CHAPTER 3

Functions and Algorithms

3.1 INTRODUCTION

One of the most important concepts in mathematics is that of a function. The terms "map," "mapping," "transformation," and many others mean the same thing; the choice of which word to use in a given situation is usually determined by tradition and the mathematical background of the person using the term.

Related to the notion of a function is that of an algorithm. The notation for presenting an algorithm and a discussion of its complexity is also covered in this chapter.

3.2 FUNCTIONS

Suppose that to each element of a set A we assign a unique element of a set B; the collection of such assignments is called *a function* from A into B. The set A is called the *domain* of the function, and the set B is called the *target set* or *codomain*.

Functions are ordinarily denoted by symbols. For example, let f denote a function from A into B. Then we write

$$f: A \to B$$

which is read: "f is a function from A into B," or "f takes (or maps) A into B." If $a \in A$, then $f(a)$ (read: "f of a") denotes the unique element of B which f assigns to a; it is called the *image* of a under f, or the *value* of f at a. The set of all image values is called the *range* or *image* of f. The image of $f: A \to B$ is denoted by $\mathrm{Ran}(f)$, $\mathrm{Im}(f)$ or $f(A)$.

Frequently, a function can be expressed by means of a mathematical formula. For example, consider the function which sends each real number into its square. We may describe this function by writing

$$f(x) = x^2 \quad \text{or} \quad x \mapsto x^2 \quad \text{or} \quad y = x^2$$

In the first notation, x is called a *variable* and the letter f denotes the function. In the second notation, the barred arrow $\mapsto$ is read "goes into." In the last notation, x is called the *independent variable* and y is called the *dependent variable* since the value of y will depend on the value of x.

Remark: Whenever a function is given by a formula in terms of a variable x, we assume, unless it is otherwise stated, that the domain of the function is $\mathbf{R}$ (or the largest subset of $\mathbf{R}$ for which the formula has meaning) and the codomain is $\mathbf{R}$.

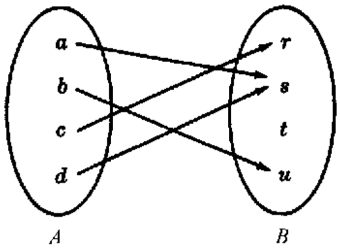


Fig. 3-1

EXAMPLE 3.1

(a) Consider the function $f(x) = x^3$, i.e., f assigns to each real number its cube. Then the image of 2 is 8, and so we may write $f(2) = 8$.

(b) Figure 3-1 defines a function f from $A = \{a, b, c, d\}$ into $B = \{r, s, t, u\}$ in the obvious way. Here

$$f(a) = s, \quad f(b) = u, \quad f(c) = r, \quad f(d) = s$$

The image of f is the set of image values, $\{r, s, u\}$. Note that t does not belong to the image of f because t is not the image of any element under f.

(c) Let A be any set. The function from A into A which assigns to each element in A the element itself is called the *identity function* on A and it is usually denoted by 1_A, or simply 1. In other words, for every $a \in A$,

$$1_A(a) = a.$$

(d) Suppose S is a subset of A, that is, suppose $S \subseteq A$. The *inclusion map* or *embedding* of S into A, denoted by $i\colon S \hookrightarrow A$ is the function such that, for every $x \in S$,

$$i(x) = x$$

The *restriction* of any function $f\colon A \to B$, denoted by $f|_S$ is the function from S into B such that, for any $x \in S$,

$$f|_S(x) = f(x)$$

Functions as Relations

There is another point of view from which functions may be considered. First of all, every function $f\colon A \to B$ gives rise to a relation from A to B called the *graph of f* and defined by

$$\text{Graph of } f = \{(a, b) \mid a \in A, b = f(a)\}$$

Two functions $f\colon A \to B$ and $g\colon A \to B$ are defined to be *equal*, written $f = g$, if $f(a) = g(a)$ for every $a \in A$; that is, if they have the same graph. Accordingly, we do not distinguish between a function and its graph. Now, such a graph relation has the property that each a in A belongs to a unique ordered pair (a, b) in the relation. On the other hand, any relation f from A to B that has this property gives rise to a function $f\colon A \to B$, where $f(a) = b$ for each (a, b) in f. Consequently, one may equivalently define a function as follows:

Definition: A function $f\colon A \to B$ is a relation from A to B (i.e., a subset of $A \times B$) such that each $a \in A$ belongs to a unique ordered pair (a, b) in f.

Although we do not distinguish between a function and its graph, we will still use the terminology "graph of f" when referring to f as a set of ordered pairs. Moreover, since the graph of f is a relation, we can draw its picture as was done for relations in general, and this pictorial representation is itself sometimes called the graph of f. Also, the defining condition of a function, that each $a \in A$ belongs to a unique pair (a, b) in f, is equivalent to the geometrical condition of each vertical line intersecting the graph in exactly one point.

EXAMPLE 3.2

(a) Let $f\colon A \to B$ be the function defined in Example 3.1 (b). Then the graph of f is as follows:

$$\{(a, s),\ (b, u),\ (c, r),\ (d, s)\}$$

(b) Consider the following three relations on the set $A = \{1, 2, 3\}$:

$$f = \{(1, 3),\ (2, 3),\ (3, 1)\}, \quad g = \{(1, 2),\ (3, 1)\}, \quad h = \{(1, 3),\ (2, 1),\ (1, 2),\ (3, 1)\}$$

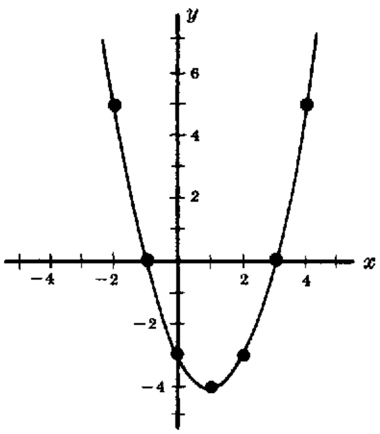
f is a function from A into A since each member of A appears as the first coordinate in exactly one ordered pair in f; here $f(1) = 3$, $f(2) = 3$, and $f(3) = 1$. g is not a function from A into A since $2 \in A$ is not the first coordinate of any pair in g and so g does not assign any image to 2. Also h is not a function from A into A since $1 \in A$ appears as the first coordinate of two distinct ordered pairs in h, $(1, 3)$ and $(1, 2)$. If h is to be a function it cannot assign both 3 and 2 to the element $1 \in A$.

(c) By a *real polynomial function*, we mean a function $f\colon \mathbf{R} \to \mathbf{R}$ of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where the a_i are real numbers. Since $\mathbf{R}$ is an infinite set, it would be impossible to plot each point of the graph. However, the graph of such a function can be approximated by first plotting some of its points and then drawing a smooth curve through these points. The points are usually obtained from a table where various values are assigned to x and the corresponding values of $f(x)$ are computed. Figure 3-2 illustrates this technique using the function $f(x) = x^2 - 2x - 3$.

x	$f(x)$
-2	5
-1	0
0	-3
1	-4
2	-3
3	0
4	5



Graph of $f(x) = x^2 - 2x - 3$

Fig. 3-2

Composition Function

Consider functions $f\colon A \to B$ and $g\colon B \to C$; that is, where the codomain of f is the domain of g. Then we may define a new function from A to C, called the *composition* of f and g and written $g \circ f$, as follows:

$$(g \circ f)(a) \equiv g(f(a))$$

That is, we find the image of a under f and then find the image of $f(a)$ under g. This definition is not really new. If we view f and g as relations, then this function is the same as the composition of f and g as relations (see Section 2.6) except that here we use the functional notation $g \circ f$ for the composition of f and g instead of the notation $f \circ g$ which was used for relations.

Consider any function $f\colon A \to B$. Then

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

where 1_A and 1_B are the identity functions on A and B, respectively.

3.3 ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

A function $f\colon A \to B$ is said to be *one-to-one* (written 1-1) if different elements in the domain A have distinct images. Another way of saying the same thing is that f is *one-to-one* if $f(a) = f(a')$ implies $a = a'$.

A function $f\colon A \to B$ is said to be an *onto* function if each element of B is the image of some element of A. In other words, $f\colon A \to B$ is onto if the image of f is the entire codomain, i.e., if $f(A) = B$. In such a case we say that f is a function from A onto B or that f maps A onto B.

A function $f\colon A \to B$ is *invertible* if its inverse relation f^{-1} is a function from B to A. In general, the inverse relation f^{-1} may not be a function. The following theorem gives simple criteria which tells us when it is.

Theorem 3.1: A function $f\colon A \to B$ is invertible if and only if f is both one-to-one and onto.

If $f\colon A \to B$ is one-to-one and onto, then f is called a *one-to-one correspondence* between A and B. This terminology comes from the fact that each element of A will then correspond to a unique element of B and vice versa.

Some texts use the terms *injective* for a one-to-one function, *surjective* for an onto function, and *bijective* for a one-to-one correspondence.

EXAMPLE 3.3 Consider the functions $f_1\colon A \to B$, $f_2\colon B \to C$, $f_3\colon C \to D$ and $f_4\colon D \to E$ defined by the diagram of Fig. 3-3. Now f_1 is one-to-one since no element of B is the image of more than one element of A. Similarly, f_2 is one-to-one. However, neither f_3 nor f_4 is one-to-one since $f_3(r) = f_3(u)$ and $f_4(v) = f_4(w)$

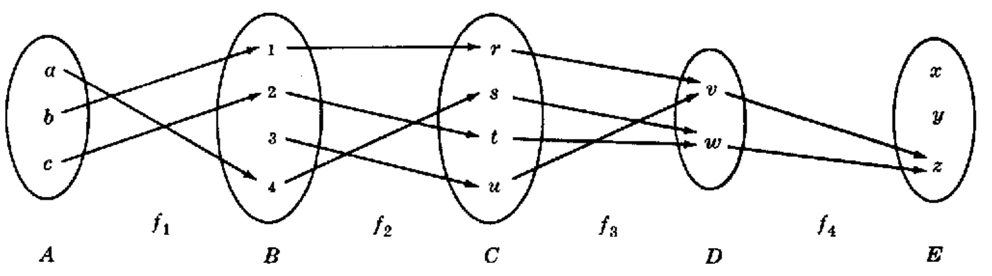


Fig. 3-3

As far as being onto is concerned, f_2 and f_3 are both onto functions since every element of C is the image under f_2 of some element of B and every element of D is the image under f_3 of some element of C, $f_2(B) = C$ and $f_3(C) = D$. On the other hand, f_1 is not onto since $3 \in B$ is not the image under f_4 of any element of A. and f_4 is not onto since $x \in E$ is not the image under f_4 of any element of D.

Thus f_1 is one-to-one but not onto, f_3 is onto but not one-to-one and f_4 is neither one-to-one nor onto. However, f_2 is both one-to-one and onto, i.e., is a one-to-one correspondence between A and B. Hence f_2 is invertible and f_2^{-1} is a function from C to B.

Geometrical Characterization of One-to-One and Onto Functions

Consider now functions of the form $f : \mathbf{R} \to \mathbf{R}$. Since the graphs of such functions may be plotted in the Cartesian plane $\mathbf{R}^2$ and since functions may be identified with their graphs, we might wonder whether the concepts of being one-to-one and onto have some geometrical meaning. The answer is yes. Specifically:

(1) f:**R** → **R** is one-to-one if each horizontal line intersects the graph of f in at most one point.

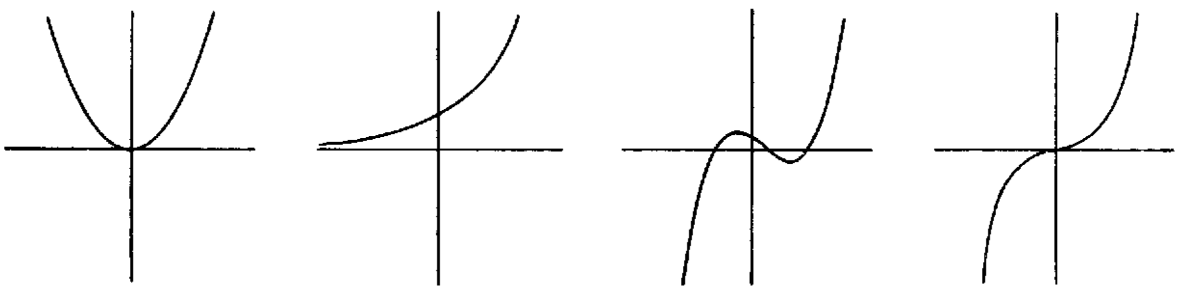
(2) f:**R** → **R** is an onto function if each horizontal line intersects the graph of f at one or more points.

Accordingly, if f is both one-to-one and onto, i.e. invertible, then each horizontal line will intersect the graph of f at exactly one point.

EXAMPLE 3.4 Consider the following four functions from **R** into **R**:

$$f_1(x) = x^2, \quad f_2(x) = 2^x, \quad f_3(x) = x^3 - 2x^2 - 5x + 6, \quad f_4(x) = x^3$$

The graphs of these functions appear in Fig. 3-4. Observe that there are horizontal lines which intersect the graph of f_1 twice and there are horizontal lines which do not intersect the graph of f_1 at all; hence f_1 is neither one-to-one nor onto. Similarly, f_2 is one-to-one but not onto, f_3 is onto but not one-to-one and f_4 is both one-to-one and onto. The inverse of f_4 is the cube root function, i.e., $f_4^{-1}(x) = \sqrt[3]{x}$.



$f_1(x) = x^2$ $\quad$ $f_2(x) = 2^x$ $\quad$ $f_3(x) = x^3 - 2x^2 - 5x + 6$ $\quad$ $f_4(x) = x^3$

Fig. 3-4

Permutations

An invertible (bijective) function σ: $X \to X$ is called a *permutation* on X. The composition and inverses of permutations on X and the identity function on X are also permutations on X.

Suppose $X = \{1, 2, \ldots, n\}$. Then a permutation σ on X is frequently denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

where $j_1 = \sigma(i)$. The set of all such permutations is denoted by S_n, and there are $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$ of them. For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

are permutations in S_6, and there are $6! = 720$ of them. Sometimes, we only write the second line of the permutation, that is, we denote the above permutations by writing $\sigma = 462513$ and $\tau = 643125$.

3.4 MATHEMATICAL FUNCTIONS, EXPONENTIAL AND LOGARITHMIC FUNCTIONS

This section presents various mathematical functions which appear often in the analysis of algorithms, and in computer science in general, together with their notation. We also discuss the exponential and logarithmic functions, and their relationship.

Floor and Ceiling Functions

Let x be any real number. Then x lies between two integers called the floor and the ceiling of x. Specifically,

$\lfloor x \rfloor$, called the *floor* of x, denotes the greatest integer that does not exceed x.

$\lceil x \rceil$, called the *ceiling* of x, denotes the least integer that is not less than x.

If x is itself an integer, then $\lfloor x \rfloor = \lceil x \rceil$; otherwise $\lfloor x \rfloor + 1 = \lceil x \rceil$. For example,

$$\lfloor 3.14 \rfloor = 3, \quad \left\lfloor \sqrt{5} \right\rfloor = 2, \quad \lfloor -8.5 \rfloor = -9, \quad \lfloor 7 \rfloor = 7, \quad \lfloor -4 \rfloor = -4,$$

$$\lceil 3.14 \rceil = 4, \quad \left\lceil \sqrt{5} \right\rceil = 3, \quad \lceil -8.5 \rceil = -8, \quad \lceil 7 \rceil = 7, \quad \lceil -4 \rceil = -4$$

Integer and Absolute Value Functions

Let x be any real number. The *integer value* of x, written INT(x), converts x into an integer by deleting (truncating) the fractional part of the number. Thus

$$\text{INT}(3.14) = 3, \quad \text{INT}(\sqrt{5}) = 2, \quad \text{INT}(-8.5) = -8, \quad \text{INT}(7) = 7$$

Observe that $\text{INT}(x) = \lfloor x \rfloor$ or $\text{INT}(x) = \lceil x \rceil$ according to whether x is positive or negative.

The *absolute value* of the real number x, written ABS(x) or $|x|$, is defined as the greater of x or $-x$. Hence $\text{ABS}(0) = 0$, and, for $x \neq 0$, $\text{ABS}(x) = x$ or $\text{ABS}(x) = -x$, depending on whether x is positive or negative. Thus

$$|-15| = 15, \quad |7| = 7, \quad |-3.33| = 3.33, \quad |4.44| = 4.44, \quad |-0.075| = 0.075$$

We note that $|x| = |-x|$ and, for $x \neq 0$, $|x|$ is positive.

Remainder Function and Modular Arithmetic

Let k be any integer and let M be a positive integer. Then

$$k \pmod{M}$$

(read: k modulo M) will denote the integer remainder when k is divided by M. More exactly, $k \pmod{M}$ is the unique integer r such that

$$k = Mq + r \quad \text{where} \quad 0 \leq r < M$$

When k is positive, simply divide k by M to obtain the remainder r. Thus

$$25 \pmod{7} = 4, \quad 25 \pmod{5} = 0, \quad 35 \pmod{11} = 2, \quad 3 \pmod{8} = 3$$

If k is negative, divide $|k|$ by M to obtain a remainder r'; then $k \pmod{M} = M - r'$ when $r' \neq 0$. Thus

$$-26 \pmod{7} = 7 - 5 = 2, \quad -371 \pmod{8} = 8 - 3 = 5, \quad -39 \pmod{3} = 0$$

The term "mod" is also used for the mathematical congruence relation, which is denoted and defined as follows:

$$a \equiv b \pmod{M} \quad \text{if any only if} \quad M \text{ divides } b - a$$

M is called the *modulus*, and $a \equiv b \pmod{M}$ is read "a is congruent to b modulo M". The following aspects of the congruence relation are frequently useful:

$$0 \equiv M \pmod{M} \quad \text{and} \quad a \pm M \equiv a \pmod{M}$$

Arithmetic modulo M refers to the arithmetic operations of addition, multiplication, and subtraction where the arithmetic value is replaced by its equivalent value in the set

$$\{0, 1, 2, \ldots, M-1\} \quad \text{or in the set} \quad \{1, 2, 3, \ldots, M\}$$

For example, in arithmetic modulo 12, sometimes called "clock" arithmetic,

$$6+9 \equiv 3, \quad 7 \times 5 \equiv 11, \quad 1-5 \equiv 8, \quad 2+10 \equiv 0 \equiv 12$$

(The use of 0 or M depends on the application.)

Exponential Functions

Recall the following definitions for integer exponents (where m is a positive integer):

$$a^m = a \cdot a \cdots a (m \text{ times}), \quad a^0 = 1, \quad a^{-m} = \frac{1}{a^m}$$

Exponents are extended to include all rational numbers by defining, for any rational number m/n,

$$a^{m/n} = \sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

For example,

$$2^4 = 16, \;\; 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \;\; 125^{2/3} = 5^2 = 25$$

In fact, exponents are extended to include all real numbers by defining, for any real number x,

$$a^x = \lim_{r \to x} a^r, \quad \text{where } r \text{ is a rational number}$$

Accordingly, the exponential function $f(x) = a^x$ is defined for all real numbers.

Logarithmic Functions

Logarithms are related to exponents as follows. Let b be a positive number. The logarithm of any positive number x to be the base b, written

$$\log_b x$$

represents the exponent to which b must be raised to obtain x. That is,

$$y = \log_b x \quad \text{and} \quad b^y = x$$

are equivalent statements. Accordingly,

$$\begin{array}{llll} \log_2 8 = 3 & \text{since} \;\; 2^3 = 8; & \log_{10} 100 = 2 & \text{since} \;\; 10^2 = 100 \\ \log_2 64 = 6 & \text{since} \;\; 2^6 = 64; & \log_{10} 0.001 = -3 & \text{since} \;\; 10^{-3} = 0.001 \end{array}$$

Furthermore, for any base b, we have $b^0 = 1$ and $b^1 = b$; hence

$$\log_b 1 = 0 \quad \text{and} \quad \log_b b = 1$$

The logarithm of a negative number and the logarithm of 0 are not defined.

Frequently, logarithms are expressed using approximate values. For example, using tables or calculators, one obtains

$$\log_{10} 300 = 2.4771 \quad \text{and} \quad \log_e 40 = 3.6889$$

as approximate answers. (Here $e = 2.718281\ldots$.)

Three classes of logarithms are of special importance: logarithms to base 10, called *common logarithms*; logarithms to base e, called *natural logarithms;* and logarithms to base 2, called *binary logarithms*. Some texts write

$$\ln x \text{ for } \log_e x \qquad \text{and} \qquad \lg x \text{ or } \log x \text{ for } \log_2 x$$

The term $\log x$, by itself, usually means $\log_{10} x$; but it is also used for $\log_e x$ in advanced mathematical texts and for $\log_2 x$ in computer science texts.

Frequently, we will require only the floor or the ceiling of a binary logarithm. This can be obtained by looking at the powers of 2. For example,

$$\lfloor \log_2 100 \rfloor = 6 \quad \text{since} \quad 2^6 = 64 \quad \text{and} \quad 2^7 = 128$$
$$\lceil \log_2 1000 \rceil = 9 \quad \text{since} \quad 2^8 = 512 \quad \text{and} \quad 2^9 = 1024$$

and so on.

Relationship between the Exponential and Logarithmic Functions

The basic relationship between the exponential and the logarithmic functions

$$f(x) = b^x \quad \text{and} \quad g(x) = \log_b x$$

is that they are inverses of each other; hence the graphs of these functions are related geometrically. This relationship is illustrated in Fig. 3-5 where the graphs of the exponential function $f(x) = 2^x$, the logarithmic function $g(x) = \log_2 x$, and the linear function $h(x) = x$ appear on the same coordinate axis. Since $f(x) = 2^x$ and $g(x) = \log_2 x$ are inverse functions, they are symmetric with respect to the linear function $h(x) = x$ or, in other words, the line $y = x$.

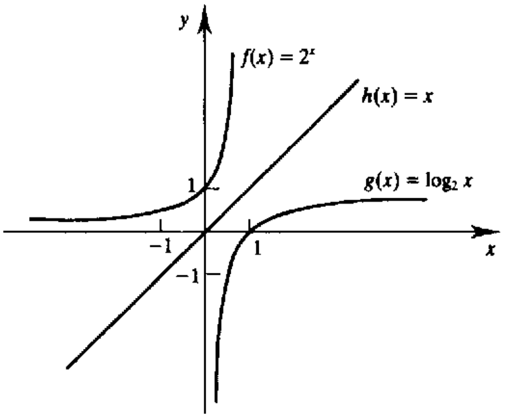


Fig. 3-5

Figure 3-5 also indicates another important property of the exponential and logarithmic functions. Specifically, for any positive c, we have

$$g(c) < h(c) < f(c), \quad \text{that is,} \quad g(c) < c < f(c)$$

In fact, as c increases in value, the vertical distances $h(c) - g(c)$ and $f(c) - g(c)$ increase in value. Moreover, the logarithmic function $g(x)$ grows very slowly compared with the linear function $h(x)$, and the exponential function $f(x)$ grows very quickly compared with $h(x)$.

3.5 SEQUENCES, INDEXED CLASSES OF SETS

Sequences and indexed classes of sets are special types of functions with their own notation. We discuss these objects in this section. We also discuss the summation notation here.

Sequences

A *sequence* is a function from the set $\mathbf{N} = \{1, 2, 3, \ldots\}$ of positive integers into a set A. The notation a_n is used to denote the image of the integer n. Thus a sequence is usually denoted by

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

Sometimes the domain of a sequence is the set $\{0, 1, 2, \ldots\}$ of nonnegative integers rather than $\mathbf{N}$. In such a ease we say 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 3.5

(a) The following are two familiar sequences:

(i) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ which may be defined by $a_n = \frac{1}{n}$;

(ii) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ which may be defined by $b_n = 2^{-n}$

Note that 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

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

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 $a_1a_2 \ldots a_m$, 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*. Strings over an alphabet A and certain operations on these strings will be discussed in detail in Chapter 13.

Summation Symbol, Sums

Here we introduce the summation symbol $\sum$ (the Greek letter sigma). Consider a sequence $a_1, a_2, a_3, \ldots$. Then we define the following:

$$\sum_{J=1}^{n} a_j = a_1 + a_2 + \cdots + a_n \quad \text{and} \quad \sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$$

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

EXAMPLE 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

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

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

The last sum appears very often. It has the value $n(n+1)/2$. That is:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \text{for example,} \quad 1 + 2 + \cdots + 50 = \frac{50(51)}{2} = 1275$$

Indexed Classes of Sets

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

$$\{A_i \mid i \in I\} \quad \text{or} \quad \{A_i\}_{i \in I} \quad \text{or simply} \quad \{A_i\}$$

The set I is called the *indexing set*, and the elements of I are called *indices*. If f is one-to-one and onto, we say that S is indexed by I.

The concepts of union and intersection are defined for indexed classes of sets as follows:

$$\cup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\} \quad \text{and} \quad \cap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}$$

In the case that I is a finite set, this is just the same as our previous definition of union and intersection. If I is $\mathbf{N}$, we may denote the union and intersection, respectively, as follows:

$$A_1 \cup A_2 \cup A_3 \cup \ldots \quad \text{and} \quad A_1 \cap A_2 \cap A_3 \cap \ldots$$

EXAMPLE 3.7 Let I be the set $\mathbf{Z}$ of integers. To each $n \in \mathbf{Z}$, we assign the following infinite interval in $\mathbf{R}$:

$$A_n = \{x \mid x \le n\} = (-\infty, n]$$

For any real number a, there exists integers n_1 and n_2 such that $n_1 < a < n_2$; so $a \in A_{n_2}$ but $a \notin A_{n_1}$. Hence

$$a \in \cup_n A_n \quad \text{but} \quad a \notin \cap_n A_n$$

Accordingly,

$$\cup_n A_n = \mathbf{R} \quad \text{but} \quad \cap_n A_n = \emptyset$$

3.6 RECURSIVELY DEFINED FUNCTIONS

A function is said to be *recursively defined* if the function definition refers to itself. In order for the definition not to be circular, the function definition must have the following two properties:

(1) There must be certain arguments, called *base values*, for which the function does not refer to itself.
(2) Each time the function does refer to itself, the argument of the function must be closer to a base value.

A recursive function with these two properties is said to be *well-defined*.

The following examples should help clarify these ideas.

Factorial Function

The product of the positive integers from 1 to n, inclusive, is called "n factorial" and is usually denoted by $n!$. That is,

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$$

It is also convenient to define $0! = 1$, so that the function is defined for all nonnegative integers. Thus:

$$0! = 1, \quad 1! = 1, \quad 2! = 2 \cdot 1 = 2, \quad 3! = 3 \cdot 2 \cdot 1 = 6, \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120, \quad 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

And so on. Observe that

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \quad \text{and} \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

This is true for every positive integer n; that is,

$$n! = n \cdot (n-1)!$$

Accordingly, the factorial function may also be defined as follows:

Definition 3.1 (Factorial Function):

(a) If $n = 0$, then $n! = 1$.
(b) If $n > 0$, then $n! = n \cdot (n-1)!$

Observe that the above definition of $n!$ is recursive, since it refers to itself when it uses $(n-1)!$. However:

(1) The value of $n!$ is explicitly given when $n = 0$ (thus 0 is a base value).
(2) The value of $n!$ for arbitrary n is defined in terms of a smaller value of n which is closer to the base value 0.

Accordingly, the definition is not circular, or, in other words, the function is well-defined.

EXAMPLE 3.8 Figure 3-6 shows the nine steps to calculate 4! using the recursive definition. Specifically:

Step 1. This defines 4! in terms of 3!, so we must postpone evaluating 4! until we evaluate 3. This postponement is indicated by indenting the next step.

Step 2. Here 3! is defined in terms of 2!, so we must postpone evaluating 3! until we evaluate 2!.

Step 3. This defines 2! in terms of 1!.

Step 4. This defines 1! in terms of 0!.

Step 5. This step can explicitly evaluate 0!, since 0 is the base value of the recursive definition.

Steps 6 to 9. We backtrack, using 0! to find 1!, using 1! to find 2!, using 2! to find 3!, and finally using 3! to find 4!. This backtracking is indicated by the "reverse" indention.

Observe that we backtrack in the reverse order of the original postponed evaluations.

$$\begin{array}{lllll}
(1) & 4! = 4 \cdot 3! & & & \\
(2) & & 3! = 3 \cdot 2! & & \\
(3) & & & 2! = 2 \cdot 1! & \\
(4) & & & & 1! = 1 \cdot 0! \\
(5) & & & & \quad 0! = 1 \\
(6) & & & & 1! = 1 \cdot 1 = 1 \\
(7) & & & 2! = 2 \cdot 1 = 2 & \\
(8) & & 3! = 3 \cdot 2 = 6 & & \\
(9) & 4! = 4 \cdot 6 = 24 & & &
\end{array}$$

Fig. 3-6

Level Numbers

Let P be a procedure or recursive formula which is used to evaluate $f(X)$ where f is a recursive function and X is the input. We associate a *level number* with each execution of P as follows. The original execution of P is assigned level 1; and each time P is executed because of a recursive call, its level is one more than the level of the execution that made the recursive call. The *depth* of recursion in evaluating $f(X)$ refers to the maximum level number of P during its execution.

Consider, for example, the evaluation of 4! Example 3.8, which uses the recursive formula $n! = n(n-1)!$. Step 1 belongs to level 1 since it is the first execution of the formula. Thus:

Step 2 belongs to level 2; Step 3 to level 3, . . . ; Step 5 to level 5.

On the other hand, Step 6 belongs to level 4 since it is the result of a return from level 5. In other words, Step 6 and Step 4 belong to the same level of execution. Similarly,

Step 7 belongs to level 3; Step 8 to level 2; and Step 9 to level 1.

Accordingly, in evaluating 4!, the depth of the recursion is 5.

Fibonacci Sequence

The celebrated Fibonacci sequence (usually denoted by $F_0, F_1, F_2, \ldots$) is as follows:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad \ldots$$

That is, $F_0 = 0$ and $F_1 = 1$ and each succeeding term is the sum of the two preceding terms. For example, the next two terms of the sequence are

$$34 + 55 = 89 \quad \text{and} \quad 55 + 89 = 144$$

A formal definition of this function follows:

Definition 3.2 (Fibonacci Sequence):

(a) If $n = 0$, or $n = 1$, then $F_n = n$.
(b) If $n > 1$, then $F_n = F_{n-2} + F_{n-1}$.

This is another example of a recursive definition, since the definition refers to itself when it uses F_{n-2} and F_{n-1} However:

(1) The base values are 0 and 1.
(2) The value of F_n is defined in terms of smaller values of n which are closer to the base values.

Accordingly, this function is well-defined.

Ackermann Function

The Ackermann function is a function with two arguments, each of which can be assigned any nonnegative interger, that is, 0, 1, 2, ... This function is defined as:

Definition 3.3 (Ackermann function):

(a) If $m = 0$, then $A(m, n) = n + 1$.
(b) If $m \neq 0$ but $n = 0$, then $A(m, n) = A(m-1, 1)$.
(c) If $m \neq 0$ and $n \neq 0$, then $A(m, n) = A(m-1, A(m, n-1))$.

Once more, we have a recursive definition, since the definition refers to itself in parts (b) and (c). Observe that $A(m, n)$ is explicitly given only when $m = 0$. The base criteria are the pairs

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (0, 3), \quad \ldots, (0, n), \quad \ldots$$

Although it is not obvious from the definition, the value of any $A(m, n)$ may eventually be expressed in terms of the value of the function on one or more of the base pairs.

The value of $A(1, 3)$ is calculated in Problem 3.21. Even this simple case requires 15 steps. Generally speaking, the Ackermann function is too complex to evaluate on any but a trivial example. Its importance comes from its use in mathematical logic. The function is stated here mainly to give another example of a classical recursive function and to show that the recursion part of a definition may be complicated.

3.7 CARDINALITY

Two sets A and B are said to be *equipotent*, or to have the *same number of elements* or the *same cardinality*, written $A \simeq B$, if there exists a one-to-one correspondence $f: A \to B$. A set A is *finite* if A is empty or if A has the same cardinality as the set $\{1, 2, \ldots, n\}$ for some positive integer n. A set is *infinite* if it is not finite. Familiar examples of infinite sets are the natural numbers **N**, the integers **Z**, the rational numbers **Q**, and the real numbers **R**.

We now introduce the idea of "cardinal numbers". We will consider cardinal numbers simply as symbols assigned to sets in such a way that two sets are assigned the same symbol if and only if they have the same cardinality. The cardinal number of a set A is commonly denoted by $|A|$, $n(A)$, or card (A). We will use $|A|$.

The obvious symbols are used for the cardinality of finite sets. That is, 0 is assigned to the empty set $\emptyset$, and n is assigned to the set $\{1, 2, \ldots, n\}$. Thus $|A| = n$ if and only if A has n elements. For example,

$$|\{x, y, z\}| = 3 \quad \text{and} \quad |\{1, 3, 5, 7, 9\}| = 5$$

The cardinal number of the infinite set **N** of positive integers is $\aleph_0$ ("aleph-naught"). This symbol was introduced by Cantor. Thus $|A| = \aleph_0$ if and only if A has the same cardinality as **N**.

EXAMPLE 3.9 Let $E = \{2, 4, 6, \ldots\}$, the set of even positive integers. The function $f: \mathbf{N} \to E$ defined by $f(n) = 2n$ is a one-to-one correspondence between the positive integers **N** and E. Thus E has the same cardinality as **N** and so we may write

$$|E| = \aleph_0$$

A set with cardinality $\aleph_0$ is said to be *denumerable* or *countably infinite*. A set which is finite or denumerable is said to be *countable*. One can show that the set **Q** of rational numbers is countable. In fact, we have the following theorem (proved in Problem 3.13) which we will use subsequently.

Theorem 3.2: A countable union of countable sets is countable.

That is, if $A_1, A_2, \ldots$ are each countable sets, then the following union is countable:

$$A_1 \cup A_2 \cup A_3 \cup \ldots$$

An important example of an infinite set which is uncountable, i.e., not countable, is given by the following theorem which is proved in Problem 3.14.

Theorem 3.3: The set **I** of all real numbers between 0 and 1 is uncountable.

Inequalities and Cardinal Numbers

One also wants to compare the size of two sets. This is done by means of an inequality relation which is defined for cardinal numbers as follows. For any sets A and B, we define $|A| \le |B|$ if there exists a function $f: A \to B$ which is one-to-one. We also write

$$|A| < |B| \quad \text{if} \quad |A| \le |B| \quad \text{but} \quad |A| \ne |B|$$

For example, $|\mathbf{N}| < |\mathbf{I}|$, where $\mathbf{I} = \{x: 0 \le x \le 1\}$, since the function $f: \mathbf{N} \to \mathbf{I}$ defined by $f(n) = 1/n$ is one-to-one, but $|\mathbf{N}| \ne |\mathbf{I}|$ by Theorem 3.3.

Cantor's Theorem, which follows and which we prove in Problem 3.25, tells us that the cardinal numbers are unbounded.

Theorem 3.4 (Cantor): For any set A, we have $|A| < |\text{Power}(A)|$ (where Power(A) is the power set of A, i.e., the collection of all subsets of A).

The next theorem tells us that the inequality relation for cardinal numbers is antisymmetric.

Theorem 3.5: (Schroeder-Bernstein): Suppose A and B are sets such that

$$|A| \leq |B| \quad \text{and} \quad |B| \leq |A|$$

Then $|A| = |B|$.

We prove an equivalent formulation of this theorem in Problem 3.26.

3.8 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 formally discussed in the next section.

EXAMPLE 3.10 (Polynomial Evaluation) Suppose, for a given polynomial $f(x)$ and value $x = a$, we want to find $f(a)$, say,

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

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 $3 + 2 + 1 = 6$ 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:

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

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 3.11 (Greatest Common Divisor) Let a and b be positive integers with, say, $b < a$; and suppose we want to find $d = \text{GCD}(a, b)$, 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, say by testing all the numbers from 2 to $a/2$, and all the divisors of b. Then we pick the largest common divisor. For example, suppose $a = 258$ and $b = 60$. The divisors of a and b follow:

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

Accordingly, $d = \text{GCD}(258, 60) = 6$.

(b) (***Euclidean Algorithm***)**:** Here we divide a by b to obtain a remainder r_1. (Note $r_1 < b$.) Then we divide b by the remainder r_1 to obtain a second remainder r_2. (Note $r_2 < r_1$.) Next we divide r_1 by r_2 to obtain a third remainder r_3. (Note $r_3 < r_2$.) We continue dividing r_k by r_{k+1} to obtain a remainder r_{k+2}. Since

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

eventually we obtain a remainder $r_m = 0$. Then $r_{m-1} = \text{GCD}\ (a, b)$. 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 $r_2 = 6 = \text{GCD}(258, 60)$.

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 $d = \text{GCD}(a, b)$ is not obvious; it is discussed in Section 11.6.

3.9 COMPLEXITY OF ALGORITHMS

The analysis of algorithms is a major task in 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. For example, 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 are as follows:

(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; one possible assumption might be that the possible permutations of a data set are equally likely. 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

$$E = n_1 p_1 + n_2 p_2 + \cdots + n_k p_k$$

These ideas are illustrated below.

Linear Search

Suppose a linear array DATA contains n elements, and suppose a specific ITEM of information is given. We want either to find the location LOC of ITEM in the array DATA, or to send some message, such as LOC $= 0$, to indicate that ITEM does not appear in DATA. The linear search algorithm solves this problem by comparing ITEM, one by one, with each element in DATA. That is, we compare ITEM with DATA[1], then DATA[2], and so on, until we find LOC such that ITEM = DATA[LOC].

The complexity of the search algorithm is given by the number C of comparisons between ITEM and DATA[K]. We seek $C(n)$ for the worst case and the average case.

(1) ***Worst Case***: Clearly the worst case occurs when ITEM is the last element in the array DATA or is not there at all. In either situation, we have

$$C(n) = n$$

Accordingly, $C(n) = n$ is the worst-case complexity of the linear search algorithm.

(2) ***Average Case***: Here we assume that ITEM does appear in DATA, and that it is equally likely to occur at any position in the array. Accordingly, the number of comparisons can be any of the numbers $1, 2, 3, \ldots, n$, and each number occurs with probability $p = 1/n$. Then

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

This agrees with our intuitive feeling that the average number of comparisons needed to find the location of ITEM is approximately equal to half the number of elements in the DATA list.

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

$$\log n, \quad n, \quad n \log n, \quad n^2, \quad n^3, \quad 2^n$$

The rates of growth for these standard functions are indicated in Fig. 3-7, 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 grow according to the exponent c.

n \ $g(n)$	$\log n$	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. 3-7 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 3.4: 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

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

In other words, $f(x) = 0(g(x))$ if a constant multiple of $|g(x)|$ exceeds $|f(x)|$ for all x greater than some real number k.

We also write:

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

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

Consider now a polynomial $P(x)$ of degree m. We show in Problem 3.24 that $P(x) = O(x^m)$. Thus, for example,

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

Complexity of Well-known Algorithms

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.

To indicate the convenience of this notation, we give the complexity of certain well-known searching and sorting algorithms in computer science:

(a) Linear search: $O(n)$ (c) Bubble sort: $O(n^2)$
(b) Binary search: $O(\log n)$ (d) Merge-sort: $O(n \log n)$

Solved Problems

FUNCTIONS

3.1. Let $X = \{1, 2, 3, 4\}$. Determine whether each relation on X is a function from X into X.

(a) $f = \{(2, 3), (1, 4), (2, 1), (3.2), (4, 4)\}$

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

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

Recall that a subset f of $X \times X$ is a function $f\colon X \to X$ if and only if each $a \in X$ appears as the first coordinate in exactly one ordered pair in f.

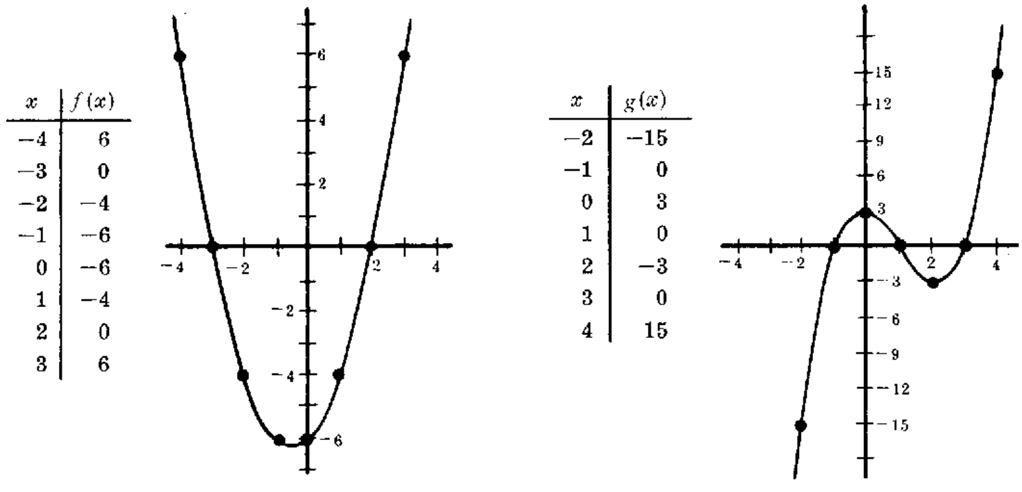
(a) No. Two different ordered pairs (2, 3) and (2, 1) in f have the same number 2 as their first coordinate.

(b) No. The element $2 \in X$ does not appear as the first coordinate in any ordered pair in g.

(c) Yes. Although $2 \in X$ appears as the first coordinate in two ordered pairs in h, these two ordered pairs are equal.

3.2. Sketch the graph of: (a) $f(x) = x^2 + x - 6$; (b) $g(x) = x^3 - 3x^2 - x + 3$.

Set up a table of values for x and then find the corresponding values of the function. Since the functions are polynomials, plot the points in a coordinate diagram and then draw a smooth continuous curve through the points. See Fig. 3-8.



x	$f(x)$
-4	6
-3	0
-2	-4
-1	-6
0	-6
1	-4
2	0
3	6

Graph of $f = x^2 + x - 6$

x	$g(x)$
-2	-15
-1	0
0	3
1	0
2	-3
3	0
4	15

Graph of $g = x^3 - 3x^2 - x - 3$

Fig. 3-8

3.3. Let $A = \{a, b, c\}$, $B = \{x, y, z\}$, $C = \{r, s, t\}$. Let $f\colon A \to B$ and $g\colon B \to C$ be defined by:

$$f = \{(a, y)(b, x), (c, y)\} \quad \text{and} \quad g = \{(x, s), (y, t), (z, r)\}.$$

Find: (a) composition function $g \circ f\colon A \to C$; (b) $\operatorname{Im}(f), \operatorname{Im}(g), \operatorname{Im}(g \circ f)$.

(a) Use the definition of the composition function to compute:

$$(g \circ f)(a) = g(f(a)) = g(y) = t$$
$$(g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

That is $g \circ f = \{(a, t), (b, s), (c, t)\}$.

(b) Find the image points (or second coordinates):

$$\operatorname{Im}(f) = \{x, y\}, \quad \operatorname{Im}(g) = \{r, s, t\}, \quad \operatorname{Im}(g \circ f) = \{s, t\}$$

3.4. Let $f: \mathbf{R} \to \mathbf{R}$ and $g: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x + 1$ and $g(x) = x^2 - 2$. Find the formula for the composition function $g \circ f$.

Compute $g \circ f$ as follows: $(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$.

Observe that the same answer can be found by writing

$$y = f(x) = 2x + 1 \quad \text{and} \quad z = g(y) = y^2 - 2$$

and then eliminating y from both equations:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

3.5. Let the functions $f: A \to B$, $g: B \to C$, $h: C \to D$ be defined by Fig. 3-9. Determine if each function is: (*a*) onto, (*b*) one-to-one, (*c*) invertible.

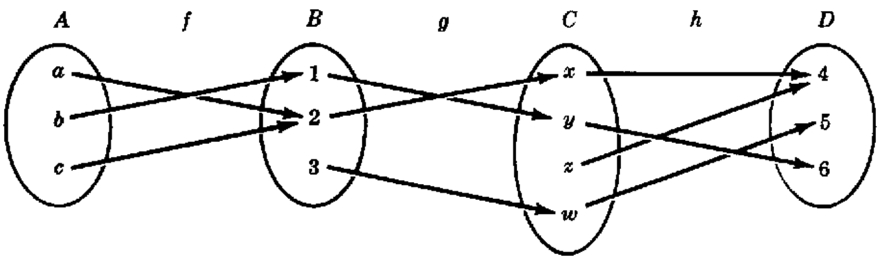


Fig. 3-9

(*a*) The function $f: A \to B$ is not onto since $3 \in B$ is not the image of any element in A.

The function $g: B \to C$ is not onto since $z \in C$ is not the image of any element in B.

The function $h: C \to D$ is onto since each element in D is the image of some element of C.

(*b*) The function $f: A \to B$ is not one-to-one since a and c have the same image 2.

The function $g: B \to C$ is one-to-one since 1, 2 and 3 have distinct images.

The function $h: C \to D$ is not one-to-one since x and z have the same image 4.

(*c*) No function is one-to-one and onto; hence no function is invertible.

3.6. Consider permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$ in S_6.
Find: (*a*) composition $\tau \circ \sigma$; (*b*) σ^{-1}.

(*a*) Note that σ sends 1 into 3 and τ sends 3 into 6. So the composition $\tau \circ \sigma$ sends 1 into 6. I.e. $(\tau \circ \sigma)(1) = 6$. Moreover, $\tau \circ \sigma$ sends 2 into 6 into 1 that is, $(\tau \circ \sigma)(2) = 1$, Similarly,

$$(\tau \circ \sigma)(3) = 5, \quad (\tau \circ \sigma)(4) = 3, \quad (\tau \circ \sigma) = 2, \quad (\tau \circ \sigma)(6) = 4$$

Thus

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

(*b*) Look for 1 in the second row of σ. Note σ sends 5 into 1. Hence $\sigma^{-1}(1) = 5$. Look for 2 in the second row of σ. Note σ sends 6 into 2. Hence $\sigma^{-1}(2) = 6$. Similarly, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$, $\sigma^{-1}(5) = 4$, $\sigma^{-1}(6) = 2$. Thus

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}$$

3.7. Consider functions $f\colon A \to B$ and $g\colon B \to C$. Prove the following:

(a) If f and g are one-to-one, then the composition function $g \circ f$ is one-to-one.

(b) If f and g are onto functions, then $g \circ f$ is an onto function.

(a) Suppose $(g \circ f)(x) = (g \circ f)(y)$; then $g(f(x)) = g(f(y))$. Hence $f(x) = f(y)$ because g is one-to-one. Furthermore, $x = y$ since f is one-to-one. Accordingly $g \circ f$ is one-to-one.

(b) Let c be any arbitrary element of C. Since g is onto, there exists a $b \in B$ such that $g(b) = c$. Since f is onto, there exists an $a \in A$ such that $f(a) = b$. But then

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Hence each $c \in C$ is the image of some element $a \in A$. Accordingly, $g \circ f$ is an onto function.

3.8. Let $f\colon \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x - 3$. Now f is one-to-one and onto; hence f has an inverse function f^{-1}. Find a formula for f^{-1}.

Let y be the image of x under the function f:

$$y = f(x) = 2x - 3$$

Consequently, x will be the image of y under the inverse function f^{-1}. Solve for x in terms of y in the above equation:

$$x = (y + 3)/2$$

Then $f^{-1}(y) = (y + 3)/2$. Replace y by x to obtain

$$f^{-1}(x) = \frac{x+3}{2}$$

which is the formula for f^{-1} using the usual independent variable x.

3.9. Prove the following generalization of DeMorgan's law: For any class of sets $\{A_i\}$ we have

$$(\cup_i\ A_i)^{\mathrm{c}} = \cap_i A_i^{\mathrm{c}}$$

We have:

$$x \in (\cup_i A_i)^{\mathrm{c}} \quad \text{iff } x \notin \cup_i A_i, \quad \text{iff } \forall_i \in I, x \notin A_i, \quad \text{iff } \forall_i \in I, x \in A_i^{\mathrm{c}}, \quad \text{iff } x \in \cap_i A_i^{\mathrm{c}}$$

Therefore, $(\cup_i A_i)^{\mathrm{c}} = \cap_i A_i^{\mathrm{c}}$. (Here we have used the logical notations iff for "if and only" if and $\forall$ for "for all.")

CARDINALITY

3.10. Find the cardinal number of each set:

(a) $A = \{a, b, c, \ldots, y, z\}$, (c) $C = \{10, 20, 30, 40, \ldots\}$,

(b) $B = \{x \mid x \in \mathbf{N},\ x^2 = 5\}$, (d) $D = \{6, 7, 8, 9, \ldots\}$.

(a) $|A| = 26$ since there are 26 letters in the English alphabet.

(b) $|B| = 0$ since there is no positive integer whose square is 5, that is, B is empty.

(c) $|C| = \aleph_0$ because $f\colon \mathbf{N} \to C$, defined by $f(n) = 10_n$, is a one-to-one correspondence between $\mathbf{N}$ and C.

(d) $|D| = \aleph_0$ because $g\colon \mathbf{N} \to D$, defined by $g(n) = n + 5$ is a one-to-one correspondence between $\mathbf{N}$ and D.

3.11. Show that the set $\mathbf{Z}$ of integers has cardinality $\aleph_0$.

The following diagram shows a one-to-one correspondence between $\mathbf{N}$ and $\mathbf{Z}$:

$$\begin{array}{rccccccccc} \mathbf{N} = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ \mathbf{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \ldots \end{array}$$

That is, the following function $f\colon \mathbf{N} \to \mathbf{Z}$ is one-to-one and onto:

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (1-n)/2 & \text{if } n \text{ is odd}^{n/2} \end{cases}$$

Accordingly, $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$.

3.12. Let $A_1, A_2, \ldots$ be a countable number of finite sets. Prove that the union $S = \cup_i A_i$ is countable.

Essentially, we list the elements of A_1, then we list the elements of A_2 which do not belong to A_1, then we list the elements of A_3 which do not belong to A_1 or A_2, i.e., which have not already been listed, and so on. Since the A_i are finite, we can always list the elements of each set. This process is done formally as follows.

First we define sets $B_1, B_2, \ldots$ where B_i contains the elements of A_i which do not belong to preceding sets, i.e., we define

$$B_1 = A_1 \quad \text{and} \quad B_k = A_k \backslash (A_1 \cup A_2 \cup \cdots \cup A_{k-1})$$

Then the B_i are disjoint and $S = \cup_i B_i$. Let $b_{i1}, b_{i2}, \ldots, b_{im}$, be the elements of B_i. Then $S = \{b_{ij}\}$. Let $f: S \to \mathbf{N}$ be defined as follows:

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j$$

If S is finite, then S is countable. If S is infinite then f is a one-to-one correspondence between S and $\mathbf{N}$. Thus S is countable.

3.13. Prove Theorem 3.2: A countable union of countable sets is countable.

Suppose $A_1, A_2, A_3, \ldots$ are a countable number of countable sets. In particular, suppose $a_{i1}, a_{i2}, a_{i3}, \ldots$ are the elements of A_i. Define sets $B_2, B_3, B_4, \ldots$ as follows:

$$B_k = \{a_{ij} \mid i + j = k\}$$

For example, $B_6 = \{a_{15},\ a_{24},\ a_{33},\ a_{12},\ a_{51}\}$. Observe that each B_k is finite and

$$S = \cup_i A_i = \cup_k B_k$$

By the preceding problem $\cup_k B_k$ is countable. Hence $S = \cup_i A_i$ is countable and the theorem is proved.

3.14. Prove Theorem 3.3: The set $\mathbf{I}$ of all real numbers between 0 and 1 inclusive is uncountable.

The set $\mathbf{I}$ is clearly infinite, since it contains $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Suppose $\mathbf{I}$ is denumerable. Then there exists a one-to-one correspondence $f: N \to \mathbf{I}$. Let $f(1) = a_1, f(2) = a_2, \ldots$; that is, $\mathbf{I} = \{a_1, a_2, a_3, \ldots\}$. We list the elements $a_1, a_2, \ldots$. in a column and express each in its decimal expansion:

$$\begin{aligned}
a_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\
a_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\
a_3 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\
a_4 &= 0.x_{41}x_{42}x_{43}x_{44}\ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

where $x_{ij} \in \{0, 1, 2, \ldots, 9\}$. (For those numbers which can be expressed in two different decimal expansions, e.g., $0.2000000\ldots = 0.1999999\ldots$, we choose the expansion which ends with nines.)

Let $b = 0.y_1y_2y_3y_4\ldots$ be the real number obtained as follows:

$$y_i = \begin{cases} 1 & \text{if } x_{ii} \neq 1 \\ 2 & \text{if } x_{ii} = 1 \end{cases}$$

Now $b \in \mathbf{I}$. But

$$\begin{aligned}
b &\neq a_1 \text{ because } y_1 \neq x_{11} \\
b &\neq a_2 \text{ because } y_2 \neq x_{22} \\
b &\neq a_3 \text{ because } y_3 \neq x_{33} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Therefore b does not belong to $\mathbf{I} = \{a_1, a_2, \ldots\}$. This contradicts the fact that $b \in \mathbf{I}$. Hence the assumption that $\mathbf{I}$ is denumerable must be false, so $\mathbf{I}$ is uncountable.

SPECIAL MATHEMATICAL FUNCTIONS

3.15. Find: (*a*) $\lfloor 7.5 \rfloor, \lfloor -7.5 \rfloor, \lfloor -18 \rfloor$; (*b*) $\lceil 7.5 \rceil, \lceil -7.5 \rceil, \lceil -18 \rceil$.

(*a*) By definition, $\lfloor x \rfloor$ denotes the greatest integer that does not exceed x, hence $\lfloor 7.5 \rfloor = 7$, $\lfloor -7.5 \rfloor = -8$, $\lfloor -18 \rfloor = -18$.

(*b*) By definition, $\lceil x \rceil$ denotes the least integer that is not less than x, hence $\lceil 7.5 \rceil = 8$, $\lceil -7.5 \rceil = -7$, $\lceil -18 \rceil = -18$.

3.16. Find: (a) 25 (mod7); (b) 25 (mod5); (c) -35 (mod 11); (d) -3 (mod 8).

When k is positive, simply divide k by the modulus M to obtain the remainder r. Then $r = k(\text{mod } M)$. If k is negative, divide $|k|$ by M to obtain the remainder r'. Then $k(\text{mod } M) = M - r'$ (when $r' \neq 0$). Thus:

(a) $25 \text{ (mod 7)} = 4$ (c) $-35 \text{ (mod 11)} = 11 - 2 = 9$

(b) $25 \text{ (mod 5)} = 0$ (d) $-3 \text{ (mod 8)} = 8 - 3 = 5$

3.17. Evaluate modulo $M = 15$: (a) $9 + 13$; (b) $7 + 11$; (c) $4 - 9$; (d) $2 - 10$.

Use $a \pm M = a(\text{mod } M)$:

(a) $9 + 13 = 22 = 22 - 15 = 7$ (c) $4 - 9 = -5 = -5 + 15 = 10$

(b) $7 + 11 = 18 = 18 - 15 = 3$ (d) $2 - 10 = -8 = -8 + 15 = 7$

3.18. Simplify: (a) $\dfrac{n!}{(n-1)!}$; (b) $\dfrac{(n+2)!}{n!}$.

(a) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$ or, simply, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$

(b) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n-1) = n^2 + 3n + 2$

3.19. Evaluate: (a) $\log_2 8$; (b) $\log_2 64$; (c) $\log_{10} 100$; (d) $\log_{10} 0.001$.

(a) $\log_2 8 = 3$ since $2^3 = 8$ (c) $\log_{10} 100 = 2$ since $10^2 = 100$

(b) $\log_2 64 = 6$ since $2^6 = 64$ (d) $\log_{10} 0.001 = -3$ since $10^{-3} = 0.001$

RECURSIVE FUNCTIONS

3.20. Let a and b be positive integers, and suppose Q is defined recursively as follows:

$$Q(a, b) = \begin{cases} 0 & \text{if } a < b \\ Q(a - b, b) + 1 & \text{if } b \leq a \end{cases}$$

(a) Find: (i) $Q(2, 5)$; (ii) $Q(12, 5)$.

(b) What does this function Q do? Find $Q(5861, 7)$.

(a) (i) $Q(2, 5) = 0$ since $2 < 5$.

(ii) $$\begin{aligned} Q(12, 5) &= Q(7, 5) + 1 \\ &= [Q(2, 5) + 1] + 1 = Q(2, 5) + 2 \\ &= 0 + 2 = 2 \end{aligned}$$

(b) Each time b is subtracted from a, the value of Q is increased by 1. Hence $Q(a, b)$ finds the quotient when a is divided by b. Thus $Q(5861, 7) = 837$.

3.21. Use the definition of the Ackermann function to find $A(1, 3)$.

Figure 3-10 shows the 15 steps that are used to evaluate $A(1, 3)$.

The forward indention indicates that we are postponing an evaluation and are recalling the definition, and the backward indention indicates that we are backtracking. Observe that (a) of the definition is used in Steps 5, 8, 11 and 14; (b) in Step 4; and (c) in Steps 1, 2, and 3. In the other steps we are backtracking with substitutions.

(1)	$A(1, 3) = A(0, A(1, 2))$	(9)	$A(1, 1) = 3$
(2)	$A(1, 2) = A(0, A(1, 1))$	(10)	$A(1, 2) = A(0, 3)$
(3)	$A(1, 1) = A(0, A(1, 0))$	(11)	$A(0, 3) = 3 + 1 = 4$
(4)	$A(1, 0) = A(0, 1)$	(12)	$A(1, 2) = 4$
(5)	$A(0, 1) = 1 + 1 = 2$	(13)	$A(1, 3) = A(0, 4)$
(6)	$A(1, 0) = 2$	(14)	$A(0, 4) = 4 + 1 = 5$
(7)	$A(1, 1) = A(0, 2)$	(15)	$A(1, 3) = 5$
(8)	$A(0, 2) = 2 + 1 = 3$		

Fig. 3-10

MISCELLANEOUS PROBLEMS

3.22. Find the domain D of each of the following real-valued functions of a real variable:

(*a*) $f(x) = \frac{1}{x-2}$ (*c*) $f(x) = \sqrt{25 - x^2}$
(*b*) $f(x) = x^2 - 3x - 4$ (*d*) x^2 where $0 \le x \le 2$

When a real-valued function of a real variable is given by a formula $f(x)$, then the domain D consists of the largest subset of $\mathbf{R}$ for which $f(x)$ has meaning and is real, unless otherwise specified.

(*a*) f is not defined for $x - 2 = 0$, i.e., for $x = 2$; hence $D = \mathbf{R}\backslash\{2\}$.
(*b*) f is defined for every real number; hence $D = \mathbf{R}$.
(*c*) f is not defined when $25 - x^2$ is negative; hence $D = [-5, 5] = \{x \mid -5 \le x \le 5\}$.
(*d*) Here, the domain of f is explicitly given as $D = \{x \mid 0 \le x \le 2\}$.

3.23. For any $n \in \mathbf{N}$, let $D_n = (0, 1/n)$, the open interval from 0 to $1/n$. Find:

(*a*) $D_3 \cup D_4$; (*b*) $D_3 \cap D_{20}$; (*c*) $D_s \cup D_t$; (*d*) $D_s \cap D_t$.

(*a*) Since (0, 1/3) is a superset of (0, 1/7), $D_3 \cup D_4 = D_3$.
(*b*) Since (0, 1/20) is a subset of (0, 1/3), $D_3 \cap D_{20} = D_{20}$.
(*c*) Let $m = \min(s, t)$, that is, the smaller of the two numbers s and t; then D_m is equal to D_s or D_t contains the other as a subset. Hence $D_s \cap D_t = D_m$.
(*d*) Let $M = \max(s, t)$, that is, the larger of the two numbers s and t; then $D_s \cap D_t = D_m$.

3.24. Suppose $P(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_m n^2$ has degree m. Prove $P(n) = O(n^m)$.

Let $b_0 = |a_0|,\ b_1 = |a_1|, \ldots, b_m = |a_m|$. Then for $n \ge 1$,

$$\begin{aligned} p(n) &\le b_0 + b_1 n + b_2 n^2 + \cdots + b_m n^m = \left(\frac{b_0}{n^m} + \frac{b_1}{n^{m-1}} + \cdots + b_m\right) n^m \\ &\le (b_0 + b_1 + \cdots + b_m) n^m = M n^m \end{aligned}$$

where $M = |a_0| + |a_1| + \cdots + |a_m|$. Hence $P(n) = O(n^m)$.

For example, $5x^3 + 3x = O(x^3)$ and $x^5 - 4000000x^2 = O(x^5)$.

3.25. Prove Theorem 3.4 (Cantor): $|A| < |\text{Power}(A)|$ (where Power (A) is the power set *of* A).

The function $g\colon A \to \text{Power}(A)$ defined by $g(a) = \{a\}$ is clearly one-to-one; hence $|A| \le |\text{Power}(A)|$.

If we show that $|A| \ne |\text{Power}(A)|$, then the theorem will follow. Suppose the contrary, that is, suppose $|A| = |\text{Power}(A)|$ and that $f\colon A \to \text{Power}(A)$ is a function which is both one-to-one and onto. Let $a \in A$ be called a "bad" element if $a \notin f(a)$, and let B be the set of bad elements. In other words,

$$B = \{x : x \in A,\ x \notin f(x)\}$$

Now B is a subset of A. Since $f\colon A \to \text{Power}(A)$ is onto, there exists $b \in A$ such that $f(b) = B$. Is b a "bad" element or a "good" element? If $b \in B$ then, by definition of B, $b \notin f(b) = B$, which is impossible. Likewise, if $b \notin B$ then $b \in f(b) = B$, which is also impossible. Thus the original assumption that $|A| = |\text{Power}(A)|$ has led to a contradiction. Hence the assumption is false, and so the theorem is true.

3.26. Prove the following equivalent formulation of the Schroeder–Bernstein Theorem 3.5:

Suppose $X \supseteq Y \supseteq X_1$ and $X \simeq X_1$. Then $X \simeq Y$.

Since $X \simeq X_1$ there exists a one-to-one correspondence (bijection) $f: X \to X_1$ Since $X \supseteq Y$, the restriction of f to Y, which we also denote by f, is also one-to-one. Let $f(Y) = Y_1$. Then Y and Y_1 are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

and $f: Y \to Y_1$ is bijective. But now $Y \supseteq X_1 \supseteq Y_1$ and $Y \simeq Y_1$. For similar reasons, X_1 and $f(X_1) = X_2$ are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

and $f: X_1 \to X_2$ is bijective. Accordingly, there exist equipotent sets $X, X_1, X_2, \ldots$ and equipotent sets $Y, Y_1, Y_2, \ldots$ such that

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2 \supseteq Y_2 \supseteq X_3 \supseteq Y_3 \supseteq \cdots$$

and $f: X_k \to X_{k+1}$ and $f: Y_k \to Y_{k+1}$ are bijective.

Let

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Then

$$X = (X \backslash Y) \cup (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup \cdots \cup B$$
$$Y = (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup (Y_1 \backslash X_2) \cup \cdots \cup B$$

Furthermore, $X \backslash Y$, $X_1 \backslash Y_1$, $X_2 \backslash Y_2, \ldots$ are equipotent. In fact, the function

$$f : (X_k \backslash Y_k) \to (X_{k+1} \backslash Y_{k+1})$$

is one-to-one and onto.

Consider the function $g: X \to Y$ defined by the diagram in Fig. 3-11. That is,

$$g(x) = \begin{cases} f(x) & \text{if } x \in X_k \backslash Y_k \text{ or } x \in X \backslash Y \\ x & \text{if } x \in Y_k \backslash X_k \textit{ or } x \in B \end{cases}$$

Then g is one-to-one and onto. Therefore $X \simeq Y$.

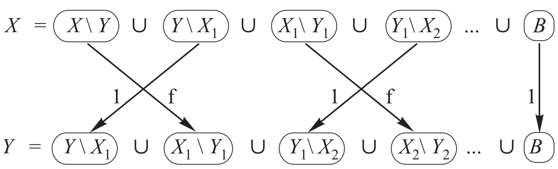


Fig. 3-11

Supplementary Problems

FUNCTIONS

3.27. Let $W = \{a, b, c, d\}$. Decide whether each set of ordered pairs is a function from W into W.

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

3.28. Let $V = \{1, 2, 3, 4\}$. For the following functions $f: V \to V$ and $g: V \to V$, find:

(a) $f \circ g$; (b), $g \circ f$; (c) $f \circ f$:

$$f = \{(1, 3),\ (2, 1),\ (3, 4),\ (4, 3)\} \quad \text{and} \quad g = \{(1, 2),\ (2, 3),\ (3, 1),\ (4, 1)\}$$

3.29. Find the composition function $h \circ g \circ f$ for the functions in Fig. 3-9.

ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

3.30. Determine if each function is one-to-one.

(a) To each person on the earth assign the number which corresponds to his age.
(b) To each country in the world assign the latitude and longitude of its capital.
(c) To each book written by only one author assign the author.
(d) To each country in the world which has a prime minister assign its prime minister.

3.31. Let functions *f*, *g*, *h* from $V = \{1, 2, 3, 4\}$ into *V* be defined by: $f(n) = 6 - n$, $g(n) = 3$, $h = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Decide which functions are:

(a) one-to-one; (b) onto; (c) both; (d) neither.

3.32. Let functions *f*, *g*, *h* from **N** into **N** be defined by $f(n) = n + 2$, (b) $g(n) = 2^n$; $h(n) =$ number of positive divisors of n. Decide which functions are:

(a) one-to-one; (b) onto; (c) both; (d) neither; (e) Find $h'(2) = \{x | h(x) = 2\}$.

3.33. Decide which of the following functions are: (a) one-to-one; (b) onto; (c) both; (d) neither.

(1) f: $\mathbf{Z}^2 \to \mathbf{Z}$ where $f(n, m) = n - m$; (3) h: $\mathbf{Z} \times (\mathbf{Z}\backslash 0) \to \mathbf{Q}$ where $h(n, m) = n/m$;
(2) g: $\mathbf{Z}^2 \to \mathbf{Z}^2$ where $g(n, m) = (m, n)$; (4) k: $\mathbf{Z} \to \mathbf{Z}^2$ where $k(n) = (n, n)$.

3.34. Let f: $\mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 3x - 7$. Find a formula for the inverse function f^{-1}: $\mathbf{R} \to \mathbf{R}$.

3.35. Consider permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ in S_6.

Find: (a) $\tau \circ \sigma$; (b) $\sigma \circ \tau$; (c) σ^2; (d) σ^{-1}; (e) τ^{-1}

PROPERTIES OF FUNCTIONS

3.36. Prove: Suppose f: $A \to B$ and g: $B \to A$ satisfy $g \circ f = 1_A$. Then *f* is one-to-one and *g* is onto.

3.37. Prove Theorem 3.1: A function f: $A \to B$ is invertible if and only if *f* is both one-to-one and onto.

3.38. Prove: Suppose f: $A \to B$ is invertible with inverse function f^{-1}: $B \to A$. Then $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$.

3.39. Suppose f: $A \to B$ is one-to-one and $g : A \to B$ is onto. Let x be a subset of A.

(a) Show $f 1_x$, the restriction of f to x, is one-to-one.
(b) Show $g 1_x$, need not be onto.

3.40. For each $n \in \mathbf{N}$, consider the open interval $A_n = (0, 1/n) = \{x \mid 0 < x < 1/n\}$. Find:

(a) $A_2 \cup A_8$; (c) $\cup(A_i \mid i \in J)$; (e) $\cup(A_i \mid i \in K)$;
(b) $A_3 \cap A_7$; (d) $\cap(A_i \mid i \in J)$; (f) $\cap(A_i \mid i \in K)$.

where *J* is a finite subset of **N** and **K** is an infinite subset of **N**.

3.41. For each $n \in N$, let $D_n = \{n, 2n, 3n, \ldots\} = \{\text{multiples of } n\}$.

(a) Find: (i) $D_2 \cap D_7$; (ii) $D_6 \cap D_8$; (iii) $D_3 \cap D_{12}$; (iv) $D_3 \cup D_{12}$.
(b) Prove that $\cap(D_i | i \in K) = \emptyset$ where *K* is an infinite subset of **N**.

3.42. Consider an indexed class of sets $\{A_i \mid i \in I\}$, a set **B** and an index i_0 in I.
Prove: (a) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$; (b) $\cap (A_i \mid i \in I) \subseteq A_{i_0} \subseteq \cup(A_i \mid i \in I)$.

CARDINAL NUMBERS

3.43. Find the cardinal number of each set: (a) $\{x \mid x$ is a letter in "BASEBALL"$\}$;
(b) Power set of $A = \{a, b, c, d, e\}$; (c) $\{x \mid x^2 = 9, 2x = 8\}$.

3.44. Find the cardinal number of:

(a) all functions from $A = \{a, b, c, d\}$ into $B = \{1, 2, 3, 4, 5\}$;

(b) all functions from P into Q where $|P| = r$ and $|Q| = s$;

(c) all relations on $A = \{a, b, c, d\}$;

(d) all relations on P where $|P| = r$.

3.45. Prove:

(a) Every infinite set A contains a denumerable subset D.

(b) Each subset of a denumerable set is finite or denumerable.

(c) If A and B are denumerable, then $A \times B$ is denumerable.

(e) The set **Q** of rational numbers is denumerable.

3.46. Prove: (a) $|A \times B| = |B \times A|$; (b) If $A \subseteq B$ then $|A| \leq |B|$; (c) If $|A| = |B|$ then $P(A)| = |P(B)|$.

SPECIAL FUNCTIONS

3.47. Find: (a) $\lfloor 13.2 \rfloor$, $\lfloor -0.17 \rfloor$, $\lfloor 34 \rfloor$; (b) $\lceil 13.2 \rceil$, $\lceil -0.17 \rceil$, $\lceil 34 \rceil$.

3.48. Find:

(a) $29 \pmod 6$; (c) $5 \pmod{12}$; (e) $-555 \pmod{11}$.

(b) $200 \pmod{20}$; (d) $-347 \pmod 6$;

3.49. Find: (a) $3! + 4!$; (b) $3!(3! + 2!)$; (c) $6!/5!$; (d) $30!/28!$.

3.50. Evaluate: (a) $\log_2 16$; (b) $\log_3 27$; (c) $\log_{10} 0.01$.

MISCELLANEOUS PROBLEMS

3.51. Let n be an integer. Find $L(25)$ and describe what the function L does where L is defined by:

$$L(n) = \begin{cases} 0 & \text{if } n = 1 \\ L(\lfloor n/2 \rfloor) + 1 & \text{if } n > 1 \end{cases}$$

3.52. Let a and b be integers. Find $Q(2, 7)$, $Q(5, 3)$, and $Q(15, 2)$, where $Q(a, b)$ is defined by:

$$Q(a, b) = \begin{cases} 5 & \text{if } a < b \\ Q(a - b,\ b + 2) + a & \text{if } a \geq b \end{cases}$$

3.53. Prove: The set P of all polynomials $p(x) = a_0 + a_1 x + \cdots + a_x^m$ with integral coefficients (that is, where $a_0, a_1, \ldots, a_m$ are integers) is denumerable.

Answers to Supplementary Problems

3.27. (a) Yes; (b) No; (c) Yes; (d) No.

3.28. (a) $\{(1, 1), (2, 4), (3, 3), (4, 3)\}$;
(b) $\{(1, 1), (2, 2), (3, 1), (4, 1)\}$;
(c) $\{(1, 4), (2, 3), (3, 3), (4, 4)\}$.

3.29. $\{(a, 4), (b, 6), (c, 4)\}$

3.30. (a) No, (b) yes, (c) no, (d) yes.

3.31. (a) f, h; (b) f, h; (c) f, h; (d) g.

3.32. (a) f, g; (b) h; (c) none; (d) none; (e) {all prime numbers}.

3.33. (a) g, k; (b) f, g, h; (c) g; (d) none.

3.34. $f^{-1}(x) = (x + 7)/3$

3.35. (a) 425631; (b) 416253; (c) 534261; (d) 415623; (e) 453261.

3.40. (a) A_2; (b) A_7; (c) A_r where r is the smallest integer in J; (d) A_s where s is the largest integer in J; (e) A_r where r is the smallest integer in K; (f) Ø.

3.41. (i) D_{14}; (ii) D_{24}; (iii) D_{12} (iv) D_3.

3.43. (a) 5; (b) $2^5 = 32$; (c) 0.

3.44. (a) $5^4 = 625$; (b) s^r; (c) $2^{16} = 65\ 536$; (d) 2.

3.47. (a) 13, −1, 34; (b) 14, 0, 34.

3.48. (a) 5; (b) 0; (c) 2; (d) $6 - 5 = 1$; (e) $11 - 5 = 6$.

3.49. (a) 30; (b) 48; (c) 6; (d) 870.

3.50. (a) 4; (b) 3; (c) −2.

3.51. $L(25) = 4$. Each time n is divided by 2, the value of L is increased by 1. Hence L is the greatest integer such that $2^L < N$. Thus $L(n) = \lfloor \log_2 n \rfloor$.

3.52. $Q(2, 7) = 5$, $Q(5, 3) = 10$, $Q(15, 2) = 42$.

3.53. Hint: Let P_k denote the set of polynomials $p(x)$ such that $m \leq k$ and each $|a_i| \leq k$. P_k is finite and $P = \cup_k P_k$.