wedge \langle y, z\rangle \in S\}$$
>
> The operation of obtaining $R \circ S$ from R and S is called *composition* of relations.

Note that $R \circ S$ is empty if the intersection of the range of R and the domain of S is empty. $R \circ S$ is nonempty if there is at least one ordered pair $\langle x, y\rangle \in R$ such that the second member $y \in Y$ of the ordered pair is a first member in an ordered pair in S. For the relation $R \circ S$, the domain is a subset of X and the range is a subset of Z. In fact, the domain is a subset of the domain of R, and its range is a subset of the range of S. From the graphs of R and S one can easily construct the graph of $R \circ S$. As an example, see Fig. 2-3.21.

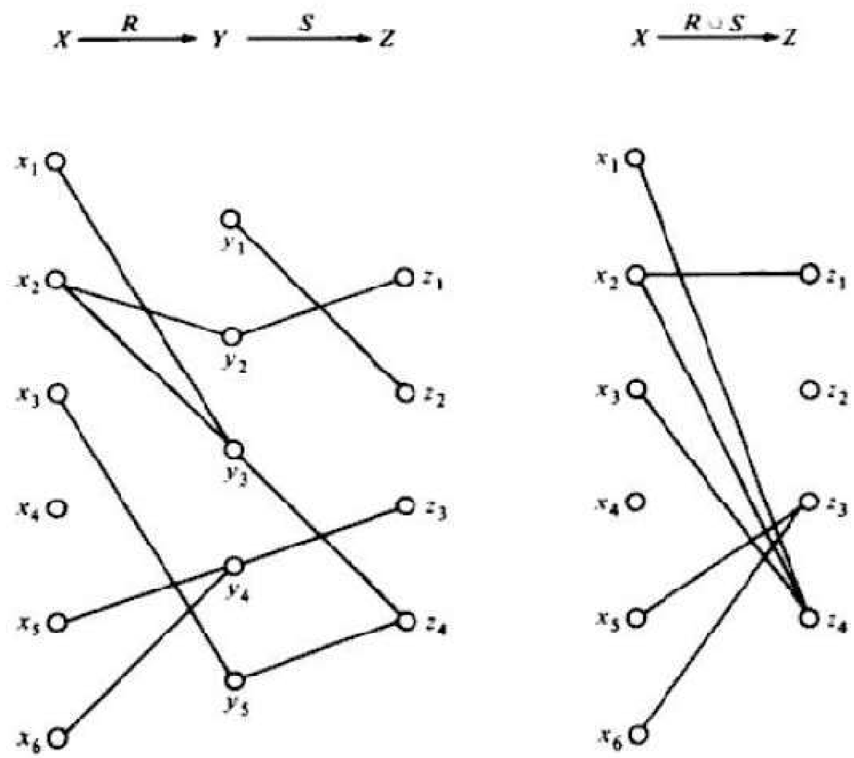


FIGURE 2-3.21 Relations R, S, and $R \circ S$.

The operation of composition is a binary operation on relations, and it produces a relation from two relations. The same operations can be applied again to produce other relations. For example, let R be a relation from X to Y, S a relation from Y to Z, and P a relation from Z to W. Then $R \circ S$ is a relation from X to Z. We can form $(R \circ S) \circ P$, which is a relation from X to W. Similarly, we can also form $R \circ (S \circ P)$, which again is a relation from X to W.

Let us assume that $(R \circ S) \circ P$ is nonempty, and let $\langle x, y \rangle \in R$, $\langle y, z \rangle \in S$, and $\langle z, w \rangle \in P$. This assumption means $\langle x, z \rangle \in R \circ S$ and $\langle x, w \rangle \in (R \circ S) \circ P$. Of course, $\langle y, w \rangle \in S \circ P$ and $\langle x, w \rangle \in R \circ (S \circ P)$, which shows that

$$(R \circ S) \circ P = R \circ (S \circ P)$$

This result can be stated by saying that the operation of composition on relations is associative. We may delete the parentheses in writing $(R \circ S) \circ P$, so that

$$(R \circ S) \circ P = R \circ (S \circ P) = R \circ S \circ P$$

The same result follows from the partial graph given in Fig. 2-3.22.

EXAMPLE 1 Let $R = \{\langle 1, 2 \rangle, \langle 3, 4 \rangle, \langle 2, 2 \rangle\}$ and $S = \{\langle 4, 2 \rangle, \langle 2, 5 \rangle, \langle 3, 1 \rangle, \langle 1, 3 \rangle\}$. Find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$, and $R \circ R \circ R$.

SOLUTION

$$\begin{aligned}
R \circ S &= \{\langle 1, 5 \rangle, \langle 3, 2 \rangle, \langle 2, 5 \rangle\} \\
S \circ R &= \{\langle 4, 2 \rangle, \langle 3, 2 \rangle, \langle 1, 4 \rangle\} \neq R \circ S \\
(R \circ S) \circ R &= \{\langle 3, 2 \rangle\} \\
R \circ (S \circ R) &= \{\langle 3, 2 \rangle\} = (R \circ S) \circ R \\
R \circ R &= \{\langle 1, 2 \rangle, \langle 2, 2 \rangle\} \\
S \circ S &= \{\langle 4, 5 \rangle, \langle 3, 3 \rangle, \langle 1, 1 \rangle\} \\
R \circ R \circ R &= \{\langle 1, 2 \rangle, \langle 2, 2 \rangle\}
\end{aligned}$$

////

EXAMPLE 2 Let R and S be two relations on a set of positive integers $\mathbf{I}$:

$$R = \{\langle x, 2x \rangle \mid x \in \mathbf{I}\} \qquad S = \{\langle x, 7x \rangle \mid x \in \mathbf{I}\}$$

Find $R \circ S$, $R \circ R$, $R \circ R \circ R$, and $R \circ S \circ R$.

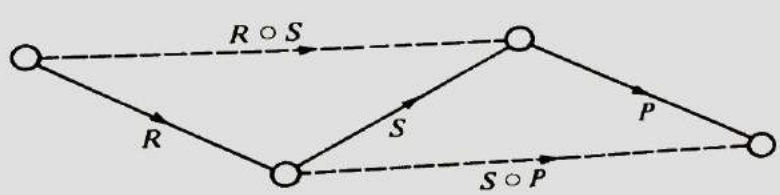


FIGURE 2-3.22 Associativity of composition.

SOLUTION

$$R \circ S = \{\langle x, 14x\rangle \mid x \in \mathbf{I}\} = S \circ R$$
$$R \circ R = \{\langle x, 4x\rangle \mid x \in \mathbf{I}\}$$
$$R \circ R \circ R = \{\langle x, 8x\rangle \mid x \in \mathbf{I}\}$$
$$R \circ S \circ R = \{\langle x, 28x\rangle \mid x \in \mathbf{I}\}$$

////

We know that the relation matrix of a relation R from a set $X = \{x_1, x_2, \ldots, x_m\}$ to a set $Y = \{y_1, y_2, \ldots, y_n\}$ is given by a matrix having m rows and n columns. We shall denote the relation matrix of R by M_R. M_R has entries which are 1s and 0s. Similarly the relation matrix M_S of a relation S from the set Y to a set $Z = \{z_1, z_2, \ldots, z_p\}$ is an $n \times p$ matrix. The relation matrix of $R \circ S$ can be obtained from the matrices M_R and M_S in the following manner.

From the definition it is clear that $\langle x_i, z_k\rangle \in R \circ S$ if there is at least one element of Y, say y_j, such that $\langle x_i, y_j\rangle \in R$ and $\langle y_j, z_k\rangle \in S$. There may be more than one element of Y which has properties similar to those of y_j; for example, $\langle x_i, y_r\rangle \in R$ and $\langle y_r, z_k\rangle \in S$. In all such cases, $\langle x_i, z_k\rangle \in R \circ S$. Thus when we scan the ith row of M_R and kth column of M_S and we come across at least one j, such that the entries in the jth location of the row as well as the column under consideration are 1s, then the entry in the ith row and kth column of $M_{R\circ S}$ is also 1; otherwise it is 0. Scanning a row of M_R along with every column of M_S gives one row of $M_{R\circ S}$. Similarly, we can obtain all the other rows.

EXAMPLE 3 For the relations R and S given in Example 1 over the set $\{1, 2, \ldots, 5\}$, obtain the relation matrices for $R \circ S$ and $S \circ R$.

SOLUTION

$$\underset{M_R}{\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} \circ \underset{M_S}{\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{M_{R\circ S}}{\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

$$\underset{M_S}{\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} \circ \underset{M_R}{\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{M_{S\circ R}}{\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

In general, let the relations A and B be represented by $n \times m$ and $m \times r$ matrices respectively. Then the composition $A \circ B$ which we denote by the relation matrix C is expressed as

$$c_{ij} = \bigvee_{k=1}^{m} a_{ik} \wedge b_{kj} \qquad i = 1, 2, \ldots, n; j = 1, 2, \ldots, r$$

where $a_{ik} \wedge b_{kj}$ and $\bigvee_{k=1}^{m}$ indicate bit-ANDing and bit-ORing respectively (see Sec. 2-2.5).

Definition 2-3.14 Given a relation R from X to Y, a relation $\tilde{R}$ from Y to X is called the *converse* of R, where the ordered pairs of $\tilde{R}$ are obtained by interchanging the members in each of the ordered pairs of R. This means, for $x \in X$ and $y \in Y$, that $x\ R\ y \Leftrightarrow y\ \tilde{R}\ x$.

From the definition of $\tilde{R}$ it follows that $\tilde{\tilde{R}} = R$. The relation matrix $M_{\tilde{R}}$ of $\tilde{R}$ can be obtained by simply interchanging the rows and columns of M_R. Such a matrix is called the *transpose* of M_R. Therefore

$$M_{\tilde{R}} = \text{transpose of } M_R$$

The graph of $\tilde{R}$ is also obtained from that of R by simply reversing the arrows on each arc.

We shall now consider the converse of a composite relation. For this purpose, let R be a relation from X to Y and S be a relation from Y to Z. Obviously, $\tilde{R}$ is a relation from Y to X, $\tilde{S}$ from Z to Y; $R \circ S$ is a relation from X to Z, and $R \mathbin{\tilde{\circ}} S$ is a relation from Z to X. Also the relation $\tilde{S} \circ \tilde{R}$ is from Z to X. We now show that

$$R \mathbin{\tilde{\circ}} S = \tilde{S} \circ \tilde{R}$$

If $x\ R\ y$ and $y\ S\ z$, then $x\ (R \circ S)\ z$ and $z\ (R \mathbin{\tilde{\circ}} S)\ x$. But $z\ \tilde{S}\ y$ and $y\ \tilde{R}\ x$, so that $z\ (\tilde{S} \circ \tilde{R})\ x$. This is true for any $x \in X$ and $z \in Z$; hence the required result.

The same rule can be expressed in terms of the relation matrices by saying that the transpose of $M_{R \circ S}$ is the same as the matrix $M_{\tilde{S} \circ \tilde{R}}$. The matrix $M_{\tilde{S} \circ \tilde{R}}$ can be obtained from the matrices $M_{\tilde{S}}$ and $M_{\tilde{R}}$, which in turn can be obtained from the matrices M_S and M_R.

EXAMPLE 4 Given the relation matrices M_R and M_S, find $M_{R \circ S}$, $M_{\tilde{R}}$, $M_{\tilde{S}}$, $M_{R \tilde{\circ} S}$, and show that $M_{R \tilde{\circ} S} = M_{\tilde{S} \circ \tilde{R}}$.

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad M_S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

SOLUTION

$$M_{\tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \text{transpose of } M_R$$

$$M_{\tilde{S}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \text{transpose of } M_S$$

$$M_{R \circ S} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad M_{\widetilde{R \circ S}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$M_{\tilde{S} \circ \tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = M_{\widetilde{R \circ S}}$$

////

The following hold for any relations R and S.

1 $\tilde{\tilde{R}} = R$
2 $R = S \Leftrightarrow \tilde{R} = \tilde{S}$
3 $R \subseteq S \Leftrightarrow \tilde{R} \subseteq \tilde{S}$
4 $\widetilde{R \cup S} = \tilde{R} \cup \tilde{S}$
5 $\widetilde{R \cap S} = \tilde{R} \cap \tilde{S}$

We shall leave the proofs as exercises.

Let us now consider some distinct relations R_1, R_2, R_3, R_4 in a set

$X = \{a, b, c\}$ given by

$$R_1 = \{\langle a, b\rangle, \langle a, c\rangle, \langle c, b\rangle\}$$
$$R_2 = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle\}$$
$$R_3 = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, c\rangle\}$$
$$R_4 = \{\langle a, b\rangle, \langle b, a\rangle, \langle c, c\rangle\}$$

Denoting the composition of a relation by itself as

$$R \circ R = R^2 \qquad R \circ R \circ R = R \circ R^2 = R^3 \qquad \cdots \qquad R \circ R^{m-1} = R^m \qquad \cdots$$

let us write the powers of the given relations. Clearly

$$R_1^2 = \{\langle a, b\rangle\} \qquad R_1^3 = \varnothing \qquad R_1^4 = \varnothing \qquad \cdots$$
$$R_2^2 = \{\langle a, c\rangle, \langle b, a\rangle, \langle c, b\rangle\} \qquad R_2^3 = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$$
$$R_2^4 = R_2 \qquad R_2^5 = R_2^2 \qquad R_2^6 = R_2^3 \qquad \cdots$$
$$R_3^2 = \{\langle a, c\rangle, \langle b, c\rangle, \langle c, c\rangle\} = R_3^3 = R_3^4 = R_3^5 \cdots$$
$$R_4^2 = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\} \qquad R_4^3 = R_4 \qquad R_4^5 = R_4^2 \qquad \cdots$$

Given a finite set X, containing n elements, and a relation R in X, we can interpret R^m $(m = 1, 2, \ldots)$ in terms of its graph. This interpretation is done for a number of applications in Chap. 5. With the help of such an interpretation or from the examples given here, it is possible to say that there are at most n distinct powers of R, for R^m, $m > n$, can be expressed in terms of $R, R^2, \ldots, R^n$. Our next step is to construct the relation in X given by

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

Naturally, this construction will require only a finite number of powers of R to be calculated, and these calculations can easily be performed by using the matrix representation of the relation R and the Boolean multiplication of these matrices. Let us now see what the corresponding relations R_1^+, R_2^+, R_3^+, and R_4^+ are

$$R_1^+ = R_1 \cup R_1^2 \cup R_1^3 \cdots = R_1$$
$$R_2^+ = R_2 \cup R_2^2 \cup R_2^3 \cdots = R_2 \cup R_2^2 \cup R_2^3$$
$$= \{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle, \langle a, c\rangle, \langle b, a\rangle, \langle c, b\rangle, \langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$$
$$R_3^+ = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, c\rangle, \langle a, c\rangle\}$$
$$R_4^+ = \{\langle a, b\rangle, \langle b, a\rangle, \langle c, c\rangle, \langle a, a\rangle, \langle b, b\rangle\}$$

Observe that the relations $R_1^+, R_2^+, \ldots, R_4^+$ are all transitive and that $R_1 \subseteq R_1^+$, $R_2 \subseteq R_2^+, \ldots, R_4 \subseteq R_4^+$. From the graphs of these relations one can easily see that R_i^+ is obtained from R_i $(i = 1, 2, 3, 4)$ by adding only those ordered pairs to R_i such that R_i^+ is transitive. We now define R^+ in general.

Definition 2-3.15 Let X be any finite set and R be a relation in X. The relation $R^+ = R \cup R^2 \cup R^3 \cup \cdots$ in X is called the *transitive closure* of R in X.

Theorem 2-3.2 The transitive closure R^+ of a relation R in a finite set X is transitive. Also for any other transitive relation P in X such that $R \subseteq P$, we have $R^+ \subseteq P$. In this sense, R^+ is the smallest transitive relation containing R.

PROOF First, to show that R^+ is transitive, let us assume that $a\ R^+\ b$ and $b\ R^+\ c$ for some $a, b, c \in X$. Since $a\ R^+\ b$, we must have a sequence of elements $d_1, d_2, \ldots, d_k \in X$ such that $d_1 = a$, $d_k = b$, and $d_1\ R\ d_2$, $d_2\ R\ d_3$, $\ldots$, $d_{k-1}\ R\ d_k$. Here we have assumed that $a\ R^k\ b$ for some k. Similarly, since $b\ R^+\ c$, we must have a sequence of elements, say $e_1, e_2, \ldots, e_j$, such that $e_1 = b$, $e_j = c$, and $e_1\ R\ e_2$, $e_2\ R\ e_3$, $\ldots$, $e_{j-1}\ R\ e_j$. Here we have assumed that $b\ R^j\ c$ for some j. It follows from these assumptions that $a\ R^{k+j}\ c$, implying that $a\ R^+\ c$. Hence R^+ must be transitive.

Let us now assume that $a\ R^+\ b$ for some $a, b \in X$, so that there exists a sequence of elements $c_1, c_2, \ldots, c_m \in X$ such that $a = c_1$, $b = c_m$, and $c_i\ R\ c_{i+1}$ for $i = 1, 2, \ldots, m-1$. If there is a transitive relation P in X such that $R \subseteq P$, then $c_i\ P\ c_{i+1}$ for $i = 1, 2, \ldots, m-1$, so that $c_1\ P\ c_m$, that is, $a\ P\ b$. Since $\langle a, b\rangle$ is an arbitrary element of R^+, we see by the same argument that $R^+ \subseteq P$. Hence R^+ is the smallest transitive relation which includes R. ////

Transitive closures of relations have important applications in certain areas such as networks, syntactic analysis, fault detection and diagnosis in switching circuits, etc. A number of these applications are discussed in Chap. 5.

EXERCISES 2-3.7

1 Prove the equivalences and equalities (1) to (5) given at the end of the section (following Example 4).

2 Show that if a relation R is reflexive, then $\tilde{R}$ is also reflexive. Show also that similar remarks hold if R is transitive, irreflexive, symmetric, or antisymmetric.

3 What nonzero entries are there in the relation matrix of $R \cap \tilde{R}$ if R is an antisymmetric relation?

4 Let E be the identity relation on a set X and R be any relation in X; show that $E \cup R \cup \tilde{R}$ is a compatibility relation.

5 Given the relation matrix M_R of a relation R on the set $\{a, b, c\}$, find the relation matrices of $\tilde{R}$, $R^2 = R \circ R$, $R^3 = R \circ R \circ R$, and $R \circ \tilde{R}$.

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

6 Two equivalence relations R and S are given by their relation matrices M_R and M_S. Show that $R \circ S$ is not an equivalence relation.

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad M_S = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Obtain equivalence relations R_1 and R_2 on $\{1, 2, 3\}$ such that $R_1 \circ R_2$ is also an equivalence relation.

2-3.8 Partial Ordering

Definition 2-3.16 A binary relation R in a set P is called a *partial order relation* or a *partial ordering* in P iff R is reflexive, antisymmetric, and transitive.

It is conventional to denote a partial ordering by the symbol $\leq$. This symbol does not necessarily mean "less than or equal to" as is used for real numbers. Since the relation of partial ordering is reflexive, we shall henceforth call it a relation on a set, say P. If $\leq$ is a partial ordering on P, then the ordered pair $\langle P, \leq \rangle$ is called a *partially ordered set* or a *poset*.

Definition 2-3.17 Let $\langle P, \leq \rangle$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$, then $\leq$ is called a *simple ordering* or *linear ordering* on P, and $\langle P, \leq \rangle$ is called a *totally ordered* or *simply ordered set* or a *chain*.

Note that it is not necessary to have $x \leq y$ or $y \leq x$ for every x and y in a partially ordered set P. In fact, x may not be related to y, in which case we say that x and y are *incomparable*.

If R is a partial ordering on P, then it is easy to see that the converse of R, namely $\tilde{R}$, is also a partial ordering on P. If R is denoted by $\leq$, then $\tilde{R}$ is denoted by $\geq$. This means that if $\langle P, \leq \rangle$ is a partially ordered set, then $\langle P, \geq \rangle$ is also a partially ordered set. $\langle P, \geq \rangle$ is called the dual of $\langle P, \leq \rangle$.

We now define another relationship which is associated with every partial ordering $\leq$ on P and which is denoted by $<$. This relation $<$ is defined, for every $x, y \in P$, as

$$x < y \Leftrightarrow x \leq y \wedge x \neq y$$

Similarly, corresponding to the converse partial ordering $\geq$, there is a relation $>$ such that

$$x > y \Leftrightarrow x \geq y \wedge x \neq y$$

Note that the relations $<$ and $>$ are antisymmetric and transitive. In addition, these relations are irreflexive. We now give some partial order relations which are frequently used.

1 Less Than or Equal to, Greater Than or Equal to: Let R be the set of real numbers. The relation "*less than or equal to,*" or $\leq$, is a partial ordering on R. The converse of this relation, "*greater than or equal to,*" or $\geq$, is also a partial ordering on R. Associated relations are "*less than,*" or $<$, and "*greater than,*" or $>$, respectively

2 Inclusion: Let $\rho(A) = 2^A = X$ be the power set of A, that is, X is the set of subsets of A. The relation of inclusion ($\subseteq$) on X is a partial ordering. Associated with the relation $\subseteq$ is a relation called proper inclusion ($\subset$) which is irreflexive, antisymmetric, and transitive.

As a special case, we let $A = \{a, b, c\}$. Then

$$X = \rho(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$$

It is easy to write the elements of the relation $\subseteq$. Note that $\{a\}$ and $\{b, c\}$, $\{a, b\}$ and $\{a, c\}$, etc., are incomparable.

3 Divides and Integral Multiple: If a and b are positive integers, then we say "a divides b," written $a \mid b$, iff there is an integer c such that $ac = b$. Alternatively, we say that "b is an *integral multiple of a*." The relation "*divides*" is a partial order relation. Let X be the set of positive integers. The relations "divides" and "integral multiple of" are partial orderings on X, and each is the converse of the other.

As a special case, let $X = \{2, 3, 6, 8\}$ and let $\leq$ be the relation "divides" on X. Then

$$\leq \; = \{\langle 2, 2\rangle, \langle 3, 3\rangle, \langle 6, 6\rangle, \langle 8, 8\rangle, \langle 2, 8\rangle, \langle 2, 6\rangle, \langle 3, 6\rangle\}$$

The relation "integral multiple of," written as $\geq$, is given by

$$\geq \; = \{\langle 2, 2\rangle, \langle 3, 3\rangle, \langle 6, 6\rangle, \langle 8, 8\rangle, \langle 8, 2\rangle, \langle 6, 2\rangle, \langle 6, 3\rangle\}$$

4 Lexicographic Ordering: A useful example of simple or total ordering is the lexicographic ordering. We shall define it for certain ordered pairs first and then generalize it.

Let R be the set of real numbers and let $P = R \times R$. The relation $\geq$ on R is assumed to be the usual relation of "greater than or equal to." For any two ordered pairs $\langle x_1, y_1\rangle$ and $\langle x_2, y_2\rangle$ in P, we define the total ordering relation S as follows:

$$\langle x_1, y_1\rangle \; S \; \langle x_2, y_2\rangle \Leftrightarrow (x_1 > x_2) \lor ((x_1 = x_2) \land (y_1 \geq y_2))$$

It is clear that if $\langle x_1, y_1\rangle \not S \langle x_2, y_2\rangle$, then we must have $\langle x_2, y_2\rangle \; S \; \langle x_1, y_1\rangle$, so that S is a total ordering on P. The partial ordering S is called the *lexicographic ordering*. The significance of the terminology will become clear after we generalize the above ordering relation. The following are some of the ordered pairs of P which are S-related:

$$\langle 2, 2\rangle \; S \; \langle 2, 1\rangle$$
$$\langle 3, 1\rangle \; S \; \langle 1, 5\rangle$$
$$\langle 2, 2\rangle \; S \; \langle 2, 2\rangle$$
$$\langle 3, 2\rangle \; S \; \langle 1, 1\rangle$$

We now generalize this concept. For this purpose, let R be a total ordering relation on a set X and let

$$P = X \cup X^2 \cup X^3 \cup \cdots \cup X^n = \bigcup_i X^i \qquad (n = 1, 2, 3, \ldots)$$

This equation means that the set P consists of strings of elements of X of length less than or equal to n. We may assume some fixed value of n. A string of length p may be considered as an ordered p-tuple. We now define a total ordering S on P called lexicographic ordering. For this purpose, let $\langle u_1, u_2, \ldots, u_p\rangle$ and $\langle v_1, v_2, \ldots, v_q\rangle$, with $p \leq q$, be any two elements of P. Note that before starting, to compare two strings to determine the ordering in P, the strings are interchanged if necessary so that $p \leq q$. Now

$$\langle u_1, u_2, \ldots, u_p\rangle \; S \; \langle v_1, v_2, \ldots, v_q\rangle$$

if any one of the following holds:

1. $\langle u_1, u_2, \ldots, u_p \rangle = \langle v_1, v_2, \ldots, v_p \rangle$
2. $u_1 \neq v_1$ and $u_1 \; R \; v_1$ in X
3. $u_i = v_i, i = 1, 2, \ldots, k \; (k < p)$, and $u_{k+1} \neq v_{k+1}$ and $u_{k+1} \; R \; v_{k+1}$ in X

If none of these conditions is satisfied, then

$$\langle v_1, v_2, \ldots, v_q \rangle \; S \; \langle u_1, u_2, \ldots, u_p \rangle$$

As a special case of lexicographic ordering, let $X = \{a, b, c, \ldots, z\}$ and let R be a simple ordering on X denoted by $\leq$ where $a \leq b \leq c \leq \cdots \leq z$ and $P = X \cup X^2 \cup X^3$. Thus, P consists of all "words" or strings of 3 or fewer than 3 letters from X. Let S denote the lexicographic ordering on P described earlier. We will have

me S met	by condition 1
bet S met	by condition 2
beg S bet	by condition 3
get S go	by the last rule

since "go" and "get" are compared and the conditions 1, 2, and 3 are not satisfied.

The order in which the words in an English dictionary appear is a familiar example of lexicographic ordering. Instead of using S to denote the lexicographic ordering, it is customary to use names such as "lexically less than or equal to" or "lexically greater than."

We shall now describe how the lexicographic ordering is used in sorting character data on a computer. For this purpose, let X denote the set of characters available on a particular computer. It is necessary first to define a simple ordering on the elements of X (frequently called the collating sequence). One method is to compare the numeric values of the coded representation of each character in the computer by using the relation "less than or equal to." This ordering may vary from one computer to another. An example of a code which has such an ordering is the Extended Binary Coded Decimal Interchange Code (EBCDIC). In any case, we have a totally ordered set $\langle X, \leq \rangle$, and character strings are formed from the elements of X. Since blanks are also permitted to appear in such strings, a blank is treated as a character, i.e., an element of X. It is convenient to assume that a blank is less than all other elements of X. Not only do blanks appear inside a string, but sometimes it will be convenient to add blanks at the end of a string. It will be assumed that such additions do not alter the relative ordering of a string.

Now we consider how two given strings of equal length are compared for the purpose of ordering them lexicographically. If one string is shorter than the other, we simply assume that it is padded at the right end (because we shall assume the scanning is done from left to right) with the number of blanks sufficient that both strings to be compared are of equal length. In some cases, it may be necessary to distinguish between a given string and the one to which some blanks are added. This distinction can be made by comparing the strings for lexical equality and then comparing them according to their lengths.

2-3.9 Partially Ordered Set: Representation and Associated Terminology

In a partially ordered set $\langle P, \leq \rangle$, an element $y \in P$ is said to *cover* an element $x \in P$ if $x < y$ and if there does not exist any element $z \in P$ such that $x \leq z$ and $z \leq y$; that is,

$$y \text{ covers } x \Leftrightarrow (x < y \wedge (x \leq z \leq y \Rightarrow x = z \vee z = y))$$

Sometimes the term "immediate predecessor" is also used. Note that "cover" as used here should not be confused with the "cover" of a set defined in Sec. 2-3.4.

A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $\langle P, \leq \rangle$. In such a diagram, each element is represented by a small circle or a dot. The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between x and y if y covers x. If $x < y$ but y does not cover x, then x and y are not connected directly by a single line. However, they are connected through one or more elements of P. It is possible to obtain the set of ordered pairs in $\leq$ from

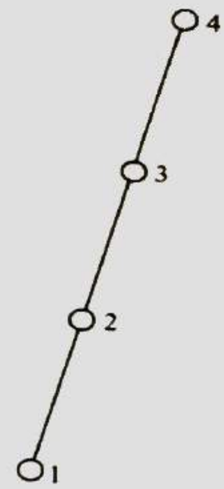


FIGURE 2-3.23 Hasse diagram.

such a diagram. Several examples of partially ordered sets and their Hasse diagrams follow.

For a totally ordered set $\langle P, \leq \rangle$, the Hasse diagram consists of circles, one below the other, as in Fig. 2-3.23. Thus a totally ordered set is called a chain. If we let $P = \{1, 2, 3, 4\}$ and $\leq$ be the relation "less than or equal to," then the Hasse diagram is as shown in Fig. 2-3.23.

Consider the set $P = \{\varnothing, \{a\}, \{a, b\}, \{a, b, c\}\}$ and the relation of inclusion $\subseteq$ on P. The Hasse diagram of $\langle P, \subseteq \rangle$ is similar to that given in Fig. 2-3.23 except that the nodes are relabeled.

The two relations defined above are not equal, but they have the same Hasse diagram. Such situations will be shown to occur frequently, and the reason for these occurrences is explained in Chap. 4 in the discussion of the order isomorphism of two partially ordered sets.

EXAMPLE 1 Let $X = \{2, 3, 6, 12, 24, 36\}$ and the relation $\leq$ be such that $x \leq y$ if x divides y. Draw the Hasse diagram of $\langle X, \leq \rangle$.

SOLUTION The Hasse diagram is given in Fig. 2-3.24. ////

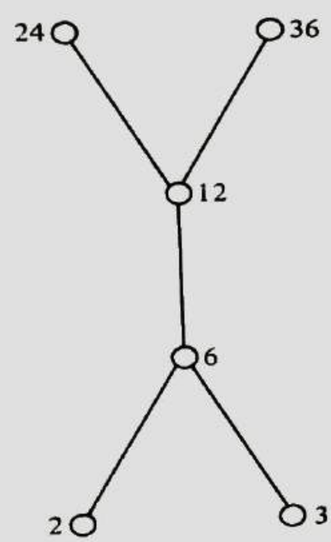


FIGURE 2-3.24 Hasse diagram of divides relation.

EXAMPLE 2 Let A be a given finite set and $\rho(A)$ its power set. Let $\subseteq$ be the inclusion relation on the elements of $\rho(A)$. Draw Hasse diagrams of $\langle \rho(A), \subseteq \rangle$ for (*a*) $A = \{a\}$; (*b*) $A = \{a, b\}$; (*c*) $A = \{a, b, c\}$; (*d*) $A = \{a, b, c, d\}$.

SOLUTION The required Hasse diagrams are given in Fig. 2-3.25*a* to *d*. ////

The following points may be noted about Hasse diagrams in general. For a given partially ordered set, a Hasse diagram is not unique, as can be seen from Fig. 2-3.25*b*. From a Hasse diagram of $\langle P, \leq \rangle$, the Hasse diagram of $\langle P, \geq \rangle$, which is the dual of $\langle P, \leq \rangle$, can be obtained by rotating the diagram through 180° so that the points at the top become the points at the bottom. Some Hasse diagrams have a unique point which is above all the other points, and similarly some Hasse diagrams have a unique point which is below all other points. Such was the case for all the Hasse diagrams given in Example 2, while the Hasse diagram given in Example 1 does not possess this property. The Hasse diagrams become more complicated when the number of elements in the partially ordered set is large.

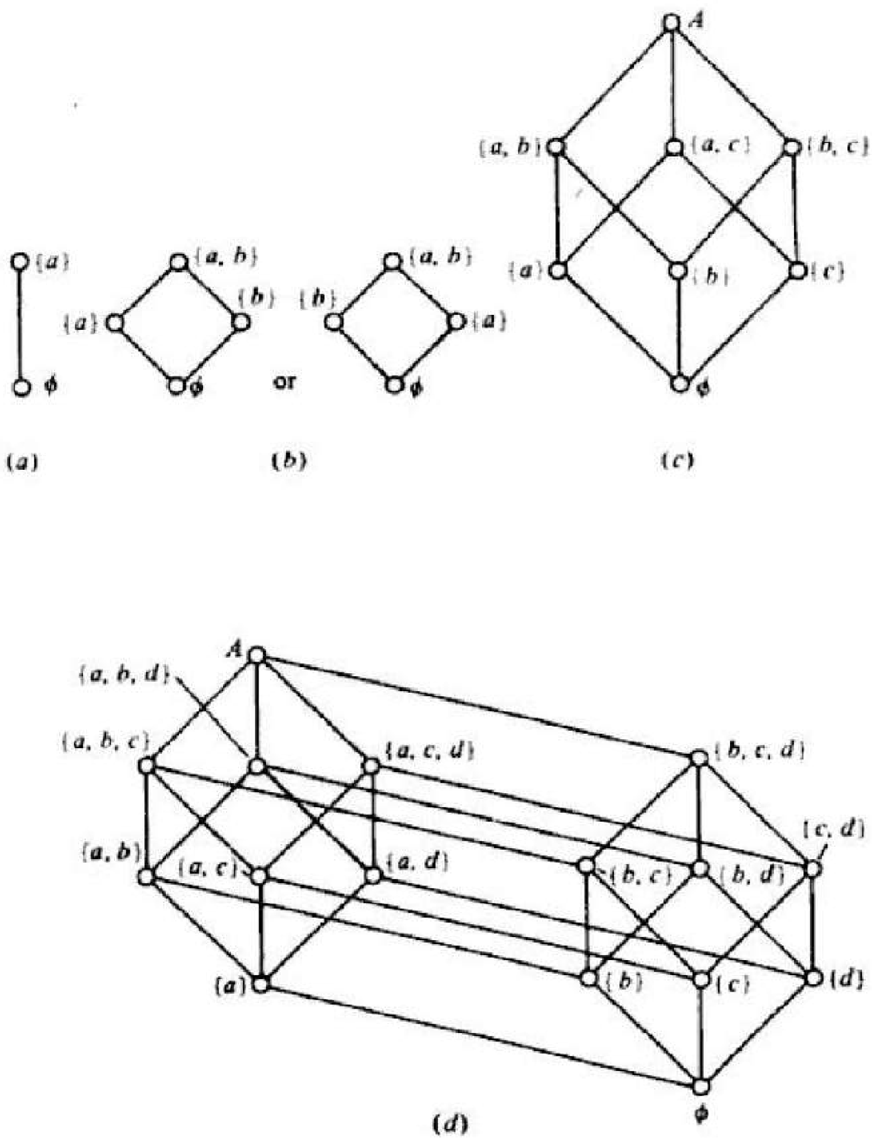


FIGURE 2-3.25 Hasse diagrams of $\langle \rho(A), \subseteq \rangle$.

EXAMPLE 3 Let A be the set of factors of a particular positive integer m and let $\leq$ be the relation divides, i.e.,

$$\leq \;=\; \{\langle x, y\rangle \mid x \in A \;\wedge\; y \in A \;\wedge\; (x \text{ divides } y)\}$$

Draw Hasse diagrams for (a) $m = 2$; (b) $m = 6$; (c) $m = 30$; (d) $m = 210$; (e) $m = 12$; and (f) $m = 45$.

SOLUTION The required Hasse diagrams for (a) to (d) are the same as given in Fig. 2-3.25a to d. Hasse diagrams of (e) and (f) are given in Fig. 2-3.26. ////

In Examples 2 and 3 we saw that the Hasse diagrams (a) to (d) are identical. However, Hasse diagrams (e) and (f) of Example 3 cannot be given by the Hasse diagram of any power set of a set, because a power set has 2^n elements, while in (e) and (f) we only have 6 elements in each of the partially ordered sets. Of course, in all the cases given in Example 3 we again have a single element at the top and a single element at the bottom because if p is any divisor of m, we have $1 \leq p \leq m$.

Hasse diagrams can also be drawn for any relation which is antisymmetric and transitive but not necessarily reflexive. Examples of such relations are proper inclusion and any relation $<$ associated with the partial ordering relation $\leq$. Any family tree or organization chart of the military or of any establishment is a Hasse diagram in this sense. We shall, however, assume that a Hasse diagram represents a partial ordering unless otherwise stated. Some Hasse diagrams are given in Fig. 2-3.27.

We shall now introduce terminology for partially ordered sets which will be found useful in Chap. 4. To this end, let $\langle P, \leq\rangle$ denote a partially ordered set.

If there exists an element $y \in P$ such that $y \leq x$ for all $x \in P$, then y is called the *least member* in P relative to the partial ordering $\leq$. Similarly, if there exists an element $y \in P$ such that $x \leq y$ for all $x \in P$, then y is called the *greatest*

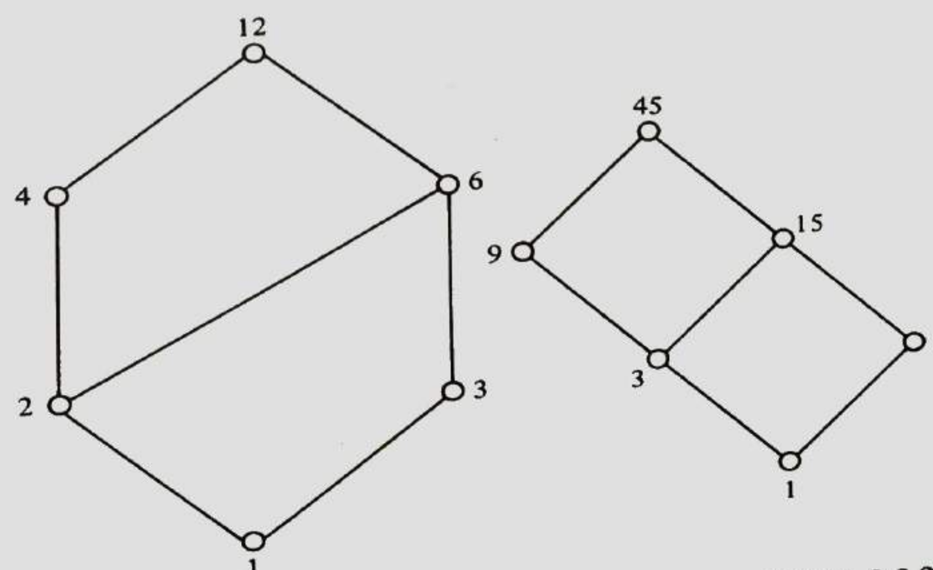


FIGURE 2-3.26

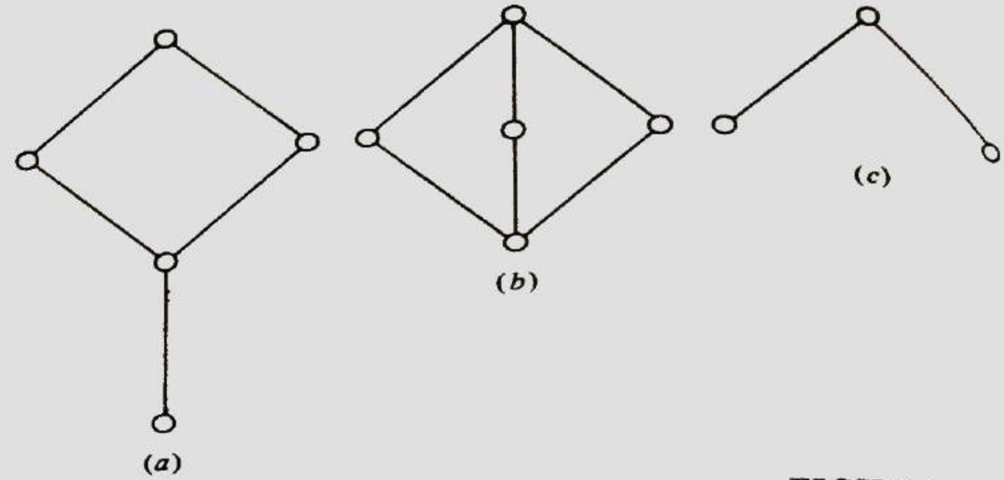


FIGURE 2-3.27

member in P relative to $\leq$. From the definition it is clear that the least member, if it exists, is unique; so also is the greatest member. It may happen that the least or the greatest member does not exist. The least member is usually denoted by 0 and the greatest by 1.

If the Hasse diagram of a partially ordered set is available, then it is easy to see whether the least or the greatest member exists. From Fig. 2-3.23 it is clear that the least member is 1 and the greatest is 4. In Example 1 there is no least or greatest member, while in Example 2 the least member is $\varnothing$ and the greatest member is A in all cases. In every simple ordering or chain, the least and the greatest members always exist. The Hasse diagram of Fig. 2-3.27c shows that the greatest member exists but there is no least member.

An element $y \in P$ is called a *minimal member* of P relative to a partial ordering $\leq$ if for no $x \in P$ is $x < y$. A minimal member need not be unique. All those members which appear at the lowest level of a Hasse diagram of a partially ordered set are minimal members. Similarly, an element $y \in P$ is called a *maximal member* of P relative to a partial ordering $\leq$ if for no $x \in P$ is $y < x$. In the Hasse diagram of Fig. 2-3.27c, there are two minimal members and one maximal member. Distinct minimal members are incomparable, and distinct maximal members are also incomparable.

It is not always necessary to draw the Hasse diagram of a partially ordered set in order to determine the least, greatest, maximal, and minimal members. However, their determination becomes simple when such a diagram is available.

We now extend these ideas to the subsets of a partially ordered set.

Definition 2-3.18 Let $\langle P, \leq \rangle$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is an *upper bound* for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in P$ is a *lower bound* for A if for all $a \in A$, $x \leq a$.

Let us consider the partially ordered set $\langle \rho(A), \subseteq \rangle$ in Example 2c. We choose a subset B of $\rho(A)$ given by $\{\{b, c\}, \{b\}, \{c\}\}$. Then $\{b, c\}$ and A are upper bounds for B, while $\varnothing$ is its lower bound. For the subset $C = \{\{a, c\}, \{c\}\}$, the upper bounds are $\{a, c\}$ and A while the lower bounds are $\{c\}$ and $\varnothing$. In Example 1, if $A = \{2, 3, 6\}$, then 6, 12, 24, and 36 are upper bounds for A, and there is no lower bound.

Note that upper and lower bounds of a subset are not necessarily unique. We therefore define the following terms.

Definition 2-3.19 Let $\langle P, \leq \rangle$ be a partially ordered set and let $A \subseteq P$. An element $x \in P$ is a *least upper bound*, or *supremum*, for A if x is an upper bound for A and $x \leq y$ where y is any upper bound for A. Similarly, the *greatest lower bound*, or *infimum*, for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lower bounds y.

A least upper bound, if it exists, is unique, and the same is true for a greatest lower bound. The least upper bound is abbreviated as "LUB" or "sup," and the greatest lower bound is abbreviated as "GLB" or "inf."

For a simply ordered set or a chain, every subset has a supremum and an infimum. Similarly, the partially ordered sets given in Examples 2 and 3 are such that every subset has a supremum and an infimum. This, however, is not generally the case, as can be seen from Example 1 in which the set $A = \{2, 3, 6\}$ has the LUB $A = 6$, while the GLB A does not exist. Similarly, for the subset $\{2, 3\}$, the supremum is again 6, but there is no infimum. For the subset $\{12, 6\}$, the supremum is 12 and the infimum is 6. The partially ordered sets which are such that every subset has a supremum and an infimum form an important subclass of partially ordered sets. Such sets are discussed in Chap. 4.

For a partially ordered set $\langle P, \leq \rangle$, we know that its dual $\langle P, \geq \rangle$ is also a partially ordered set. The least member of P relative to the ordering $\leq$ is the greatest member in P relative to the ordering $\geq$, and vice versa. Similarly, the maximal and minimal elements are interchanged. For any subset $A \subseteq P$, the GLB A in $\langle P, \leq \rangle$ is the same as the LUB A in $\langle P, \geq \rangle$.

We shall end this section by defining a property which has important applications in the use of the principle of transfinite induction.

Definition 2-3.20 A partially ordered set is called *well-ordered* if every nonempty subset of it has a least member.

As a consequence of this definition, it follows that every well-ordered set is totally ordered, because for any subset, say $\{x, y\}$, we must have either x or y as its least member. Of course, every totally ordered set need not be well-ordered. A finite totally ordered set is also well-ordered.

A simple example of a well-ordered set is the set $\mathbf{I}_n = \{1, 2, \ldots, n\}$ or the set $\mathbf{I} = \{1, 2, \ldots\}$. Similarly the sets $\mathbf{I}_n \times \mathbf{I}_n$ or $\mathbf{I} \times \mathbf{I}$ are well-ordered under the natural ordering of "less than or equal." It is possible, however, to define a certain partial ordering on $\mathbf{I} \times \mathbf{I}$ such that it is no longer a well-ordered set.

EXERCISES 2-3.9

1 Draw the Hasse diagrams of the following sets under the partial ordering relation "divides," and indicate those which are totally ordered.

$\{2, 6, 24\}$ $\quad \{3, 5, 15\}$ $\quad \{1, 2, 3, 6, 12\}$ $\quad \{2, 4, 8, 16\}$ $\quad \{3, 9, 27, 54\}$

2 If R is a partial ordering relation on a set X and $A \subseteq X$, show that $R \cap (A \times A)$ is a partial ordering relation on A.

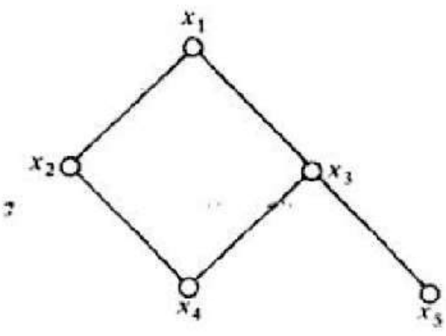


FIGURE 2-3.28

3 Give an example of a set X such that $\langle \rho(X), \subseteq \rangle$ is a totally ordered set.
4 Give a relation which is both a partial ordering relation and an equivalence relation on a set.
5 Let S denote the set of all the partial ordering relations on a set P. Define a partial ordering relation on S and interpret this relation in terms of the elements of P.
6 Figure 2-3.28 gives the Hasse diagram of a partially ordered set $\langle P, R \rangle$, where $P = \{x_1, x_2, \ldots, x_5\}$. Find which of the following are true: $x_1 \, R \, x_2$, $x_4 \, R \, x_1$, $x_3 \, R \, x_5$, $x_2 \, R \, x_5$, $x_1 \, R \, x_1$, $x_2 \, R \, x_3$, and $x_4 \, R \, x_5$. Find the least and greatest members in P if they exist. Also find the maximal and minimal elements of P. Find the upper and lower bounds of $\{x_2, x_3, x_4\}$, $\{x_3, x_4, x_5\}$, and $\{x_1, x_2, x_3\}$. Also indicate the LUB and GLB of these subsets if they exist.
7 Show that there are only five distinct Hasse diagrams for partially ordered sets that contain three elements.

2-4 FUNCTIONS

In this section we study a particular class of relations called functions. We are primarily concerned with discrete functions which transform a finite set into another finite set. There are several such transformations involved in the computer implementation of any program. Computer output can be considered as a function of the input. A compiler transforms a program into a set of machine language instructions (the object program). After introducing the concept of function in general, we discuss unary and binary operations which form a class of functions. Such operations have important applications in the study of algebraic structures in Chaps. 3 and 4. Also discussed is a special class of functions known as hashing functions that are used in organizing files on a computer, along with other techniques associated with such organizations. A PL/I program for the construction of a symbol table is also given.

2-4.1 Definition and Introduction

Definition 2-4.1 Let X and Y be any two sets. A relation f from X to Y is called a *function* if for every $x \in X$ there is a unique $y \in Y$ such that $\langle x, y \rangle \in f$.

Note that the definition of function requires that a relation must satisfy two additional conditions in order to qualify as a function. The first condition is that every $x \in X$ must be related to some $y \in Y$, that is, the domain of f must be X and not merely a subset of X. The second requirement of uniqueness can be expressed as

$$\langle x, y \rangle \in f \wedge \langle x, z \rangle \in f \Rightarrow y = z$$

Terms such as "transformation," "map" (or "mapping"), "correspondence," and "operation" are used as synonyms for "function." The notations $f: X \to Y$ or $X \xrightarrow{f} Y$ are used to express f as a function from X to Y. Pictorially, a function is generally shown as in Fig. 2-4.1.

For a function $f: X \to Y$, if $\langle x, y \rangle \in f$, then x is called an *argument* and the corresponding y is called the *image* of x under f. Instead of writing $\langle x, y \rangle \in f$, it is customary to write $y = f(x)$ and to call y the *value of the function* f at x. Other ways of expressing $y = f(x)$ are $f: x \to y$, $x \xrightarrow{f} y$, and, of course, $\langle x, y \rangle \in f$. As an extension of this notation to the whole set X, we sometimes denote the range of f, viz., R_f, by $f(X)$. The range of f is defined as

$$\{y \mid \exists x \in X \wedge y = f(x)\}$$

It was mentioned that the domain of f is X, that is, $D_f = X$. The range of f is denoted by R_f and $R_f \subseteq Y$. The set Y is called the *codomain* of f. Some authors permit $D_f \subseteq X$, but according to our definition $D_f = X$.

Since a function is a relation, we can use a relation matrix or a graph to represent it in some cases. Note that from the definition of a function it follows that every row of its relation matrix must have only one entry which is 1 while all other entries in this row are 0s. Therefore, one can replace the relation matrix by a single column, i.e., a vector consisting of entries which are images of the arguments. Thus the column consists of entries which show a correspondence between the argument and the image of the function under the argument. In certain other cases, this correspondence can be expressed more easily by a rule. For example, $f(x) = x^2$ for $x \in \mathbf{R}$ represents the function $\{\langle x, x^2 \rangle \mid x \in \mathbf{R}\}$ where $\mathbf{R}$ is the set of real numbers and $f: \mathbf{R} \to \mathbf{R}$. Graphs of some functions are shown in Fig. 2-4.2.

Note that more than one element $x \in X$ may have the same function value; for example, $g(x_1) = g(x_2) = y_3$ for the function g whose graph is given in Fig. 2-4.2.

The following are some illustrations of functions.

1 Let $X = \{1, 5, P, \text{Jack}\}$, $Y = \{2, 5, 7, q, \text{Jill}\}$, and $f = \{\langle 1, 2\rangle, \langle 5, 7\rangle, \langle P, q\rangle, \langle \text{Jack}, q\rangle\}$. Obviously $D_f = X$, $R_f = \{2, 7, q\}$, and $f(1) = 2$, $f(5) = 7$, $f(P) = q$, $f(\text{Jack}) = q$.

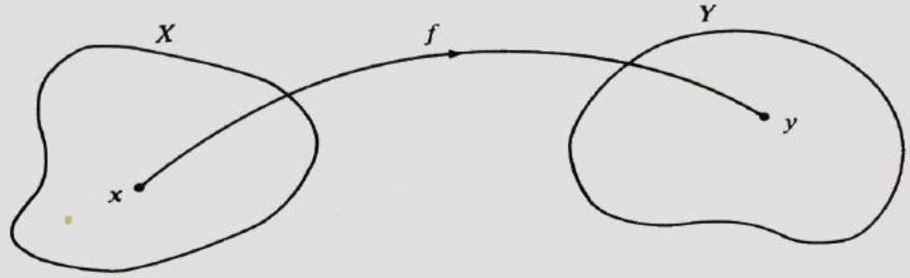


FIGURE 2-4.1 Representation of a function.

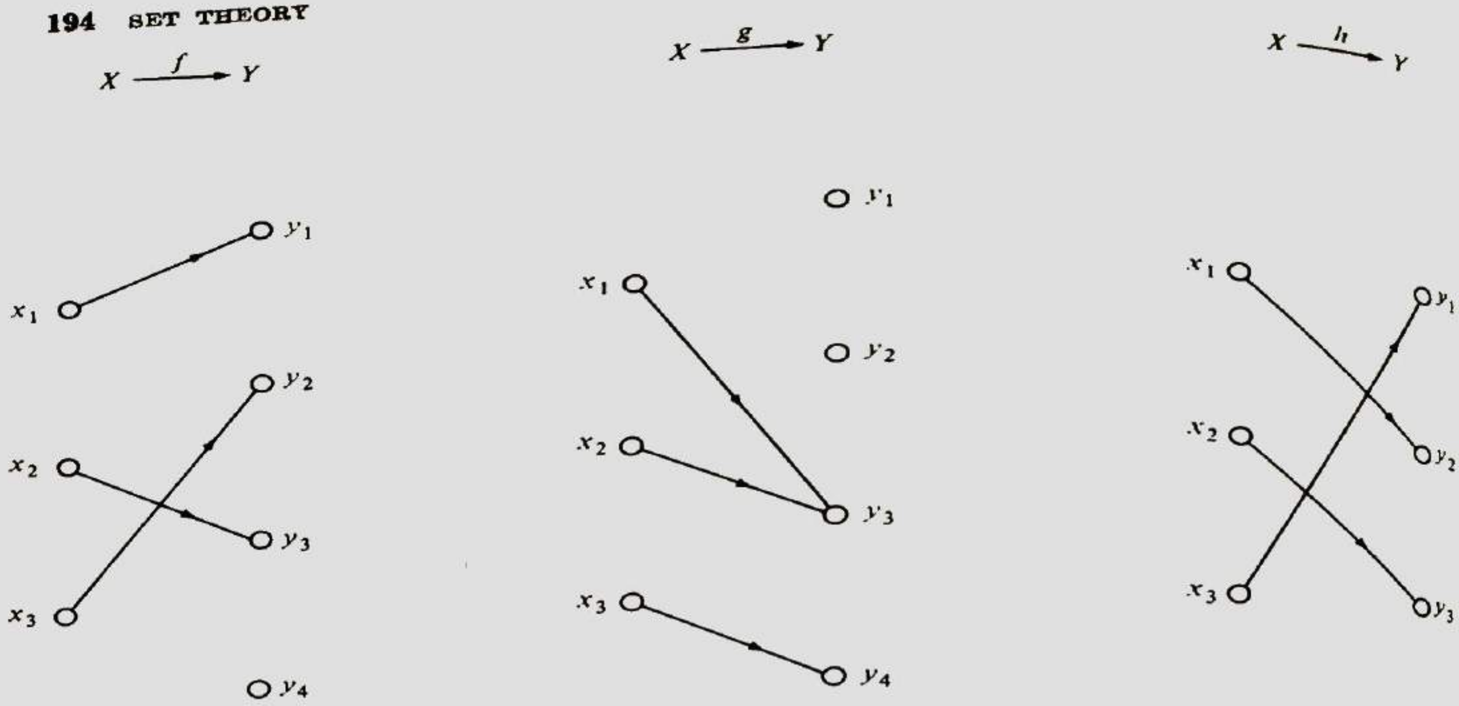


FIGURE 2-4.2 Graphs of functions.

2 Let $X = Y = \mathbf{R}$ and $f(x) = x^2 + 2$. $D_f = \mathbf{R}$ and $R_f \subseteq \mathbf{R}$. The values of f for different values of $x \in \mathbf{R}$ all lie on a parabola, as shown in Fig. 2-4.3.

3 Let $X = Y = \mathbf{R}$ and let

$$f = \{\langle x, x^2 \rangle \mid x \in \mathbf{R}\}$$

$$g = \{\langle x^2, x \rangle \mid x \in \mathbf{R}\}$$

Clearly f is a function from X to Y. However, g is not a function because the uniqueness condition is violated, as can be seen by noting that for any real number a, $\langle a^2, a \rangle$ and $\langle a^2, -a \rangle$ are both in g.

4 Let E be the universal set and $\rho(E)$ be its power set. For any two sets $A, B \in \rho(E)$, the operations of union and intersection are mappings from

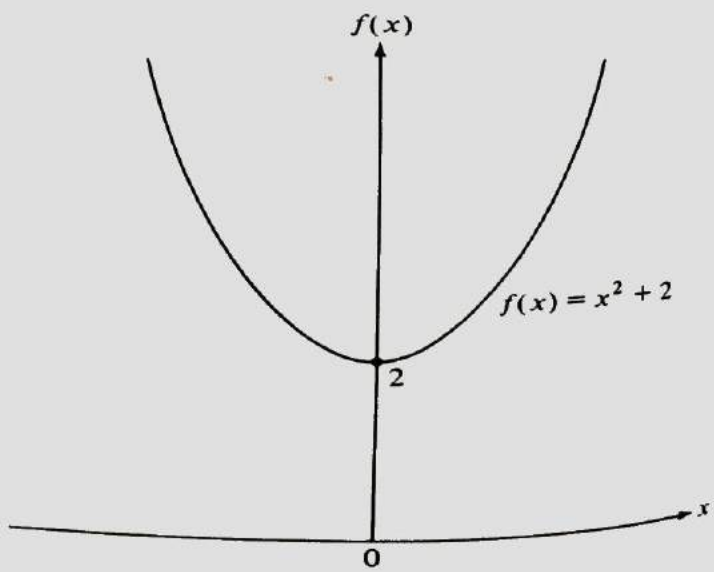


FIGURE 2-4.3

$\rho(E) \times \rho(E)$ to $\rho(E)$. Similarly, complementation is a mapping from $\rho(E)$ to $\rho(E)$.

5 Let P be the set of all positive integers and $\sigma: P \to P$ be such that $\sigma(n) = n + 1$ where $n \in P$. Obviously $\sigma(1) = 2$, $\sigma(2) = 3$, ... The function σ is called *Peano's successor function* and is used in the description of integers in Sec. 2-5.1.

6 Let X be the set of all statements in logic and let Y denote the set $\{T, F\}$, where T and F denote the truth values. The assignment of truth values to statements can be considered as a mapping from X to Y.

7 Let functions f and g be defined by

$$f = \{\langle x, \lfloor x \rfloor\rangle \mid x \in \mathbf{R} \wedge \lfloor x \rfloor = \text{the greatest integer less than or equal to } x\}$$

$$g = \{\langle x, \lceil x \rceil\rangle \mid x \in \mathbf{R} \wedge \lceil x \rceil = \text{the least integer greater than or equal to } x\}$$

The function $f(x) = \lfloor x \rfloor$ is frequently called the *floor* of x, and similarly, the function $g(x) = \lceil x \rceil$ is called the *ceiling* of x. As examples, study the following:

$$f(3.75) = \lfloor 3.75 \rfloor = 3 \qquad \lfloor 4 \rfloor = 4 \qquad \lfloor -3.75 \rfloor = -4$$

$$g(3.33) = \lceil 3.33 \rceil = 4 \qquad \lceil 4 \rceil = 4 \qquad \lceil -3.33 \rceil = -3$$

8 A program written in a high-level language is transformed (or mapped) into a machine language by a compiler. Similarly, the output from a computer is a function of its input.

Definition 2-4.2 If $f: X \to Y$ and $A \subseteq X$, then $f \cap (A \times Y)$ is a function from $A \to Y$ called the *restriction* of f to A and is sometimes written as f/A. If g is a restriction of f, then f is called the *extension* of g.

Note that $(f/A): A \to Y$ is such that for any $a \in A$, $(f/A)(a) = f(a)$. The domain of f/A is A, while that of f is X. Obviously, if g is a restriction of f, then $D_g \subseteq D_f$ and $g(x) = f(x)$ for $x \in D_g$ and $g \subseteq f$. As illustrations of these concepts, consider the following:

9 Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = x^2$ as in (3). If $\mathbf{N}$ is the set of natural numbers, $\{0, 1, 2, \ldots\}$, then $\mathbf{N} \subseteq \mathbf{R}$ and

$$f/\mathbf{N} = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 4\rangle, \langle 3, 9\rangle, \ldots\}$$

10 Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = |x|$, where $|x|$ denotes the absolute value of x. Let $\mathbf{R}_+$ be the set of positive real numbers and $g: \mathbf{R}_+ \to \mathbf{R}$ be given by $g(x) = x$; then g is a restriction of f, that is, $g = f/\mathbf{R}_+$ and f is the extension of g in $\mathbf{R}$.

Equality of functions can be defined in terms of the equality of sets since functions are sets of ordered pairs. This definition also requires that equal functions have the same domain and the same range.

We know that not all possible subsets of $X \times Y$ are functions from X to Y. The collection of all those subsets of $X \times Y$ which define a function is denoted by Y^X. The reason for using this notation will be clear from the following illustration.

11 Let $X = \{a, b, c\}$ and $Y = \{0, 1\}$. Then

$$X \times Y = \{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 0\rangle, \langle a, 1\rangle, \langle b, 1\rangle, \langle c, 1\rangle\}$$

and there are 2^6 possible subsets of $X \times Y$. Of these, only the following 2^3 subsets define functions from X to Y.

$$f_0 = \{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 0\rangle\} \qquad f_4 = \{\langle a, 1\rangle, \langle b, 0\rangle, \langle c, 0\rangle\}$$
$$f_1 = \{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 1\rangle\} \qquad f_5 = \{\langle a, 1\rangle, \langle b, 0\rangle, \langle c, 1\rangle\}$$
$$f_2 = \{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 0\rangle\} \qquad f_6 = \{\langle a, 1\rangle, \langle b, 1\rangle, \langle c, 0\rangle\}$$
$$f_3 = \{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 1\rangle\} \qquad f_7 = \{\langle a, 1\rangle, \langle b, 1\rangle, \langle c, 1\rangle\}$$

In order to determine the number of functions from X to Y when both X and Y are finite, let us assume that X and Y have m and n distinct elements respectively. Since the domain of any function from X to Y is X, there are exactly m ordered pairs in each of the functions. Further, any element $x \in X$ can have any one of the n elements of Y as its image; therefore there are n^m possible functions which are distinct. In illustration (11), $m = 3$ and $n = 2$ and there are $2^3 = 8$ functions. The number n^m also explains why the notation Y^X was used to represent the set of all functions from X to Y. The same notation is used even when X or Y are infinite sets. It must be emphasized that the number of functions depends upon the number of elements in the sets X and Y and not on the sets. Therefore, in illustration (11) if Y is any set having 2 elements, the number of functions from X to Y will still be 8.

In the construction of truth tables of a statement function of n variables, we had 2^n rows because each row defined a distinct function from the set of n variables to the set $\{T, F\}$ of truth values.

Definition 2-4.3 A mapping of $f\colon X \to Y$ is called *onto* (*surjective*, a *surjection*) if the range $R_f = Y$; otherwise it is called *into*.

In Fig. 2-4.2 the function h is an onto mapping, while the others are into mappings. Illustrations (1), (2), (3), and (5) are into mappings while (4) and (6) are onto.

Definition 2-4.4 A mapping $f\colon X \to Y$ is called *one-to-one* (*injective*, or *1–1*) if distinct elements of X are mapped into distinct elements of Y. In other words, f is one-to-one if

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

or equivalently

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

In Fig. 2-4.2, f and h are both one-to-one. Also the mapping in illustration

(5) is one-to-one, and so is $f/\mathbf{N}$ in (9). Although f in (10) is not one-to-one, its restriction g is.

It is easy to see that when X and Y are finite sets, a mapping $f: X \to Y$ can be one-to-one only if the number of elements in X is less than or equal to the number of elements in Y.

Definition 2-4.5 A mapping $f: X \to Y$ is called *one-to-one onto* (*bijective*) if it is both one-to-one and onto. Such a mapping is also called a one-to-one correspondence between X and Y.

For $f: X \to Y$ to be bijective when X and Y are finite requires that the number of elements in X be the same as the number of elements in Y. The function h whose graph is shown in Fig. 2-4.2 is bijective. Similarly, $f(x) = 2x + 1$ and $g(x) = x$ for $x \in \mathbf{R}$ are also bijective mappings from $\mathbf{R}$ to $\mathbf{R}$. We shall be interested in bijective mappings in the next section where it is shown that such functions have inverses.

EXERCISES 2-4-1

1 Let $\mathbf{N}$ be the set of natural numbers including zero. Determine which of the following functions are one-to-one, which are onto, and which are one-to-one onto.

(*a*) $f: \mathbf{N} \to \mathbf{N}$ $\quad f(j) = j^2 + 2$

(*b*) $f: \mathbf{N} \to \mathbf{N}$ $\quad f(j) = j \pmod 3$

(*c*) $f: \mathbf{N} \to \mathbf{N}$ $\quad f(j) = \begin{cases} 1 & j \text{ is odd} \\ 0 & j \text{ is even} \end{cases}$

(*d*) $f: \mathbf{N} \to \{0, 1\}$ $\quad f(j) = \begin{cases} 0 & j \text{ is odd} \\ 1 & j \text{ is even} \end{cases}$

2 Let $\mathbf{I}$ be the set of integers, $\mathbf{I}_+$ the set of positive integers, and $\mathbf{I}_p = \{0, 1, 2, \ldots, p-1\}$. Determine which of the following functions are one-to-one, which are onto, and which are one-to-one onto.

(*a*) $f: \mathbf{I} \to \mathbf{I}$ $\quad f(j) = \begin{cases} j/2 & j \text{ is even} \\ (j-1)/2 & j \text{ is odd} \end{cases}$

(*b*) $f: \mathbf{I}_+ \to \mathbf{I}_+$ $\quad f(x) = \text{greatest integer} \leq \sqrt{x}$

(*c*) $f: \mathbf{I}_7 \to \mathbf{I}_7$ $\quad f(x) = 3x \pmod 7$

(*d*) $f: \mathbf{I}_4 \to \mathbf{I}_4$ $\quad f(x) = 3x \pmod 4$

3 If X and Y are finite sets, find a necessary condition for the existence of one-to-one mappings from X to Y.

4 Do the following sets define functions? If so, give their domain and range in each case.

(*a*) $\{\langle 1, \langle 2, 3\rangle\rangle, \langle 2, \langle 3, 4\rangle\rangle, \langle 3, \langle 1, 4\rangle\rangle, \langle 4, \langle 1, 4\rangle\rangle\}$

(*b*) $\{\langle 1, \langle 2, 3\rangle\rangle, \langle 2, \langle 3, 4\rangle\rangle, \langle 3, \langle 3, 2\rangle\rangle\}$

(*c*) $\{\langle 1, \langle 2, 3\rangle\rangle, \langle 2, \langle 3, 4\rangle\rangle, \langle 1, \langle 2, 4\rangle\rangle\}$

(*d*) $\{\langle 1, \langle 2, 3\rangle\rangle, \langle 2, \langle 2, 3\rangle\rangle, \langle 3, \langle 2, 3\rangle\rangle\}$

5 List all possible functions from $X = \{a, b, c\}$ to $Y = \{0, 1\}$ and indicate in each case whether the function is one-to-one, is onto, and is one-to-one onto.

6 If $A = \{1, 2, \ldots, n\}$, show that any function from A to A which is one-to-one must also be onto, and conversely.

7 Show that the functions f and g which both are from $\mathbf{N} \times \mathbf{N}$ to $\mathbf{N}$ given by $f\langle x, y\rangle = x + y$ and $g\langle x, y\rangle = xy$ are onto but not one-to-one.

2-4.2 Composition of Functions

The operation of composition of relations can be extended to functions in the following manner.

Definition 2-4.6 Let $f: X \to Y$ and $g: Y \to Z$ be two functions. The *composite relation* $g \circ f$ such that

$$g \circ f = \{\langle x, z\rangle \mid (x \in X) \wedge (z \in Z) \wedge (\exists y)(y \in Y \wedge y = f(x) \wedge z = g(y))\}$$

is called the *composition* of functions or *relative product* of functions f and g. More precisely, $g \circ f$ is called the *left composition* of g with f.

Note that in the above definition it is assumed that the range R_f of f is a subset of the domain of g, which is Y, that is $R_f \subseteq D_g$; otherwise, $g \circ f$ is empty. Assuming that $g \circ f$ is not empty, we now show that $g \circ f$ is a function from X to Z. For this purpose, let us assume that $\langle x, z_1\rangle$ and $\langle x, z_2\rangle$ are both in $g \circ f$. This assumption requires that there is a $y \in Y$ such that $y = f(x)$ and $z_1 = g(y)$; also $z_2 = g(y)$. Since g is a function, we cannot have $z_1 = g(y)$ and $z_2 = g(y)$; hence $g \circ f$ is a function. Any function g for which $g \circ f$ can be formed is said to be *left-composable* with the function f. In such a case, $(g \circ f)(x) = g(f(x))$, where x is in the domain of $g \circ f$. The composition of functions is shown in Fig. 2-4.4.

Given $f: X \to Y$ and $g: Y \to Z$, we have the composite function $g \circ f$. However, the composite function $f \circ g$ may or may not exist. For the existence of $f \circ g$, it is necessary that $R_g \subseteq D_f$. For functions $f: X \to X$ and $g: X \to X$, the composite functions such as $f \circ g$, $g \circ f$, $f \circ f$, $g \circ g$, etc., can be formed. This point will be demonstrated by means of examples.

Consider three functions $f: X \to Y$, $g: Y \to Z$, and $h: Z \to W$. The composite functions $(g \circ f): X \to Z$ and $(h \circ g): Y \to W$ can be formed. Other composite functions such as $h \circ (g \circ f)$ and $(h \circ g) \circ f$ can also be formed. Both of these functions are from X to W. Assuming $y = f(x)$, $z = g(y)$, and $w = h(z)$, we have $\langle x, y\rangle \in f$, $\langle y, z\rangle \in g$, $\langle z, w\rangle \in h$ and $\langle x, z\rangle \in g \circ f$. $\langle y, w\rangle \in h \circ g$. Continuing the same argument, $\langle x, w\rangle \in h \circ (g \circ f)$. Similarly $\langle x, w\rangle \in (h \circ g) \circ f$. This fact being true for any x and corresponding w, we have (see also Fig. 2-4.5)

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{1}$$

Thus the composition of functions is associative, and we may drop the parentheses in writing the functions in (1), so that $h \circ g \circ f = h \circ (g \circ f) = (h \circ g) \circ f$.

The composition of functions is also shown in Fig. 2-4.6.

EXAMPLE 1 Let $X = \{1, 2, 3\}$, $Y = \{p, q\}$, and $Z = \{a, b\}$. Also let $f: X \to Y$ be $f = \{\langle 1, p\rangle, \langle 2, p\rangle, \langle 3, q\rangle\}$ and $g: Y \to Z$ be given by $g = \{\langle p, b\rangle, \langle q, b\rangle\}$. Find $g \circ f$.

SOLUTION $g \circ f = \{\langle 1, b\rangle, \langle 2, b\rangle, \langle 3, b\rangle\}$. ////

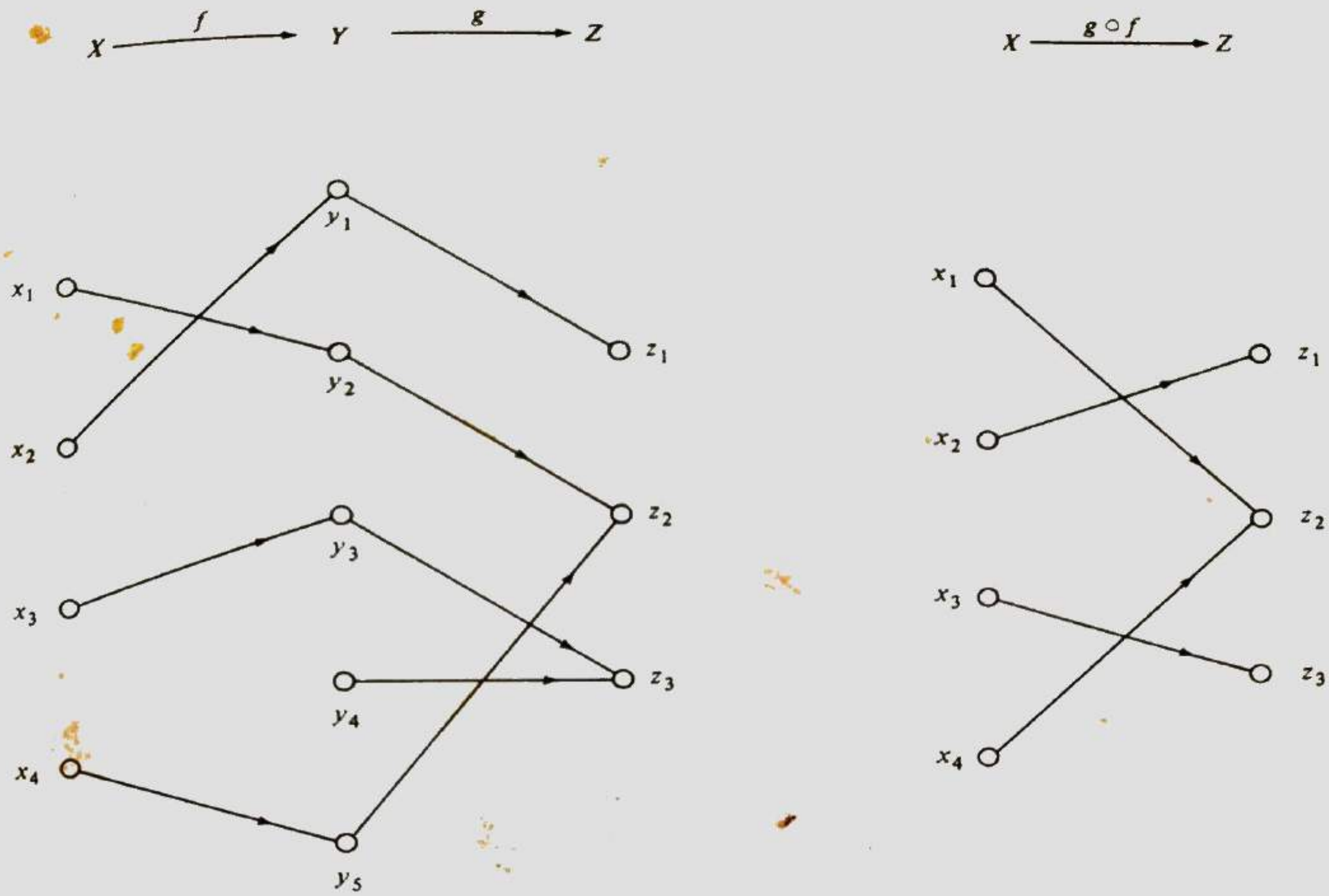


FIGURE 2-4.4 Composition of functions

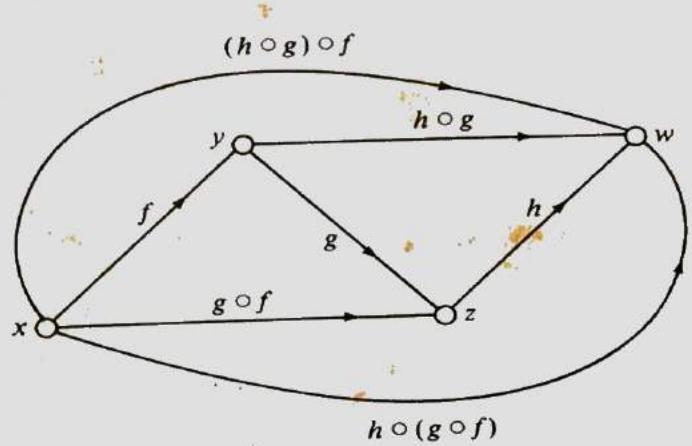


FIGURE 2-4.5

EXAMPLE 2 Let $X = \{1, 2, 3\}$ and f, g, h, and s be functions from X to X given by

$$f = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle\} \qquad g = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle\}$$

$$h = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 1\rangle\} \qquad s = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$$

Find $f \circ g$; $g \circ f$; $f \circ h \circ g$; $s \circ g$; $g \circ s$; $s \circ s$; and $f \circ s$.

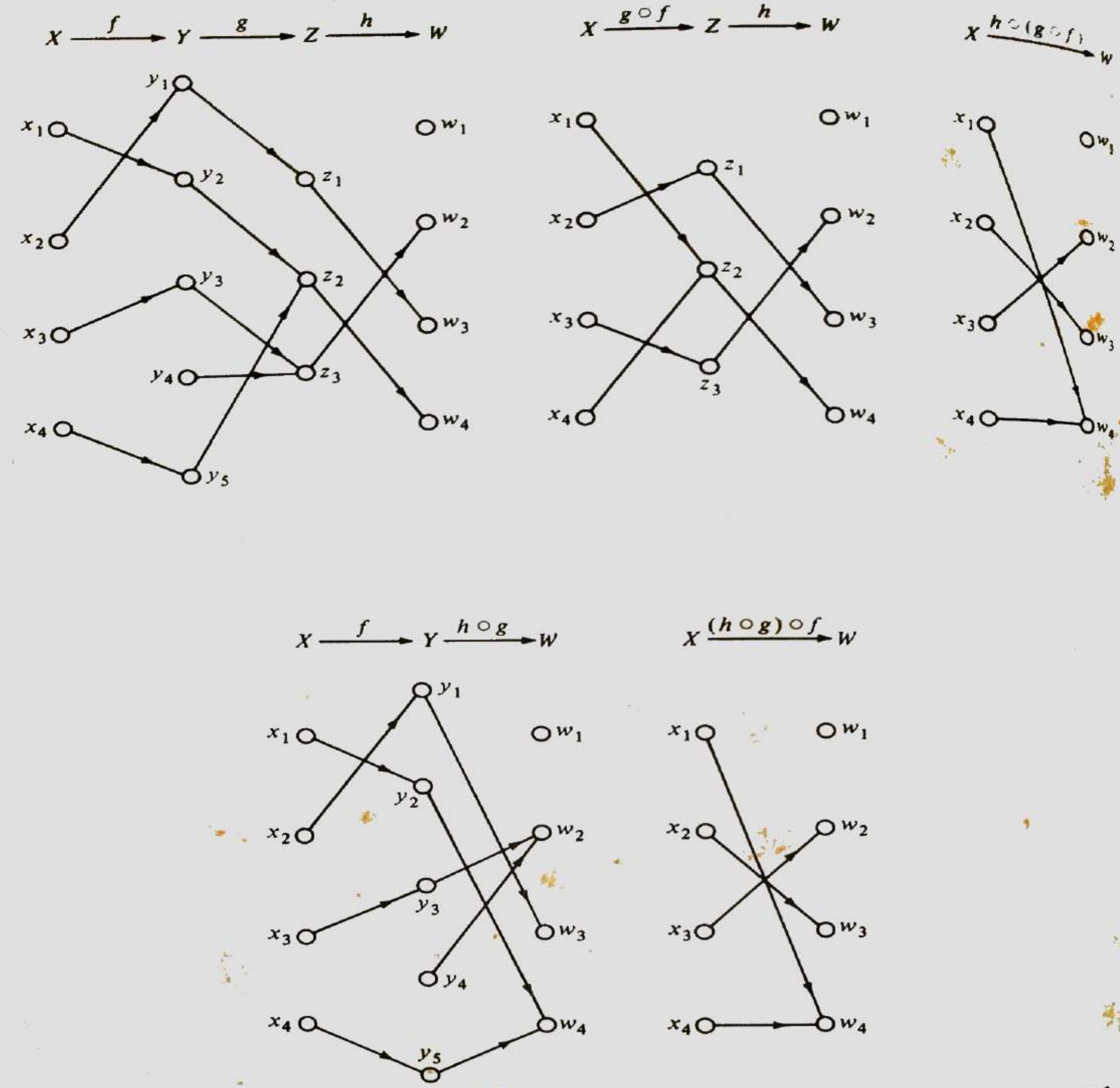


FIGURE 2-4.6

SOLUTION

$$f \circ g = \{\langle 1, 3\rangle, \langle 2, 2\rangle, \langle 3, 1\rangle\}$$
$$g \circ f = \{\langle 1, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle\} \neq f \circ g$$
$$f \circ h \circ g = \{\langle 1, 3\rangle, \langle 2, 2\rangle, \langle 3, 2\rangle\}$$
$$s \circ g = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle\} = g = g \circ s$$
$$s \circ s = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\} = s$$
$$f \circ s = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle\} = f$$

Observe that $s \circ s = s$; $f \circ s = s \circ f = f$; $g \circ s = s \circ g = g$; and $h \circ s = s \circ h = h$. ////

EXAMPLE 3 Let $f(x) = x + 2$, $g(x) = x - 2$, and $h(x) = 3x$ for $x \in \mathbf{R}$, where $\mathbf{R}$ is the set of real numbers. Find $g \circ f$; $f \circ g$; $f \circ f$; $g \circ g$; $f \circ h$; $h \circ g$; $h \circ f$; and $f \circ h \circ g$.

SOLUTION

$$g \circ f = \{\langle x, x\rangle \mid x \in \mathbf{R}\}$$
$$f \circ g = \{\langle x, x\rangle \mid x \in \mathbf{R}\} = g \circ f$$
$$f \circ f = \{\langle x, x + 4\rangle \mid x \in \mathbf{R}\}$$
$$g \circ g = \{\langle x, x - 4\rangle \mid x \in \mathbf{R}\}$$
$$f \circ h = \{\langle x, 3x + 2\rangle \mid x \in \mathbf{R}\}$$
$$h \circ g = \{\langle x, 3x - 6\rangle \mid x \in \mathbf{R}\}$$
$$h \circ f = \{\langle x, 3x + 6\rangle \mid x \in \mathbf{R}\}$$
$$(f \circ h) \circ g = \{\langle x, 3x - 4\rangle \mid x \in \mathbf{R}\} = f \circ (h \circ g) = f \circ h \circ g \qquad ////$$

EXAMPLE 4 Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = -x^2$ and $g: \mathbf{R}_+ \to \mathbf{R}_+$ be given by $g(x) = \sqrt{x}$ where $\mathbf{R}_+$ is the set of nonnegative real numbers and $\mathbf{R}$ is the set of real numbers. Find $f \circ g$. Is $g \circ f$ defined?

SOLUTION $(f \circ g)(x) = -x$ for all $x \in \mathbf{R}_+$. The function $f \circ g: \mathbf{R}_+ \to \mathbf{R}$ is defined because the range of g is $\mathbf{R}_+ \subseteq \mathbf{R}$ and $\mathbf{R}$ is the domain of f. On the other hand, the range of f is not included in the domain of g; therefore $g \circ f$ is not defined. The only element common to R_f and D_g is $\mathbf{0}$. ////

2-4.3 Inverse Functions

The converse of a relation R from X to Y was defined in Sec. 2-3.7 to be a relation $\tilde{R}$ from Y to X such that $\langle y, x\rangle \in \tilde{R} \Leftrightarrow \langle x, y\rangle \in R$; that is, the ordered pairs of $\tilde{R}$ are obtained from those of R by simply interchanging the members. The situation is not quite the same for functions. Let $\tilde{f}$ denote the converse of f, where f is considered as a relation from $X \to Y$. Naturally $\tilde{f}$ may not be a function, first, because the domain of $\tilde{f}$ may not be Y but only a subset of Y, and second, $\tilde{f}$ may not be a function from D_f to X because it may not satisfy the uniqueness condition. For example, $\langle x_1, y\rangle$ and $\langle x_2, y\rangle$ may be in f, so that $\langle y, x_1\rangle$ and $\langle y, x_2\rangle$ will be in $\tilde{f}$. In certain special cases, $\tilde{f}$ may be a function from a subset of Y to X or even from Y to X. The following examples illustrate the situation.

1 Let $X = \{1, 2, 3\}$, $Y = \{p, q, r\}$, and $f: X \to Y$ be given by $f = \{\langle 1, p\rangle, \langle 2, q\rangle, \langle 3, q\rangle\}$. Then $\tilde{f} = \{\langle p, 1\rangle, \langle q, 2\rangle, \langle q, 3\rangle\}$ and $\tilde{f}$ is not a function.

2 Let $\mathbf{R}$ be the set of real numbers and let $f: \mathbf{R} \to \mathbf{R}$ be given by

$$f = \{\langle x, x^2\rangle \mid x \in \mathbf{R}\}$$

Then $\tilde{f} = \{\langle x^2, x\rangle \mid x \in \mathbf{R}\}$ is not a function.

3 Let $\mathbf{R}$ be the set of real numbers and let $f: \mathbf{R} \to \mathbf{R}$ be given by

$$f = \{\langle x, x + 2\rangle \mid x \in \mathbf{R}\}$$

Then $\tilde{f} = \{\langle x + 2, x\rangle \mid x \in \mathbf{R}\}$ is a function from $\mathbf{R}$ to $\mathbf{R}$.

4 Let $X = \{0, 1\}$, $Y = \{p, q, r, s\}$, and $f = \{\langle 0, p\rangle, \langle 1, r\rangle\}$. Then $\tilde{f} = \{\langle p, 0\rangle, \langle r, 1\rangle\}$ is a function from a subset of Y to X, that is, $\tilde{f}: \{p, r\} \to \{0, 1\}$.

It is easy to see that for a given $f: X \to Y$, $\tilde{f}$ is a function only if f is one-to-one. But this condition does not guarantee that $\tilde{f}$ is a function from Y to X. However, if f is one-to-one and onto, i.e., if f is bijective, then $\tilde{f}$ is a function from Y to X. In such cases, $\tilde{f}$ is written as f^{-1} so that $f^{-1}: Y \to X$ and f^{-1} is called the *inverse* of the function f. If f^{-1} exists, then f is called *invertible*. Obviously f^{-1} is also one-to-one and onto.

Definition 2-4.7 A mapping $I_x: X \to X$ is called an *identity map* if $I_x = \{\langle x, x\rangle \mid x \in X\}$.

Observe that for any function $g: X \to X$ the functions $I_x \circ g$ and $g \circ I_x$ are both equal to g. Also for any function $f: X \to Y$, we have $f \circ I_x = f$. These properties of the identity function can be used in stating the following theorems about the inverse of a function.

Theorem 2-4.1 If $f: X \to Y$ is invertible, then

$$f^{-1} \circ f = I_x \qquad \text{and} \qquad f \circ f^{-1} = I_y \tag{1}$$

Theorem 2-4.2 Let $f: X \to Y$ and $g: Y \to X$. The function g is equal to f^{-1} only if

$$g \circ f = I_x \qquad \text{and} \qquad f \circ g = I_y \tag{2}$$

Both the conditions given in (2) are necessary, as can be seen from the graphs of f and g shown in Fig. 2-4.7 where $g \circ f = I_x$ but $f \circ g \neq I_y$ and $g \neq f^{-1}$.

PROOF For a proof of Theorem 2-4.2, first we show that if there is any other function $h: Y \to X$ such that

$$h \circ f = I_x \qquad \text{and} \qquad f \circ h = I_y \tag{3}$$

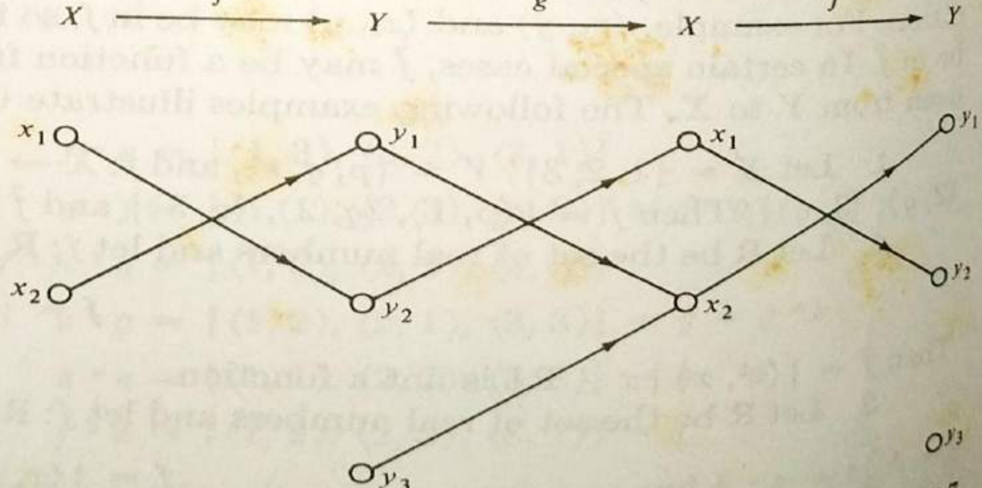


FIGURE 2-4.7

then $h = g$. Once this is proved, then $g = f^{-1}$ follows from Eq. (1). From Eqs. (2) and (3)

$$(h \circ f) \circ g = h \circ (f \circ g) = h \circ I_y = h = I_x \circ g = g$$

Let $f: X \to Y$ and $g: Y \to Z$ be such that $g \circ f: X \to Z$ can be constructed. If f and g are both one-to-one and onto, then $g \circ f$ will also be one-to-one and onto, and the inverses f^{-1}, g^{-1}, and $(g \circ f)^{-1}$ exist and are one-to-one and onto. Since $f^{-1}: Y \to X$ and $g^{-1}: Z \to Y$, we can form $f^{-1} \circ g^{-1}$. Both $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are functions from Z to X. Consider now any $x \in X$, and let $y = f(x)$ and $z = g(y)$. Thus, $\langle x, z \rangle \in g \circ f$ and $\langle z, x \rangle \in (g \circ f)^{-1}$. On the other hand, $x = f^{-1}(y)$ and $y = g^{-1}(z)$, so that $\langle z, x \rangle \in f^{-1} \circ g^{-1}$. This is true for any x, y, and z which satisfy $y = f(x)$ and $z = g(y)$; hence

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

i.e., the inverse of a composite function can be expressed in terms of the composition of the inverses in the reverse order. ////

In the remaining part of this section, we consider mappings which are bijective and from a set X onto itself. For this purpose, let F_x denote the collection of all bijective functions from X onto X, so that the elements of F_x are all invertible functions. The following properties hold.

1 For any $f, g \in F_x$, $f \circ g$, and $g \circ f$ are also in F_x. This is called the closure property of the operation of composition, which is discussed in Sec. 2-4.4.

2 For any $f, g, h \in F_x$,

$$(f \circ g) \circ h = f \circ (g \circ h)$$

i.e., composition is associative.

3 There exists a function $I_x \in F_x$ called the *identity map* such that for any $f \in F_x$

$$I_x \circ f = f \circ I_x = f$$

4 For every $f \in F_x$, there exists an inverse function $f^{-1} \in F_x$ such that

$$f \circ f^{-1} = f^{-1} \circ f = I_x$$

In fact, (1) and (2) hold for all the elements of X^X, that is, for all the functions from X to X and not only for the elements of F_x.

EXAMPLE 1 Show that the functions $f(x) = x^3$ and $g(x) = x^{1/3}$ for $x \in \mathbf{R}$ are inverses of one another.

SOLUTION Since $(f \circ g)(x) = f(x^{1/3}) = x = I_x$ and $(g \circ f)(x) = g(x^3) = x = I_x$, then $f = g^{-1}$ or $g = f^{-1}$. ////

EXAMPLE 2 Let F_x be the set of all one-to-one onto mappings from X onto X, where $X = \{1, 2, 3\}$. Find all the elements of F_x and find the inverse of each element.

SOLUTION The graphs of functions shown in Fig. 2-4.8 represent the elements of $F_x = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$,

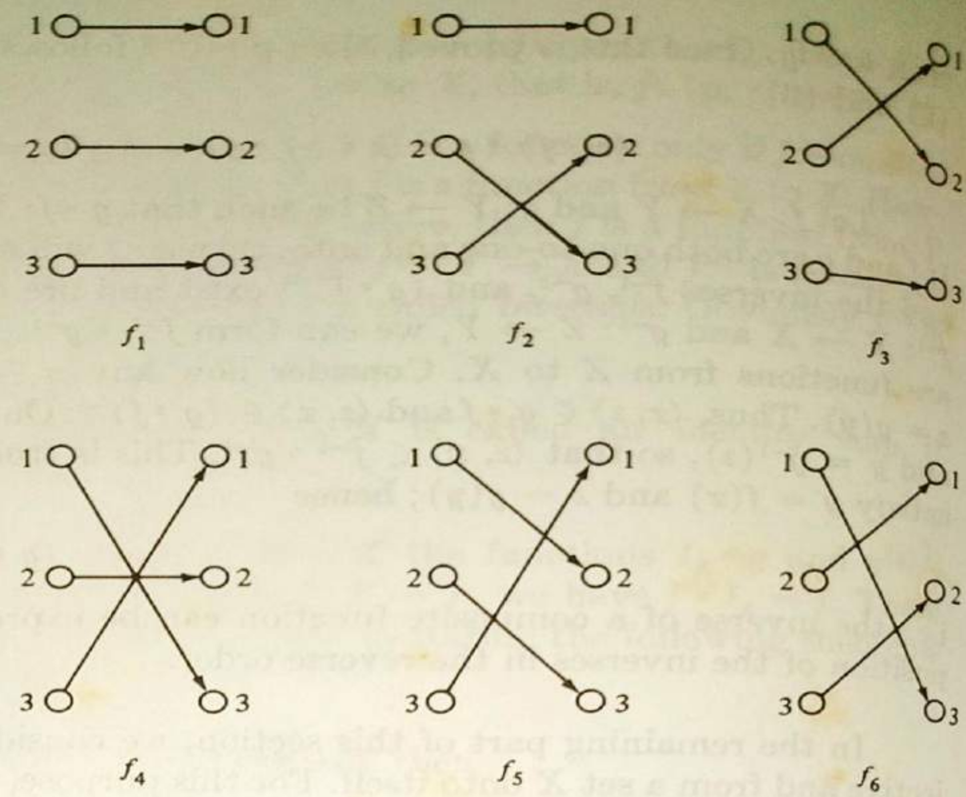


FIGURE 2-4.8

Table 2-4.1

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

and $f_5^{-1} = f_6$. Other compositions of the elements of F_x are given in Table 2-4.1, in which $f_i \circ f_j$ is entered at the intersection of the ith row and jth column. ////

The functions defined in Example 2 show the permutations of the elements of the set X. There are $3! = 6$ such permutations of 3 elements, and hence there are 6 functions from X to X which are bijective. If a set X has n elements, then there are $n!$ functions from X to X which are bijective.

EXERCISES 2-4.3

1 Let $f: \mathbf{R} \to \mathbf{R}$ and $g: \mathbf{R} \to \mathbf{R}$, where $\mathbf{R}$ is the set of real numbers. Find $f \circ g$ and $g \circ f$, where $f(x) = x^2 - 2$ and $g(x) = x + 4$. State whether these functions are injective, surjective, and bijective.

2 If $f: X \to Y$ and $g: Y \to Z$ and both f and g are onto, show that $g \circ f$ is also onto. Is $g \circ f$ one-to-one if both g and f are one-to-one?

3 Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = x^3 - 2$. Find f^{-1}.

4 How many functions are there from X to Y for the sets given below? Find also the number of functions which are one-to-one, onto, and one-to-one onto.

(a) $X = \{1, 2, 3\}$ $\quad Y = \{1, 2, 3\}$

(b) $X = \{1, 2, 3, 4\}$ $\quad Y = \{1, 2, 3\}$

(c) $X = \{1, 2, 3\}$ $\quad Y = \{1, 2, 3, 4\}$

5 Show that there exists a one-to-one mapping from $A \times B$ to $B \times A$. Is it also onto?

6 Let $X = \{1, 2, 3, 4\}$. Define a function $f: X \to X$ such that $f \neq I_x$ and is one-to-one. Find $f \circ f = f^2$, $f^3 = f \circ f^2$, f^{-1}, and $f \circ f^{-1}$. Can you find another one-to-one function $g: X \to X$ such that $g \neq I_x$ but $g \circ g = I_x$?

2-4.4 Binary and n-ary Operations

In Sec. 2-4.1 we discussed functions from a set X to a set Y. Now we restrict our discussion to functions from a set $X \times X$ to X, or more generally to functions from X^n to X, where $n = 1, 2, \ldots$. Such a mapping prescribes a unique value in X to every ordered pair or n-tuple whose members are also in X.

Definition 2-4.8 Let X be a set and f be a mapping $f: X \times X \to X$. Then f is called a *binary operation* on X. In general, a mapping $f: X^n \to X$ is called an *n-ary operation* and n is called the *order* of the operation. For $n = 1$, $f: X \to X$ is called a *unary* operation.

If an operation (or a mapping) on the members of a set produces images which are also members of the same set, then the set is said to be *closed* under that operation, and this property is called the *closure* property. The definition of binary or n-ary operations implies that the sets on which such operations are defined are closed under these operations. This property distinguishes the binary or n-ary operations from other functions.

The operations of addition, multiplication, and subtraction are binary operations on the set of integers and also on the set of real numbers. The operation of division is not a binary operation on these sets. Operations of set union and intersection are binary operations on the set of subsets of a universal set. They are also binary operations on the power set of any set. The operation of complementation (absolute or relative) is a unary operation on such sets. The operations of conjunction and disjunction are binary operations on the set of statements as well as on the set of statement formulas in statement logic. The operation of negation is a unary operation on such sets. Another example of a binary operation is the composition of bijective functions from a set X to X.

Sometimes a binary operation can be conveniently specified by a table called the composition table. Such a table was given in Example 2 of the previous subsection. The composition tables for the binary operations of union and intersection over the power set $\rho(A) = \{B_0, B_1, B_2, B_3\}$, where $A = \{a, b\}$, are given in Table 2-4.2 where $B_0 = \varnothing$, $B_1 = \{b\}$, $B_2 = \{a\}$, and $B_3 = \{a, b\} = A$.

It is customary to denote a binary operation by a symbol such as $+$, $-$, $\circ$, $*$, $\triangle$, $\cup$, $\cap$, $\vee$, $\wedge$, etc., and the value of the operation (or function) by placing the operator between the two operands. For example, $f\langle x, y\rangle$ may be written as $x\,f\,y$ or $x * y$. A similar notation is used in arithmetic where we write the

Table 2-4.2

∪	B_0	B_1	B_2	B_3
B_0	B_0	B_1	B_2	B_3
B_1	B_1	B_1	B_3	B_3
B_2	B_2	B_3	B_2	B_3
B_3	B_3	B_3	B_3	B_3

∩	B_0	B_1	B_2	B_3
B_0	B_0	B_0	B_0	B_0
B_1	B_0	B_1	B_0	B_1
B_2	B_0	B_0	B_2	B_2
B_3	B_0	B_1	B_2	B_3

sum of two real numbers x and y as $x + y$. Also in set theory the union of two sets A and B is written as $A \cup B$.

Now we discuss some general properties of binary operations. For this purpose we shall consider X to be any set.

Definition 2-4.9 A binary operation $f: X \times X \to X$ is said to be *commutative* if for every $x, y \in X$,

$$f\langle x, y\rangle = f\langle y, x\rangle$$

Definition 2-4.10 A binary operation $f: X \times X \to X$ is said to be *associative* if for every $x, y, z \in X$,

$$f\langle f\langle x, y\rangle, z\rangle = f\langle x, f\langle y, z\rangle\rangle$$

Definitions 2-4.9 and 2-4.10 can be rewritten using $*$ to denote the binary relation on X. That is, $*$ is commutative if for any $x, y \in X$, $x * y = y * x$. Similarly $*$ is associative on X if for any $x, y, z \in X$,

$$(x * y) * z = x * (y * z)$$

Definition 2-4.11 A binary operation $f: X \times X \to X$ is said to be *distributive* over the operation $g: X \times X \to X$ if for every $x, y, z \in X$

$$f\langle x, g\langle y, z\rangle\rangle = g\langle f\langle x, y\rangle, f\langle x, z\rangle\rangle$$

If we denote f by $*$ and g by $\circ$ we say $*$ is distributive over $\circ$ if for any $x, y, z \in X$

$$x * (y \circ z) = (x * y) \circ (x * z)$$

The operations of addition and multiplication over the set of real numbers are commutative and associative. Union and intersection over the power set of any set are other examples of commutative and associative operations. The operation of subtraction over the set of real numbers is not commutative. It was also shown that the composition of bijective functions from a set X to X is not commutative. The operation of multiplication is distributive over that of addition. Both union and intersection of sets distribute over each other.

Given a binary operation $*$ on a set X, we now define certain distinguished elements of X which are associated with the operation. Such elements may or may not exist.

Definition 2-4.12 Let $*$ be a binary operation on X. If there exists an element $e_l \in X$ such that $e_l * x = x$ for every $x \in X$, then e_l is called a *left identity* with respect to $*$. Similarly, if there exists an element $e_r \in X$ such that $x * e_r = x$ for every $x \in X$, then e_r is called a *right identity* with respect to $*$.

We now give a theorem which relates left and right identities if both of them exist.

Theorem 2-4.3 Let $*$ be a binary operation, and let e_l and e_r be left and right identities with respect to $*$. Then $e_l = e_r = e$ (say), such that $e * x = x * e = x$ for every $x \in X$, and in such a case $e \in X$ is unique and is called the *identity* with respect to $*$.

PROOF Since e_l and e_r are left and right identities,

$$e_l * e_r = e_l = e_r$$

Next, let us assume e_1 and e_2 are two distinct identities. Then

$$e_1 * e_2 = e_1 = e_2$$

which is a contradiction; hence an identity, if it exists, is unique. ////

For a commutative binary operation, a left identity is also a right identity, and hence any left or right identity is the identity.

The element 0 is the identity for addition, and 1 is the identity for multiplication over a set of real numbers. Similarly the empty set $\varnothing$ is the identity for the operation of union, and the universal set E is the identity for the operation of intersection over the subsets of a universal set. The identity mapping defined in Sec. 2-4.3 is the identity with respect to composition of bijective functions from a set X to X. A contradiction, i.e., an identically false statement, is an identity for disjunction, while a tautology is an identity for conjunction of statements.

Definition 2-4.13 Let $*$ be a binary operation on X. If there exists an element $0_l \in X$ such that $0_l * x = 0_l$ for every $x \in X$, then 0_l is called a *left zero* with respect to $*$. Similarly, if there exists an element $0_r \in X$ such that $x * 0_r = 0_r$ for every $x \in X$, then 0_r is called a *right zero* with respect to $*$.

A theorem similar to Theorem 2-4.3 can now be given.

Theorem 2-4.4 Let $*$ be a binary operation, and 0_l and 0_r be left and right zeros with respect to $*$. Then $0_l = 0_r = 0$ such that

$$0 * x = x * 0 = 0 \qquad \text{for all } x \in X$$

$0 \in X$ is unique and is called the *zero* with respect to $*$.

The element 0 is the zero for multiplication on a set of real numbers. The empty set $\varnothing$ is the zero for intersection, and the universal set E is the zero for the union of subsets of a universal set.

Definition 2-4.14 Let $*$ be a binary operation on X. An element $a \in X$ is called *idempotent* with respect to $*$ if $a * a = a$.

The identity and zero elements with respect to a binary operation are idempotent. There may be other idempotent elements besides the identity and zero elements. For example, every set is idempotent with respect to the operations of union and intersection.

Definition 2-4.15 Let $*$ be a binary operation on X with the identity e. An element $a \in X$ is said to be *left-invertible* if there exists an element $x_l \in X$ such that $x_l * a = e$. x_l is called a *left inverse* of a. Similarly, $a \in X$ is said to be *right-invertible* if there exists an element $x_r \in X$ such that $a * x_r = e$. x_r is called a *right inverse* of a. If an element $a \in X$ is both left-invertible and right-invertible, then a is called *invertible*.

Obviously, if a binary operation $*$ on X with the identity e is commutative, then any element that is left- or right-invertible is invertible. For operations which are associative, we can prove the following theorem.

Theorem 2-4.5 Let $*$ be a binary operation on X which is associative and which has the identity $e \in X$. If an element $a \in X$ is invertible, then both its left and right inverses are equal. Such an element is called the inverse of a because it is unique.

PROOF Let x_l and x_r be any left and right inverses of a respectively. We show that $x_l = x_r$ as follows.

$$x_l * a = a * x_r = e$$

hence

$$x_l * a * x_r = (x_l * a) * x_r = x_l * (a * x_r) = e * x_r = x_r = x_l * e = x_l$$

Here we have used the associativity of the operation $*$.

To show uniqueness, let us assume that x and y are two distinct inverses of a. Thus

$$y = y * e = y * (a * x) = (y * a) * x = e * x = x$$

which is a contradiction. ////

The unique inverse of an element $a \in X$, if it exists, is denoted by a^{-1}, so that

$$a^{-1} * a = a * a^{-1} = e$$

From symmetry it follows that $(a^{-1})^{-1} = a$.

In any binary operation the identity element, if it exists, is invertible. Since it is also idempotent, the identity is its own inverse. Other invertible elements may or may not exist. For example, every real number $a \in \mathbf{R}$ has an inverse $-a \in \mathbf{R}$ for the operation of addition. Similarly, for the operation of multiplication, the inverse of every nonzero real number $a \in \mathbf{R}$ is $1/a \in \mathbf{R}$. For a set A which is a subset of a universal set, the set A is idempotent for the operations of union as well as intersection. In Example 2 of Sec. 2-4.3, all the functions are invertible for the operation of composition. It may be noted that a zero element with respect to an operation cannot be invertible.

Definition 2-4.16 An element $a \in X$ is called *cancellable* with respect to a binary operation $*$ on X, if for every $x, y \in X$,

$$(a * x = a * y) \vee (x * a = y * a) \Rightarrow (x = y)$$

If the operation $*$ is associative and the element $a \in X$ is invertible, then a is cancellable. However, there are cases where an element is cancellable but not necessarily invertible. For example, in the set of integers any nonzero integer is cancellable with respect to the operation of multiplication, although the only integer which is invertible is the identity, that is, 1.

The properties of binary operations given here are used in Chaps. 3 and 4. We have not discussed n-ary operations in general because we will be most concerned with unary and binary operations.

Given a set X and a binary operation $*$ on X, we have represented the value of the binary operation $*$ on any two elements $x, y \in X$ by writing $x * y$. Since $x * y \in X$, we may again apply the same or any other binary operation, say $+$, on $x * y$ and an element of X, say z. Obviously the following possibilities exist:

$$(x * y) * z \qquad z * (x * y) \qquad (x * y) + z \qquad z + (x * y)$$

The parentheses have been used in the usual sense to indicate that in all these cases $x * y$ is obtained first. If the operation $*$ is associative, then $(x * y) * z = x * (y * z)$, and we may drop the parentheses. In other words, the order in which the two binary operations are carried out is not important. Sometimes the parentheses are dropped even though the operation is not associative. In such cases, a convention is adopted regarding the order in which the operations are performed. For example, in a computer program using FORTRAN, A + B + C is understood to be (A + B) + C. Note that (A + B) + C may not be equal to A + (B + C) due to rounding-off operations on a computer. In any case, we say that the operation + is assumed to be left-associative. In the case of the assignment A ← B, we understand A ← (B ← C), that is, the operation is right-associative. Similarly for a logical expression $\neg\neg P$, it is assumed that we have $\neg(\neg P)$, where $\neg P$ is formed first. Since subtraction is not associative, we write (A − B) − C as distinct from A − (B − C). However, in FORTRAN A − B − C is understood to mean (A − B) − C, and so subtraction is left-associative. It is very important to know whether an operation is understood to be left- or right-associative. This need to know is greater in the case of programming languages than in mathematics where parentheses are always used except when an operation is associative.

EXERCISES 2-4.4

1 Let $g: \mathbf{I} \times \mathbf{I} \rightarrow \mathbf{I}$ where $\mathbf{I}$ is the set of integers and

$$g\langle x, y\rangle = x * y = x + y - xy$$

Show that the binary operation $*$ is commutative and associative. Find the identity element and indicate the inverse of each element.

2 Let $*$ denote a binary operation on the set of natural numbers given by $x * y = x$. Show that $*$ is not commutative, but is associative. Which elements are idempotent? Are there any left or right identities?

3 Let $x * y =$ lowest common multiple of x and y, where $*$ is a binary operation on the set of positive integers. Show that $*$ is commutative and associative. Find the identity element and also state which elements are idempotent.

4 Let $\mathbf{I}_p = \{0, 1, 2, \ldots, p-1\}$. The operations $+_p$ and $*_p$ are given by $x +_p y = (x + y) \pmod p$ and $x *_p y = xy \pmod p$. Give composition tables for these operations for $p = 3$ and 4. Indicate the identity and zero elements. Does the operation $*_p$ distribute over $+_p$?

5 Show that $x * y = x - y$ is not a binary operation over the set of natural numbers, but that it is a binary operation on the set of integers. Is it commutative or associative?

6 Show that $x * y = x^y$ is a binary operation on the set of positive integers. Determine whether $*$ is commutative or associative.

7 How many distinct binary operations are there on the set $\{0, 1\}$? Give their composition tables and indicate which ones are commutative or associative. Can you determine the number of distinct binary operations on any finite set?

2-4.5 Characteristic Function of a Set

In this section we shall discuss functions from the universal set E to the set $\{0, 1\}$. These functions are associated with sets in the same way as the principle of specification given in Sec. 2-1.7. A one-to-one correspondence is established between these functions and the sets. With the use of these functions, statements about sets and their operations can be represented on a computer in terms of binary numbers; hence their manipulation becomes easier.

Definition 2-4.17 Let E be a universal set and A be a subset of E. The function $\psi_A: E \rightarrow \{0, 1\}$ defined by

$$\psi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

is called the *characteristic function* of the set A.

As an example, let E be the set of all persons living in Toronto and let F be the set of all females in Toronto. Then ψ_F associates the number 1 with each female and 0 with each male in Toronto.

The following properties suggest how one can use the characteristic functions of sets to determine set relations.

Let A and B be any two subsets of a universal set E. Then the following hold for all $x \in E$.

$$\psi_A(x) = 0 \Leftrightarrow A = \varnothing \tag{1}$$
$$\psi_A(x) = 1 \Leftrightarrow A = E \tag{2}$$
$$\psi_A(x) \leq \psi_B(x) \Leftrightarrow A \subseteq B \tag{3}$$
$$\psi_A(x) = \psi_B(x) \Leftrightarrow A = B \tag{4}$$
$$\psi_{A \cap B}(x) = \psi_A(x) * \psi_B(x) \tag{5}$$
$$\psi_{A \cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A \cap B}(x) \tag{6}$$
$$\psi_{\sim A}(x) = 1 - \psi_A(x) \tag{7}$$
$$\psi_{A-B}(x) = \psi_{A \cap \sim B}(x) = \psi_A(x) - \psi_{A \cap B}(x) \tag{8}$$

Note that the operations $\leq$, $=$, $+$, $*$, and $-$ used with the characteristic functions are the usual arithmetic operations because the values of the characteristic functions are always either 1 or 0. On the other hand, the equality used for sets is the usual set equality. Other set operations used above are $\cup$, $\cap$, $\sim$, and $-$. The above properties can easily be proved using the definition of characteristic functions. For example, (5) can be proved as follows:

$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$, so that $\psi_A(x) = 1$ and $\psi_B(x) = 1$ and $\psi_{A \cap B}(x) = 1 * 1 = 1$. If $x \notin A \cap B$, then $\psi_{A \cap B}(x) = 0$ and $\psi_A(x) = 0$ or $\psi_B(x) = 0$. Consequently $\psi_A(x) * \psi_B(x) = 0$.

Many set identities and other relations can be proved by using characteristic functions and the usual arithmetic operations and relations.

EXAMPLE 1 Show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

SOLUTION

$$\begin{aligned}
\psi_{A \cap (B \cup C)}(x) &= \psi_A(x) * \psi_{B \cup C}(x) && \text{(using 5)}\\
&= \psi_A(x)\,(\psi_B(x) + \psi_C(x) - \psi_{B \cap C}(x)) && \text{(using 6)}\\
&= \psi_A(x) * \psi_B(x) + \psi_A(x) * \psi_C(x)\\
&\quad - \psi_A(x) * \psi_{B \cap C}(x)\\
&= \psi_{A \cap B}(x) + \psi_{A \cap C}(x) - \psi_{A \cap (B \cap C)}(x) && \text{(using 5)}\\
&= \psi_{A \cap B}(x) + \psi_{A \cap C}(x) - \psi_{A \cap B \cap C}(x)\\
&= \psi_{A \cap B}(x) + \psi_{A \cap C}(x) - \psi_{(A \cap B) \cap (A \cap C)}(x)\\
&= \psi_{(A \cap B) \cup (A \cap C)}(x) && \text{(using 6)}
\end{aligned}$$

////

EXAMPLE 2 Show that $\sim\sim A = A$.

SOLUTION

$$\begin{aligned}
\psi_{\sim\sim A}(x) &= 1 - \psi_{\sim A}(x)\\
&= 1 - (1 - \psi_A(x)) && \text{(using 7)}\\
&= \psi_A(x)
\end{aligned}$$

////

The notation used for naming the subsets of a finite set introduced earlier in Sec. 2-1.3 can now be explained by using the characteristic function. Consider $E = \{a, b, c\}$. The subsets of E are $\varnothing$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, and $\{a, b, c\}$. The values of the characteristic functions of these subsets are given in Table 2-4.3. The values of the characteristic function of any of the subsets of E consist of three binary digits or binary triples. If we let

$$B = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

then Table 2-4.3 can be considered as a mapping from the power set of E to B. This mapping is one-to-one and onto and hence describes a one-to-one correspondence between the sets $\rho(E)$ and B. The elements of B were used to denote the corresponding subsets.

Consider a universal set E and a mapping f from the set E to a finite set $\{a_1, a_2, \ldots, a_n\}$ where $a_1, a_2, \ldots, a_n$ are all distinct. Let A_1 be the set of elements of E such that $f(x) = a_1$ for $x \in A_1$. Similarly define the subsets $A_2, A_3, \ldots, A_n$ of E. Obviously, $A_1, A_2, \ldots, A_n$ are all disjoint; in addition, $A_1 \cup A_2 \cup \cdots \cup A_n = E$, that is, $A_1, A_2, \ldots, A_n$ are the blocks of a partition of E. It is possible to write

$$f(x) = \sum_{i=1}^{n} a_i * \psi_{A_i}(x)$$

A function $f(x)$ which has a finite set of possible values is called a *simple function*. Obviously the range of a simple function is a finite set. It is possible to extend the above description to functions which have countably infinite distinct values.

Finally, we consider the characteristic functions of certain sets which were called minterms, or complete intersections in Sec. 2-3.4. It was noted that the minterms generated by a finite number of sets define a partition of the universal set. Let $X_1, X_2, \ldots, X_n$ be any n subsets of a universal set E and let $I_0, I_1, \ldots, I_{2^n-1}$ be the minterms or complete intersections of $X_1, X_2, \ldots, X_n$. Any element $x \in E$ is a member of only one of the minterms. If $x \in I_j$, then $\psi_{I_j}(x) = 1$ and $\psi_{I_m}(x) = 0$ for $m \neq j$. This statement holds for any $x \in I_j$. Now let us form a new set, say F, from the sets $X_1, \ldots, X_n$ by using the operations of union, intersection, and complementation. Then the characteristic function of F will remain constant over the sets of minterms.

2-4.6 Hashing Functions

In Sec. 2-2.5 we introduced terms such as "file," "record," "field," etc., which are used frequently in connection with the storage of information on a computer. An example of a file is the symbol table of a compiler or an assembler which con-

Table 2-4.3

x	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a, b, c\}$
a	0	1	0	0	1	1	0	1
b	0	0	1	0	1	0	1	1
c	0	0	0	1	0	1	1	1

The previous algorithm is reasonably simple and requires no further comment.

The PL/I program in Fig. 2-4.10 constructs a symbol table. It consists of a hashing function, a procedure based on the preceding algorithm, and a mainline program. The hashing function finds the remainder on dividing the bit representation (obtained by using UNSPEC) of NAME by N. If NAME contains more than three characters, then only the first three are used in the process. The MOD function is used to find the remainder when NUMBER is divided by N.

The main program is written so that up to 25 equivalence classes can be handled in the symbol table. Each name to be inserted is on one input card. On an end-of-file, control transfers to the statement labeled OUTPUT. At this point, each simple linked list representing an equivalence class is scanned, and each name in it is printed.

EXERCISES 2-4.6

1 The midsquare hashing method follows:

(*a*) Square part of the key, or the whole key if possible.

(*b*) Either (1) extract n digits from the middle of the result to give $h(\text{key}) \in \{0, 1, \ldots, 10^n - 1\}$, or (2) extract n bits from the middle of the result to give $h(\text{key}) \in \{0, 1, \ldots, 2^n - 1\}$.

Write a program which uses this procedure to hash a set of variable names. The midsquare method frequently gives satisfactory results, but in many cases the keys are unevenly distributed over the required range.

2 A hashing method often implemented, called *folding*, is performed by dividing the key into several parts and adding the parts to form a number in the required range. For example, if we have 8-digit keys and wish to obtain a 3-digit address, we may do the following:

$$h(97434658) = 974 + 346 + 58 = 378$$

$$h(31269857) = 312 + 698 + 57 = 67$$

Note that the final carry is ignored.

Implement this method in a computer program.

3 Compare the results of applying the division, midsquare, and folding hashing functions to a fixed set of keys. Make sure the range is the same or almost the same in each case. Which method distributes the keys most evenly over the elements of the range?

EXERCISES 2-4

1 Show that

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

$$f(A \cap B) \subseteq f(A) \cap f(B)$$

Construct an example to show that in general it is not possible to replace $\subseteq$ by $=$ in the second relation. Under what condition will $f(A \cap B) = f(A) \cap f(B)$?

2 Show that $f: X \to Y$ is one-to-one iff any proper subsets of X are mapped into proper subsets of Y; that is, if $A \subset B \subseteq X$, then $f(A) \subset f(B) \subseteq Y$.

3 Let $\mathbf{I}_p = \{0, 1, \ldots, p-1\}$ and $f_r: \mathbf{I}_p \to \mathbf{I}_p$ be given by

$$f_r(x) = rx \pmod p$$

where $r = 0, 1, \ldots, p-1$. Show that f is not bijective for any r unless p is prime.

4 Determine the set of all bijective mappings on the set $\{1, 2\}$. Determine the identity element and inverses of each element under the composition of functions on this set.

5 Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = x^2$ and $g: \mathbf{R} - \{2\} \to \mathbf{R}$ be given by $g(x) = x/(x-2)$. Find $f \circ g$. Is $g \circ f$ defined?

6 Let X be a set and $\rho(X)$ its power set. Show that the operations of union and intersection on $\rho(X)$ are both associative and commutative. Also every element of $\rho(X)$ is idempotent under these operations. Determine the zeroes, and show that the operations distribute over each other.

7 Show that the operation of symmetric difference $\triangle$ defined by

$$A \triangle B = (A \cup B) - (A \cap B)$$

is commutative and associative and has an identity element. Show that the inverse of A is A itself. Show that the operation of intersection, but not that of union, distributes over $\triangle$.

8 Consider the set $\mathbf{I}_+$ of positive integers and let $\mathbf{N}$ be the set of natural numbers (including zero). Observe that for any $x \in \mathbf{I}_+$ we have

$$x = 2^r(2s + 1)$$

for some r, s $\mathbf{N}$. This means that we can define a mapping $f: \mathbf{I}_+ \to \mathbf{N} \times \mathbf{N}$ such $f(x) = \langle r, s \rangle$, as indicated above. Show that f is one-to-one onto.