Chapter 5

Further Theory of Sets and Functions

5.1 INTRODUCTION

This chapter investigates some additional properties of sets and functions including set operations on collections of sets and indexed sets. We also discuss the notion of a diagram of functions.

5.2 OPERATIONS ON COLLECTIONS OF SETS

Let $\mathscr{A}$ be a collection of sets. The *union* of $\mathscr{A}$, denoted by

$$\bigcup\{A : A \in \mathscr{A}\} \qquad \text{or} \qquad \bigcup_{A \in \mathscr{A}} A \qquad \text{or simply} \qquad \bigcup \mathscr{A}$$

consists of all elements x such that x belongs to at least one set in $\mathscr{A}$; that is,

$$\bigcup\{A : A \in \mathscr{A}\} = \{x : x \in A \text{ for some } A \text{ in } \mathscr{A}\}$$

Analogously, the *intersection* of $\mathscr{A}$, denoted by

$$\bigcap\{A : A \in \mathscr{A}\} \qquad \text{or} \qquad \bigcap_{A \in \mathscr{A}} A \qquad \text{or simply} \qquad \bigcap \mathscr{A}$$

consists of all elements x such that x belongs to all the sets in $\mathscr{A}$; that is,

$$\bigcap\{A : A \in \mathscr{A}\} = \{x : x \in A \text{ for every } A \text{ in } \mathscr{A}\}$$

If $\mathscr{A}$ is empty, then we do not define the intersection of $\mathscr{A}$. In case $\mathscr{A}$ is nonempty and finite, then the above are just the same as our previous definitions of union and intersection.

EXAMPLE 5.1

(*a*) Let $\mathscr{A} = [\{1,2,3\},\ \{2,3,4\},\ \{2,3,5\}]$. Then

$$\bigcup \mathscr{A} = \{1,2,3,4,5\} \qquad \text{and} \qquad \bigcap \mathscr{A} = \{2,3\}$$

(*b*) Let A be any set and let $\mathscr{P} = \mathscr{P}(A)$ be the power set of A. Then:

$$\bigcup \mathscr{P} = A \qquad \text{and} \qquad \bigcap \mathscr{P} = \varnothing$$

(*c*) Let $\mathscr{A} = \{[-1,1],\ [-2,2],\ [-3,3],\ \ldots,\ [-n,n],\ \ldots\}$. Then

$$\bigcup \mathscr{A} = R \qquad \text{and} \qquad \bigcap \mathscr{A} = [-1,1]$$

5.3 INDEXED COLLECTIONS OF SETS

Algebraic properties of unions and intersections are usually presented in the context of one of the main ways of designating collections of sets, that is, as indexed collections of sets. Such collections of sets and the set operations on them are discussed in this section.

Indexed Collections of Sets

Let I be any nonempty set, and let $\mathscr{L}$ be a collection of sets. An *indexing function* from I to $\mathscr{L}$ is a function $f\colon I \to \mathscr{L}$. For any $i \in I$, we denote the image $f(i)$ by A_i. Thus the indexing function f is usually denoted by

$$\{A_i\colon i \in I\} \qquad \text{or} \qquad \{A_i\}_{i\in I} \qquad \text{or simply} \qquad \{A_i\}$$

The set I is called the *indexing set*, and the elements of I are called *indices*. If f is bijective, that is, one-to-one and onto, then we say that $\mathscr{L}$ is indexed by I.

Remark: Any nonempty collection $\mathscr{A}$ of distinct sets may be viewed as an indexed collection of sets by letting $\mathscr{A}$ be indexed by itself. Thus a collection of sets is usually given in the form $\{A_i\colon i \in I\}$, that is, as an indexed collection of sets.

Operations on Indexed Collections of Sets

Consider any indexed collection $\{A_i : i \in I\}$ of sets. The *union* of the collection $\{A_i : i \in I\}$, denoted by

$$\bigcup\{A_i : i \in I\} \qquad \text{or} \qquad \bigcup_{i\in I} A_i \qquad \text{or simply} \qquad \bigcup{}_i A_i$$

consists of those elements which belong to at least one of the A_i. Namely,

$$\bigcup\{A_i : i \in I\} = \{x : x \in A_i \text{ for some } i \in I\}$$

Analogously, the *intersection* of a collection set $\{A_i : i \in I\}$, denoted by

$$\bigcap\{A_i : i \in I\} \qquad \text{or} \qquad \bigcap{}_{i\in I} A_i \qquad \text{or, simply} \qquad \bigcap{}_i A_i$$

consists of those elements which belong to every A_i. Namely,

$$\bigcap\{A_i : i \in I\} = \{x : x \in A_i \text{ for every } i \in I\}$$

In the case that I is a finite set, this is just the same as our previous definitions of union and intersection.

Suppose the indexing set I is the set $\mathbf{P}$ of positive integers. Then $\{A_i\}$ is called a *sequence of sets*, usually denoted by $A_1, A_2, A_3, \ldots$, and the union and intersection of the sets may be denoted by

$$A_1 \cup A_2 \cup \cdots \qquad \text{and} \qquad A_1 \cap A_2 \cap \cdots$$

respectively.

Suppose $J \subseteq I$. Then the union and intersection of only those sets A_i where $i \in J$ is denoted, respectively, by

$$\bigcup\{A_i : i \in J\} \quad \text{and} \quad \bigcap\{A_i : i \in J\} \qquad \text{or} \qquad \bigcup{}_{i\in J} A_i \quad \text{and} \quad \bigcap{}_{i\in I} A_i$$

We emphasize that $\bigcup_i A_i$ and $\bigcap_i A_i$ can only be used when the entire indexing set I is used in the union and intersection.

EXAMPLE 5.2

(*a*) Let I be the set $\mathbf{Z}$ of integers. To each integer n we assign the following subset of $\mathbf{R}$:

$$A_n = \{x : x \leq n\}$$

In other words, A_n is the infinite interval $(-\infty, n]$. For any real number a, there exist integers n_1 and n_2 such that $n_1 < a < n_2$. Hence

$$a \in \bigcup{}_n A_n \qquad \text{but} \qquad a \notin \bigcap{}_n A_n$$

Accordingly,

$$\bigcup{}_n A_n = \mathbf{R} \qquad \text{but} \qquad \bigcap{}_n A_n = \varnothing$$

(*b*) Let $I = \{1, 2, 3, 4, 5\}$ and $J = \{2, 3, 5\}$, and let

$$A_1 = \{1, 9\}, \qquad A_2 = \{2, 4, 6, 9\}, \qquad A_3 = \{3, 6, 7, 9\}, \qquad A_4 = \{4, 8\}, \qquad A_5 = \{5, 6, 9\}$$

Then

$$\bigcap_i A_i = \varnothing \qquad \text{and} \qquad \bigcup_i A_i = \{1, 2, \ldots, 9\}$$

However,

$$\bigcap_{i \in J} A_i = \{6, 9\} \qquad \text{and} \qquad \bigcup_{i \in J} A_i = \{2, 3, 4, 5, 6, 7, 9\}$$

The following theorem tells us, in particular, that the distributive laws and DeMorgan's law in Table 1-1 can be generalized to apply to indexed collections of sets.

Theorem 5.1: Let B and $\{A_i\}$ with $i \in I$ be subsets of a universal set $\mathbf{U}$. Then:

(i) $B \cap (\cup\{A_i\}) = \cup\{B \cap A_i\}$ and $B \cup (\cap\{A_i\}) = \cap\{B \cup A_i\}$.

(ii) $(\cup\{A_i\})^c = \cap\{A_i^c\}$ and $(\cap\{A_i\})^c = \cup\{A_i^c\}$.

(iii) If J is a subset of I, then

$$\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i \qquad \text{and} \qquad \bigcap_{i \in J} A_i \supseteq \bigcap_{i \in I} A_i$$

Since the empty set $\varnothing$ is a subset of any set, Theorem 5.1(iii) should imply that the empty intersection contains any set A_i. Accordingly, one sometimes defines

$$\bigcap_{\varnothing} A_i = \mathbf{U}$$

This may seem strange, but it is similar to defining $0! = 1$ and $a^0 = 1$ in order for general properties to be true.

We also note that Theorem 5.1(i) and (ii) apply to any collection $\mathscr{A}$ of sets.

5.4 SEQUENCES, SUMMATION SYMBOL

A *sequence* is a function from the set $\mathbf{P}$ of positive integers into a set A. The notation a_n is used to denote the image of the integer k. Thus a sequence is usually denoted by

$$a_1, a_2, a_3, \ldots \qquad \text{or} \qquad \{a_n : n \in \mathbf{P}\} \qquad \text{or simply} \qquad \{a_n\}$$

Sometimes the domain of a sequence is the set $\mathbf{N} = \{0, 1, 2, \ldots\}$ of nonnegative integers rather than $\mathbf{P}$. In such a case we say that n *begins* with 0 rather than 1.

A *finite sequence* over a set A is a function from $\{1, 2, \ldots, m\}$ into A, and it is usually denoted by

$$a_1, a_2, \ldots, a_m$$

Such a finite sequence is sometimes called a *list* or an *m-tuple*.

EXAMPLE 5.3

(*a*) The familiar sequences

$$1, 1/2, 1/3, 1/4, \ldots \qquad \text{and} \qquad 1, 1/2, 1/4, 1/8, \ldots$$

may be formally defined, respectively, by

$$a_n = 1/n \qquad \text{and} \qquad b_n = 2^{-n}$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*b*) The important sequence $1, -1, 1, -1, \ldots$ may be formally defined by

$$a_n = (-1)^{n+1} \qquad \text{or, equivalently, by} \qquad b_n = (-1)^n$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*c*) (*Strings*): Suppose a set A is finite and A is viewed as a character set or an alphabet. Then a finite sequence over A is called a *string* or *word*, and it is usually written in the form $a_1a_2 \dots a_m$, that is, without parentheses. The number m of characters in the string is called its *length*. One also views the set with zero characters as a string; it is called the *empty string* or *null string*.

Summation Symbol, Sums

Consider a sequence $a_1, a_2, a_3, \dots$. Frequently we want to form sums of elements from the sequence. Such sums may sometimes be conveniently represented using the summation symbol Σ (the Greek letter sigma). Specifically, the sums

$$a_1 + a_2 + a_3 + \cdots + a_n \qquad \text{and} \qquad a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

will be denoted, respectively, by

$$\sum_{j=1}^{n} a_j \qquad \text{and} \qquad \sum_{j=m}^{n} a_j$$

The letter j in the above expression is called a *dummy index* or *dummy variable*. Other letters frequently used as dummy variables are i, k, s, and t.

EXAMPLE 5.4

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

The last sum in Example 5.4 appears often. It has the value $n(n+1)/2$. Namely,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Thus, for example,

$$1 + 2 + 3 + \cdots + 50 = \frac{50(51)}{2} = 1275$$

The formula may be proved using mathematical induction.

5.5 FUNDAMENTAL PRODUCTS

Consider a list $A_1, A_2, \dots, A_n$ of n sets. A *fundamental product* of the sets is a set of the form

$$A_1^* \cap A_2^* \cap \cdots \cap A_m^*$$

where A_i^* is either A_i or A_i^c. We note that there are 2^n such fundamental products since there is a choice of two sets for each A_i^*. One can also show (Problem 5.54) that such fundamental products are disjoint and their union is the universal set **U**.

There is a geometrical description of these fundamental products which is illustrated below.

EXAMPLE 5.5 Consider three sets A, B, C. The following lists the eight fundamental products of the three sets:

$$\begin{array}{llll} P_1 = A \cap B \cap C & P_3 = A \cap B^c \cap C & P_5 = A^n \cap B \cap C & P_7 = A^c \cap B^c \cap C \\ P_2 = A \cap B \cap C^c & P_4 = A \cap B^c \cap C^c & P_6 = A^c \cap B \cap C^c & P_8 = A^c \cap B^c \cap C^c \end{array}$$

These eight products correspond precisely to the eight disjoint regions in the Venn diagram of sets A, B, C in Fig. 5-1 as indicated by the labeling of the regions.

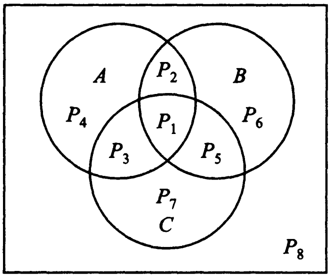

Fig. 5-1

A *Boolean expression* in the sets $A_1, A_2, \ldots, A_n$ is an expression $E = E(A_1, A_2, \ldots, A_n)$ which is built up from the sets using the operations of union, intersection, and complement. For example,

$$E_1 = (A \cup B^c)^c \cap (A^c \cap C)^c \cap (B^c \cup C) \qquad \text{and} \qquad E_2 = [(A \cap B^c) \cup (B^c \cap C)]^c$$

are Boolean expressions in the sets A, B, C.

The following theorem applies.

Theorem 5.2: Any Boolean expression $E = E(A_1, A_2, \ldots, A_n)$ is equal to the empty set $\varnothing$ or the unique union of a finite number of fundamental products.

This theorem is a special case of Theorem 11.8 on Boolean algebras. So its proof appears there. We indicate a geometrical interpretation here.

Consider sets A, B, C. Then any Boolean expression $E = E(A, B, C)$ will be uniquely represented by a finite number of regions in the Venn diagram in Fig. 5-1. Thus $E = E(A, B, C)$ is either the empty set or the union of one or more of the eight fundamental products in Fig. 5-1.

5.6 FUNCTIONS AND DIAGRAMS

Recall that we used the following diagram to represent functions $f\colon A \to B$ and $g\colon B \to C$:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$$

Similarly, the following diagram represents functions $f\colon A \to B$, $g\colon B \to C$, and $h\colon A \to C$:

$$\begin{tikzcd} A \arrow[rr, "h"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

Note that the diagram defines two functions from A to C, the function h represented by a single arrow, and the composition function $g \circ f$ represented by a sequence of two connected arrows. Each arrow or sequence of arrows connecting A to C is called a *path* from A to C.

Definition: A diagram of functions is said to be *commutative* if, for any pair of sets X and Y in the diagram, any two paths from X to Y are equal.

EXAMPLE 5.6

(*a*) Suppose the diagram of functions in Fig. 5-2(*a*) is commutative. Then:

$$i \circ h = f, \qquad g \circ i = j, \qquad g \circ f = j \circ h = g \circ i \circ h$$

(*b*) The functions $f: A \to B$ and $g: B \to A$ are inverses if and only if the diagrams in Fig. 5-2(*b*) are commutative, that is, if and only if

$$g \circ f = 1_A \qquad \text{and} \qquad f \circ g = 1_B$$

Here 1_A and 1_B are the identity functions.

$$\begin{tikzcd}
& D \arrow[d, "i"] \arrow[dr, "j"] & \\
A \arrow[ur, "h"] \arrow[r, "f"'] & B \arrow[r, "g"'] & C
\end{tikzcd}$$

(*a*)

$$\begin{tikzcd}
A \arrow[rr, "1_A"] \arrow[dr, "f"'] & & A \\
& B \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
B \arrow[rr, "1_B"] \arrow[dr, "g"'] & & B \\
& A \arrow[ur, "f"'] &
\end{tikzcd}$$

(*b*)

Fig. 5-2

5.7 SPECIAL KINDS OF FUNCTIONS, FUNDAMENTAL FACTORIZATION

This section discusses a number of special kinds of functions which frequently occur in mathematics. We also define and discuss the fundamental factorization of a function.

Restriction

Consider a function $f: A \to S$. Let B be a subset of A. Then f induces a function f' on B defined by

$$f'(b) = f(b)$$

for every $b \in B$. This function f' is called the *restriction* of f to B. It is sometimes denoted by

$$f|_B$$

EXAMPLE 5.7

(*a*) Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Recall that f is not one-to-one, e.g., $f(2) = f(-2) = 4$. Consider the restriction of f to the nonnegative real numbers $D = [0, \infty)$. Then $f|_D$ is one-to-one. [In fact, $f: D \to D$ is invertible and its inverse is the square root function $f^{-1}(x) = \sqrt{x}$.]

(*b*) Consider the functions

$$g = \{(1,3),\ (2,6),\ (3,11),\ (4,18),\ (5,27)\} \qquad \text{and} \qquad g' = \{(1,3),\ (3,11),\ (5,27)\}$$

Observe that g' is a subset of g. Thus g' is the restriction of g to $B = \{1,3,5\}$, the set of first elements of g'. Note that B is a subset of $A = \{1,2,3,4,5\}$, the set of first elements of g.

Extension

Consider a function $f: A \to S$. Suppose B to be a superset of A, that is, suppose $A \subseteq B$. Let $F: B \to S$ be a function on B such that, for every $a \in A$,

$$F(a) = f(a)$$

This function F is called an *extension* of f to B. We note that such an extension is rarely unique.

EXAMPLE 5.8

(*a*) Let f be the function on the nonnegative real numbers $D = [0, \infty)$ defined by $f(x) = x$. Then the absolute value function

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

is an extension of f to the set **R** of all real numbers. Clearly, the identity function $1_R : \mathbf{R} \to \mathbf{R}$ is also an extension of f to **R**.

(*b*) Consider the functions

$$f = \{(1,5),\ (3,11),\ (5,17)\} \qquad \text{and} \qquad F = \{(1,5),\ (2,8),\ (3,11),\ (4,14),\ (5,17)\}$$

Observe that F is a superset of f. Thus the function F is an extension of f from $\text{dom}(f) = \{1,3,5\}$ to $\text{dom}(F) = \{1,2,3,4,5\}$.

Inclusion Map

Let A be a subset of a set S, that is, $A \subseteq S$. Let $\imath$ be the function from A to S defined by

$$\imath(a) = a$$

for every $a \in A$. Then $\imath$ is called the *inclusion map*. This map is frequently denoted by writing

$$\imath : A \hookrightarrow S$$

For example, the function f: $\mathbf{Z} \to \mathbf{R}$ defined by $f(n) = n$ is the inclusion map from the integers **Z** into the real numbers **R**.

Characteristic Function

Consider a universal set **U**. For any subset A of **U**, let χ_A be the function from **U** to $\{0, 1\}$ defined by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Then χ_A is called the *characteristic function* of A.

EXAMPLE 5.9 Let $\mathbf{U} = \{a,b,c,d,e\}$ and $A = \{a,d,e\}$. Then the function

$$\{(a,1),\ (b,0),\ (c,0),\ (d,1),\ (e,1)\}$$

is the characteristic function χ_A.

On the other hand, any function f: $\mathbf{U} \to \{0, 1\}$ defines a subset A_f of **U** as follows:

$$A_f = \{x : x \in \mathbf{U},\ f(x) = 1\}$$

Furthermore, the characteristic function χ_{A_f} of A_f is the original function f. Thus there is a one-to-one correspondence between the power set $\mathscr{P}(\mathbf{U})$ of **U** and the set of all functions from **U** into $\{0, 1\}$.

Equivalence Relation and Canonical Map

Let $\equiv$ be an equivalence relation on a set S. Recall that $\equiv$ induces a partition of S into equivalence classes, called the quotient set of S by $\equiv$, and denoted and defined by

$$s/\!\equiv\, = \{[a] : a \in S\}$$

Let $\eta : S \to S/\!\equiv$ be the function defined by

$$\eta(a) = [a]$$

that is, η sends each element of S into its equivalence class. Then η is called the *canonical* or *natural map* from S into $S/\!\equiv$.

EXAMPLE 5.10 Consider the relation $\equiv$ of congruence modulo 5 on the set $\mathbf{Z}$ of integers; that is,

$$a \equiv b \pmod 5$$

if 5 divides $a - b$. Then $\equiv$ is an equivalence relation on $\mathbf{Z}$. There are five equivalence classes:

$$\begin{array}{ll}
[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\} & [3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} & [4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\} \\
[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} &
\end{array}$$

Let $\eta : \mathbf{Z} \to \mathbf{Z}/\equiv$ be the canonical map. Then

$$\eta(7) = [7] = [2], \qquad \eta(19) = [19] = [4], \qquad \eta(-12) = [-12] = [3]$$

Fundamental Factorization of a Function

Consider any function $f: A \to B$. Consider the relation $\sim$ on A defined by

$$a \sim a' \qquad \text{if} \qquad f(a) = f(a')$$

We show (Problem 5.20) that $\sim$ is an equivalence relation on A. We will let A/f denote the quotient set under this relation. Recall that $\operatorname{Im}(f) = f(A)$ denotes the image of f and it is a subset of the target set B.

The following lemma and theorem (proved in Problems 5.21 and 5.22) apply.

Lemma 5.3: The function f^*: $A/f \to f(A)$ defined by

$$f^*([a]) = f(a)$$

is well-defined and bijective.

Theorem 5.4: Let f: $A \to B$. Then the diagram in Fig. 5-3 is commutative; that is,

$$f = i \circ f^* \circ \eta$$

We note that, in Fig. 5-3, η is the canonical mapping from A into A/f, f^* is the bijective function defined above, and i is the inclusion map from $f(A)$ into B.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\eta"'] & B \\
A/f \arrow[r, "f^*"] & f(A) \arrow[u, hook, "i"']
\end{tikzcd}$$

Fig. 5-3

5.8 ASSOCIATED SET FUNCTIONS

Consider a function f: $S \to T$. Recall that the *image* $f[A]$ of any subset A of S consists of the elements in T which are images of elements in A, that is,

$$f[A] = \{b \in T : \text{there exists } a \in A \text{ such that } f(a) = b\}$$

Also recall that the *preimage* or *inverse image* $f^{-1}[B]$ of any subset B of T consists of all elements in S whose images belong to B, that is,

$$f^{-1}[B] = \{a \in S : f(a) \in T\}$$

Thus $f[A]$ is a subset of T and $f^{-1}[B]$ is a subset of S.

EXAMPLE 5.11 Let $f\colon \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Then

$$f[\{1,2,3,4\}] = \{1,4,9,16\} \qquad \text{and} \qquad f[(1,5)] = (1,25)$$

Also,

$$f^{-1}[\{4,9\}] = \{-3,-2,2,3\} \qquad \text{and} \qquad f^{-1}[(1,4)] = (1,2) \cup (-2,-1)$$

Accordingly, a function $f\colon S \to T$ induces a function, also denoted by f, from the power set $\mathcal{P}(S)$ of S into the power set $\mathcal{P}(T)$ of T, and a function f^{-1} from $\mathcal{P}(T)$ back to $\mathcal{P}(S)$. These functions f and f^{-1} are called *set functions* since they map sets into sets, i.e., their domains and target sets are collections of sets.

Observe that brackets [. .] rather than parentheses (. .) are used to distinguish between a function and its associated set functions, i.e., $f(a)$ denotes a value of the original function, whereas $f[A]$ and $f^{-1}[B]$ denote values of the associated set functions.

We note that the associated set function f^{-1} is not in general the inverse of the associated set function f. For example, for the above function $f(x) = x^2$, we have

$$f^{-1} \circ f[(1,2)] = f^{-1}[(1,4)] = (1,2) \cup (-2,-1)$$

However, we do have the following theorem.

Theorem 5.5: Let $f\colon S \to T$, and let $A \subseteq S$ and $B \subseteq T$. Then:
(i) $A \subseteq f^{-1} \circ f[A]$.
(ii) $B = f \circ f^{-1}[B]$.

As noted above, the inclusion in (i) cannot in general be replaced by equality.

5.9 CHOICE FUNCTIONS

Consider a collection $\{A_i : i \in I\}$ of subsets of a set B. A function

$$f\colon \{A_i\} \to B$$

is called a *choice function* if, for every $i \in I$,

$$f(A_i) \in A_i$$

that is, if the image of each set is an element in the set.

EXAMPLE 5.12 Consider the following subsets of $B = \{1,2,3,4,5\}$:

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

Figure 5-4 shows functions f and g from $\{A_1, A_2, A_3\}$ into B. The function f is not a choice function since $f(A_2) = 2$ does not belong to A_2, that is $f(A_2) \notin A_2$. On the other hand, g is a choice function. Namely, $g(A_1) = 2$ belongs to A_1, $g(A_2) = 4$ belongs to A_2, and $g(A_3) = 2$ belongs to A_3, that is, $g(A_i) \in A_i$, for $i = 1,2,3$.

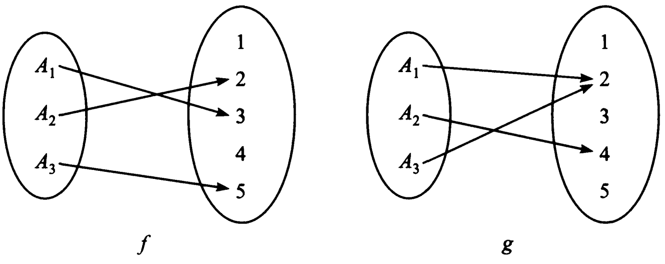

Fig. 5-4

Remark: Essentially, a choice function, for any collection of sets, "chooses" an element from each set in the collection. The question of whether or not a choice function exists for any collection of sets lies at the foundation of set theory. Chapter 9 will be devoted to this question.

5.10 ALGORITHMS AND FUNCTIONS

An algorithm M is a finite step-by-step list of well-defined instructions for solving a particular problem, say, to find the output $f(X)$ for a given function f with input X. (Here X may be a list or set of values.) Frequently, there may be more than one way to obtain $f(X)$ as illustrated by the following examples. The particular choice of the algorithm M to obtain $f(X)$ may depend on the "efficiency" or "complexity" of the algorithm; this question of the complexity of an algorithm M is discussed in the next section.

EXAMPLE 5.13 ***(Polynomial Evaluation)*** Suppose, for a given polynomial $f(x)$ and value $x = a$, we want to find $f(a)$, say,

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \qquad \text{and} \qquad a = 5$$

This can be done in the following two ways.

(a) (***Direct Method***): Here we substitute $a = 5$ directly in the polynomial to obtain

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe that there are $4 + 3 + 1 = 8$ multiplications and 3 additions. In general, evaluating a polynomial of degree n directly would require approximately

$$n + (n-1) + \cdots + 1 = \frac{n(n-1)}{2} \text{ multiplications and } n \text{ additions.}$$

(b) (***Horner's Method or Synthetic Division***): Here we rewrite the polynomial by successively factoring out x (on the right) as follows:

$$f(x) = (2x^2 - 7x + 4)x - 15 = [(2x - 7)x + 4]x - 15$$

Then

$$f(5) = [(3)5 + 4]5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

For those familiar with synthetic division, the above arithmetic is equivalent to the following synthetic division:

$$\begin{array}{r|l} 5 & 2 - 7 + \ \ 4 - 15 \\ & \quad\ 10 + 15 + 95 \\ \hline & 2 + 3 + 19 + 80 \end{array}$$

Observe that here there are 3 multiplications and 3 additions. In general, evaluating a polynomial of degree n by Horner's method would require approximately

$$n \text{ multiplications and } n \text{ additions}$$

Clearly Horner's method (b) is more efficient than the direct method (a).

EXAMPLE 5.14 (***Greatest Common Divisor***) Let a and b be positive integers with, say, $b < a$; and suppose we want to find $d = \gcd(a, b)$, the greatest common divisor of a and b. This can be done in the following two ways.

(*a*) (***Direct Method***): Here we find all the divisors of a and all the divisors of b; say, by testing all the numbers from 2 to $a/2$ and from 2 to $b/2$. Then we pick the largest common divisor. For example, suppose $a = 258$ and $b = 60$. The divisors of a and b follow:

$$\begin{aligned} a &= 258; \quad \text{divisors:} \quad 1,2,3,6,86,129,258 \\ b &= \ \ 60; \quad \text{divisors:} \quad 1,2,3,4,5,6,10,12,15,20,30,60 \end{aligned}$$

Accordingly, $d = \gcd\ (258, 60) = 6$.

(*b*) (***Euclidean Algorithm***): Here we divide a by b to obtain a remainder r_1 (where $r_1 < b$). Then we divide b by the remainder r_1 to obtain a second remainder r_2 (where $r_2 < r_1$). Next we divide r_1 by r_2 to obtain a third remainder r_3 (where $r_3 < r_2$). And so on. Since

$$a > b > r_1 > r_2 > r_3 > \cdots \qquad (*)$$

eventually we obtain a remainder $r_m = 0$. Then $r_{m-1} = \gcd\ (a, b)$. For example, suppose $a = 258$ and $b = 60$. Then:

(1) Dividing $a = 258$ by $b = 60$ yields the remainder $r_1 = 18$.
(2) Dividing $b = 60$ by $r_1 = 18$ yields the remainder $r_2 = 6$.
(3) Dividing $r_1 = 18$ by $r_2 = 6$ yields the remainder $r_3 = 0$.

Thus $r_2 = 6 = \gcd\ (258, 60)$.

Remark: The Euclidean algorithm is a very efficient way to find the greatest common divisor of two positive integers a and b. The fact that the algorithm ends follows from (*). The fact that the algorithm yields $d = \gcd\ (a, b)$ follows from properties of the integers.

5.11 COMPLEXITY OF ALGORITHMS

The analysis of algorithms is a major task in mathematics and computer science. In order to compare algorithms, we must have some criteria to measure the efficiency of our algorithms. This section discusses this important topic.

Suppose M is an algorithm, and suppose n is the size of the input data. The time and space used by the algorithm are the two main measures for the efficiency of M. The time is measured by counting the number of "key operations"; for example:

(*a*) In sorting and searching, one counts the number of comparisons.
(*b*) In arithmetic, one counts multiplications and neglects additions.

Key operations are so defined when the time for the other operations is much less than or at most proportional to the time for the key operations. The space is measured by counting the maximum of memory needed by the algorithm.

The *complexity* of an algorithm M is the function $f(n)$ which gives the running time and/or storage space requirement of the algorithm in terms of the size n of the input data. Frequently, the storage space required by an algorithm is simply a multiple of the data size. Accordingly, unless otherwise stated or implied, the term "complexity" shall refer to the running time of the algorithm.

The complexity function $f(n)$, which we assume gives the running time of an algorithm, usually depends not only on the size n of the input data but also on the particular data.

EXAMPLE 5.15 Suppose we want to search through an English short story TEXT for the first occurrence of a given 3-letter word W. Clearly, if W is the 3-letter word "the", then W likely occurs near the beginning of TEXT, so $f(n)$ will be small. On the other hand, if W is the 3-letter word "zoo", then W may not appear in TEXT at all, so $f(n)$ will be large.

The above discussion leads us to the question of finding the complexity function $f(n)$ for certain cases. The two cases one usually investigates in complexity theory follow:

(1) *Worst case*: The maximum value of $f(n)$ for any possible input.
(2) *Average case*: The expected value of $f(n)$.

The analysis of the average case assumes a certain probabilistic distribution for the input data. The average case also uses the following concept in probability theory. Suppose the numbers $n_1, n_2, \ldots, n_k$ occur with respective probabilities $p_1, p_2, \ldots, p_k$. Then the *expectation* or *average value E* is given by

$$E = n_1p_1 + n_2p_2 + \cdots + n_kp_k$$

Remark: The complexity of the average case of an algorithm is usually much more complicated to analyze than that of the worst case. Moreover, the probabilistic distribution that one assumes for the average case may not actually apply to real situations. Accordingly, unless otherwise stated or implied, the complexity of an algorithm shall mean the function which gives the running time of the worst case in terms of the input size. This is not too strong an assumption, since the complexity of the average case for many algorithms is proportional to the worst case.

Rate of Growth; Big O Notation

Suppose M is an algorithm, and suppose n is the size of the input data. Clearly the complexity $f(n)$ of M increases as n increases. It is usually the rate of increase of $f(n)$ that we want to examine. This is usually done by comparing $f(n)$ with some standard function, such as

$$\log_2 n, \qquad n, \qquad n \log_2 n, \qquad n^2, \qquad n^3, \qquad 2^n$$

The rates of growth for these standard functions are indicated in Fig. 5-5, which gives their approximate values for certain values of n. Observe that the functions are listed in the order of their rates of growth: the logarithmic function $\log_2 n$ grows most slowly, the exponential function 2^n grows most rapidly, and the polynomial functions n^c grows according to the exponent c.

$g(n)$ n	$\log n$	n	$n \log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1000	10	10^3	10^4	10^6	10^9	10^{300}

Fig. 5-5 Rate of growth of standard functions.

The way we compare our complexity function $f(n)$ with one of the standard functions is to use the functional "big O" notation which we formally define below.

Definition: Let $f(x)$ and $g(x)$ be arbitrary functions defined on R or a subset of R. We say "$f(x)$ is of order $g(x)$", written

$$f(x) = O(g(x))$$

if there exists a real number k and a positive constant C such that, for all $x > k$, we have

$$|f(x)| \leq C|g(x)|$$

Assuming $f(n)$ and $g(n)$ are functions defined on the positive integers, then

$$f(n) = O(g(n))$$

means that $f(n)$ is bounded by a constant multiple of $g(n)$ for almost all n.

Remark: The above is called the "big O" notation since $f(x) = o(g(x))$ has an entirely different meaning. We also write

$$f(x) = h(x) + O(g(x)) \qquad \text{when} \qquad f(x) - h(x) = O(g(x)).$$

EXAMPLE 5.16

(*a*) Let $P(x)$ be a polynomial of degree m. We show (Problem 5.24) that $P(x) = O(x^m)$. Thus,

$$7x^2 - 9x + 4 = O(x^2) \quad \text{and} \quad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

(*b*) The following gives the complexity of certain well-known searching and sorting algorithms in computer science:

(1) Linear search: $O(n)$ (3) Bubble sort: $O(n^2)$
(2) Binary search: $O(\log_n)$ (4) Merge-sort: $O(n \log n)$

Solved Problems

GENERALIZED OPERATIONS, INDEXED SETS

5.1. Let $\mathscr{A} = [\{1,2,3,4\},\ \{2,3,4,5\},\ \{3,4,5,6\},\ \{3,4,7,8,9\}]$.

Find: (*a*) $\bigcup \mathscr{A}$, (*b*) $\bigcap \mathscr{A}$.

(*a*) $\bigcup \mathscr{A}$ consists of all elements which belong to at least one of the sets in $\mathscr{A}$; hence

$$\bigcup \mathscr{A} = \{1,2,3,\ldots,8,9\}$$

(*b*) $\bigcap \mathscr{A}$ consists of those elements which belong to every set in $\mathscr{A}$; hence

$$\bigcap \mathscr{A} = \{3,4\}$$

5.2. Let $A_m = \{m, 2m, 3m, \ldots\}$ where $m \in \mathbf{P}$; that is, A_m consists of the positive multiples of m. Find: (*a*) $A_3 \cap A_5$; (*b*) $A_4 \cap A_6$; (*c*) $A_5 \cup A_{15}$; (*d*) $\bigcup(A_m : m \in S)$ where S is the set of prime numbers.

(*a*) The numbers which are divisible by 3 and divisible by 5 are the multiples of 15. Thus $A_3 \cap A_5 = A_{15}$.

(*b*) The multiples of 12 and no other numbers are contained in A_4 and A_6; hence $A_4 \cap A_6 = A_{12}$.

(*c*) The multiples of 21 are contained in the multiples of 7, that is, $A_{21} \subseteq A_7$. Hence $A_7 \cup A_{21} = A_7$.

(*d*) Every positive integer except 1 is a multiple of a prime number. Thus

$$\bigcup(A_m : m \in S) = \{2,3,4,\ldots\} = \mathbf{P}\backslash\{1\}$$

5.3. Let $B_n = [n, n+1]$ where $n \in \mathbf{Z}$, the integers. Find:

(*a*) $B_1 \cup B_2$; (*b*) $B_3 \cap B_4$; (*c*) $\bigcup_{i=7}^{18} B_i = \bigcup(B_i : i \in \{7,8,\ldots,18\})$; (*d*) $\bigcup(B_i : i \in \mathbf{Z})$.

(*a*) $B_1 \cup B_2$ consists of all points in the intervals $[1,2]$ and $[2,3]$; hence $B_1 \cup B_2 = [1,3]$.

(*b*) $B_3 \cap B_4$ consists of the points which lie in both $[3,4]$ and $[4,5]$; hence $B_3 \cap B_4 = \{4\}$.

(*c*) $\bigcup_{i=7}^{18} B_i$ means the union of the sets $[7,8], [8,9], \ldots, [18,19]$. Hence

$$\bigcup_{i=7}^{18} B_i = [7,19]$$

(*d*) Since every real number belongs to at least one interval $[i, i+1]$, we have $\bigcup(B_i : i \in \mathbf{Z}) = \mathbf{R}$.·