DISCRETE MATHEMATICS
（离散数学）

云南大学数学系
李 建 平

Chapter 5 FUNCTIONS

5.1 FUNCTIONS (函数)

Let A and B be nonempty sets. A **function** f from A to B, which is denoted f: A→B, is a relation from A to B such that for all x∈Dom(f), the f-relative set of x, say f(x), contains just one element of B. The relation f can then be described as the set of pairs {(a,f(a)) | a∈Dom(f)}. Functions are also called **mappings** or **transformations**(变换). The element a is called an **argument** of the function f, and f(a) is called the **value** of the function for the argument a and is also referred to as the **image** of a under f.

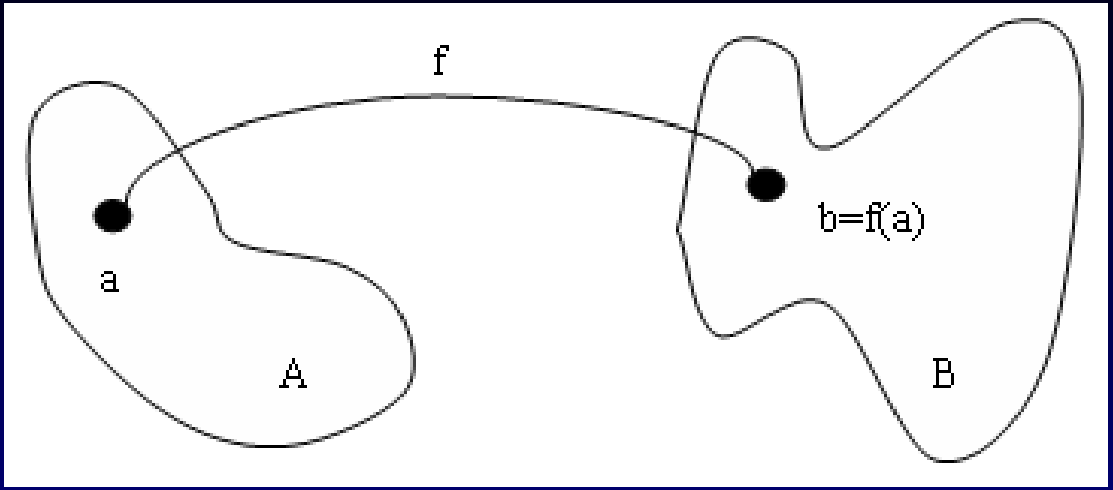

Figure 5.1

Let A be an arbitrary nonempty set. The **identity function** on A, denoted by 1_A, is defined by $1_A(a)=a$.

Suppose that f: A→B and g: B → C are functions. Then the composition of f and g, $g \circ f$ (see Section 4.7), is a relation. Thus each set $(g \circ f)(a)$, for a in

Dom(g∘f), contains just one element of C, so g∘f is a function. This is illustrated diagrammatically in Figure 5.3.

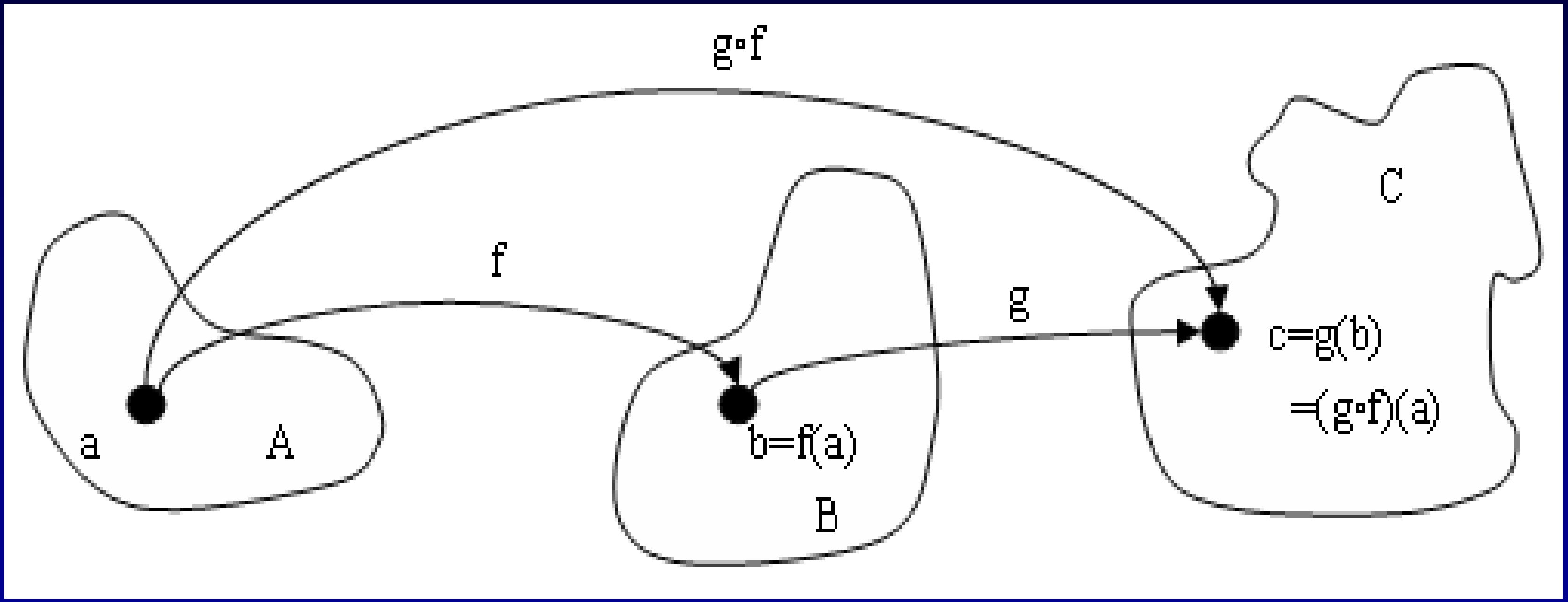

Figure 5.3

Special Types of Functions

Let f be a function from A to B. Then we say that f is **everywhere defined** if Dom(f)=A. We say that f is **onto** if Ran(f)=B. Finally, we say that f is **one to one** if we cannot have f(a)=f(a') for two distinct elements a and a' of A. The definition of one to one may be restated in the following equivalent form:

If f(a)=f(a'), then a=a'.

If f: $A \to B$ is a one-to-one function, then f associates to each element a of Dom(f) an element b=f(a) of Ran(f). Every b in Ran(f) is matched, in this way, with one and only one element of Dom(f). Such an f is often called a **bijection** between Dom(f) and Ran(f). If f is also everywhere defined and onto, then f is called a **one-to-one correspondence between A and B**.

Let R be the set of all equivalence relations on a given set A, and let Π be the set of all partitions on A. Then we can define a function f: $R\rightarrow\Pi$ as follows. For each equivalence relation R on A, let f(R)=A/R, the partition of A that corresponds to R. The discussion in Section 4.5 shows that f is one-to-one correspondence between R and Π.

- Invertible Functions (可逆函数)

A function f: A→B is said to be **invertible** if its inverse relation, f^{-1}, is also a function.

Theorem 1: Let f: A→B be a function.

(a) Then f^{-1} is a function from B to A if and only if f is one to one.

If f^{-1} is a function, then

(b) the function f^{-1} is also one to one.

(c) f^{-1} is everywhere defined if and only if f is onto.

(d) f^{-1} is onto if and only if f is everywhere defined.

Proof

(a) We prove the following equivalent statement.

F^{-1} is not a function if and only if f is not one to one.

Suppose first that f^{-1} is not a function. Then, for some b in B, $f^{-1}(b)$ must contain at least two distinct elements, a_1 and a_2. Then $f(a_1)=b=f(a_2)$, so f is not one to one.

Conversely, suppose that f is not one to one. Then $f(a_1)=f(a_2)=b$ for two distinct elements a_1 and a_2 of A. Thus $f^{-1}(b)$ contains both a_1 and a_2, so f^{-1} cannot be a function.

(b) Since $(f^{-1})^{-1}$ is the function f, part (a) shows that

f^{-1} is one to one.

(c) Recall that $Dom(f^{-1})=Ran(f)$. Thus $B=Dom(f^{-1})$ if and only if $B=Ran(f)$. In other words, f^{-1} is everywhere defined if and only if f is onto.

(d) Since $Ran(f^{-1})=Dom(f)$, $A=Dom(f)$ if and only if $A=Ran(f^{-1})$. That is, f is everywhere defined if and only if f^{-1} is onto.

Note also that if $f: A\rightarrow B$ is a one-to-one function, then the equation $b=f(a)$ is equivalent to $a=f^{-1}(b)$.

Theorem 2: Let $f: A \rightarrow B$ be any function. Then

(a) $1_B \circ f = f$.

(b) $f \circ 1_A = f$.

If f is a one-to-one correspondence between A and B, then

(c) $f^{-1} \circ f = 1_A$.

(d) $f \circ f^{-1} = 1_B$.

Theorem 3

(a) Let $f: A \rightarrow B$ and $g: B \rightarrow A$ be functions such that $g \circ f = 1_A$ and $f \circ g = 1_B$. Then f is a one-to-one correspondence between A and B, g is a one-to-one correspondence between B and A, and each is the inverse of the other.

(b) Let $f: A \rightarrow B$ and $B \rightarrow C$ be invertible. Then $g \circ f$ is invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Theorem 4: Let A and B be two **finite** sets with the same number of elements, and let $f: A \rightarrow B$ be an everywhere defined function.

(a) If f is one to one, then f is onto.

(b) If f is onto, then f is one to one.

5.2 FUNCTIONS FOR COMPUTER SCIENCE

Let A be a subset of the universal set $U=\{u_1, u_2, \ldots, u_n\}$. The **characteristic function** of A is defined as a function from U to {0,1} by the following:

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

If $A=\{4,7,9\}$ and $U=\{1,2,3,\ldots,10\}$, then $f_A(2)=0$, $f_A(4)=1$, $f_A(7)=1$, and $f_A(12)$ is undefined. It is easy to check that f_A is everywhere defined and onto, but is not one to one.

We defined a family of **mod-n** functions, one for each positive integer n. Each f_n is a function from the nonnegative integers to the set {0,1,2,3,…,n-1}. For a fixed n, any nonnegative integer z can be written as $z=kn+r$ with $0 \leqslant r \leqslant n$. Then $f_n(z)=r$.

(a) Let A be a finite set and define l: $A^* \to Z$ as $l(w)$ is the length of the string w (see Section 1.3 for the definition of A* and strings).

(b) Let B be a finite subset of the universal set U and define *pow*(B) to be the power set of B. Then *pow* is a function from V, the power set of U, to the power set of V.

5.3 GROWTH OF FUNCTIONS

Let f and g be functions whose domains are subsets of Z^+, the positive integers. We say that f is O(g), read “f is big-Oh of g” , if there exist constants c and k such $|f(n)| \leqslant c \cdot |g(n)|$ for all $n \geqslant k$. If f is O(g), then f grows no faster than g does.

We say that f and g have the **same order** if f is O(g) and g is O(f).

We define a relation Θ , big-theta, on functions whose domains are subsets of Z^+ as f Θg if and only if f and g have the same order.

Theorem 1: The relation Θ, big-theta, is an equivalence relation.

Proof: Clearly, Θ is reflexive since every function has the same order as itself. Because the definition of same order treats f and g in the same way, this definition is symmetric and the relation Θ is symmetric.

To see that Θ is transitive, suppose f and g have the same order. Then there exist c_1 and k_1 with $|f(n)| \leqslant c_1 \cdot |g(n)|$ for all $n \geqslant k_1$, and there exist c_2 and k_2 with $|g(n)| \leqslant c_2 \cdot |f(n)|$ for all $n \geqslant k_2$. Suppose that g and h have the same order, then there exist c_3, k_3

with $|g(n)| \leqslant c_3 \cdot |h(n)|$ for all $n \geqslant k_3$, and there exist c_4, k_4 with $|h(n)| \leqslant c_4 \cdot |g(n)|$ for all $n \geqslant k_4$.

Then $|f(n)| \leqslant c_1 \cdot |g(n)| \leqslant c_1(c_3 \cdot |h(n)|)$ if $n \geqslant k_1$ and $n \geqslant k_3$. Thus $|f(n)| \leqslant c_1 c_3 \cdot |h(n)|$ for all $n \geqslant \max\{k_1, k_3\}$.

Similarly, $|h(n)| \leqslant c_2 c_4 \cdot |f(n)|$ for all $n \geqslant \max\{k_2, k_4\}$.

Thus f and h have the same order and Θ is transitive.

- Rules for Determining the Θ-Class of a Function

1. $\Theta(1)$ functions are constant and have zero growth, the slowest growth possible.
2. $\Theta(\lg(n))$ is lower than $\Theta(n^k)$ if $k>0$. This means

that any logarithmic function grows more slowly than any power function with positive exponent.

3. $\Theta(n^a)$ is lower than $\Theta(n^b)$ if and only if $0<a<b$.
4. $\Theta(a^n)$ is lower than $\Theta(b^n)$ if and only if $0<a<b$.
5. $\Theta(n^k)$ is lower than $\Theta(a^n)$ for any power n^k and any $a>1$. This means that any exponential function with base greater than 1 grows more rapidly than any power function.
6. If r is not zero, then $\Theta(rf)=\Theta(f)$ for any function f.
7. If h is a nonzero function and $\Theta(f)$ is lower than (or the same as) $\Theta(g)$, then $\Theta(fh)$ is lower than (or the same as) $\Theta(gh)$.
8. If $\Theta(f)$ is lower than $\Theta(g)$, then $\Theta(f+g)=\Theta(g)$.

The Θ–class of a function that describes the number of steps performed by an algorithm is frequently referred to as the **running time**（运行时间） or the computational complexity（计算复杂性） of the algorithm. For example, the algorithm TRANS has an average running time of n^3.

5.4 PERMTATION FUNCTIONS

A bijection from a set A to itself is called a **permutation**（置换）of A.

If $A=\{a_1, a_2, \ldots, a_n\}$ is a finite set and p is a bijection on A, we list the elements of A and the corresponding function values $p(a_1), p(a_2), \ldots, p(a_n)$ in the following form:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}.$$

We often write

$$p=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{pmatrix}.$$

Theorem 1: If $A=\{a_1, a_2,\ldots, a_n\}$ is a set containing n elements, then there are

$$n!=n\cdot(n-1)\cdot\cdot\cdot 2\cdot 1 \quad \text{permutations of } A.$$

Let $b_1,b_2,\ldots,b_r$ be r distinct elements of the set $A=\{a_1, a_2,\ldots, a_n\}$. The permutation $p: A\to A$ defined by

$$p(b_1)=b_2$$
$$p(b_2)=b_3$$
$$\cdots$$
$$p(b_{r-1})=b_r$$
$$p(b_r)=b_1$$
$$p(x)=x, \text{ if } x\in A \text{ and } x\notin\{b_1,b_2,\ldots,b_r\},$$

is called a **cyclic permutation**（循环置换或轮换） of length r, or simply a **cycle** of length r, and will be denoted by $(b_1,b_2,\ldots,b_r)$.

Two cycles of a set A are said to be **disjoint** if no element of A appears in both cycles.

Theorem 2: A permutation of a finite set that is not the identity or a cycle can be written as a product of disjoint cycles of length $\geqslant 2$.

It is not difficult to show that in Theorem 2, when a permutation is written as a product of disjoint cycles, the product is unique except for the order of the cycles.

Even and Odd Permutations

A cycle of length 2 is called a **transposition** （对换）,i.e., a transposition is a cycle $p(a_i,a_j)$, where $p(a_i)=p_j$ and $p(a_j)=a_i$. Then $p\circ p=1_A$.

Every cycle can be written as a product of transpositions:

$$(b_1,b_2,\ldots,b_r)= (b_1,b_r)\circ(b_1,b_{r-1})\circ\cdots\circ(b_1,b_3)\circ(b_1,b_2).$$

This case be verified by induction on r, as follows:

Basis Step: If r=2, then the cycle is just (b_1,b_2), which already has the proper form.

Induction Step: We use P(k) to show P(k+1). Let $(b_1,b_2,\ldots,b_k,b_{k+1})$ be a cycle of length k+1. Then $(b_1,b_2,\ldots,b_k,b_{k+1})= (b_1,b_{k+1})\circ(b_1,b_2,\ldots,b_k)$, as may be verified by computing the composition. Using P(k), $(b_1,b_2,\ldots,b_k)= (b_1,b_r)\circ(b_1,b_{k-1})\circ\cdots\circ(b_1,b_2)$. Thus, by substitution,

$(b_1,b_2,\ldots,b_{k+1})= (b_1,b_{k+1})\circ(b_1,b_k)\circ\cdots\circ(b_1,b_3)\circ(b_1,b_2)$.

This completes the induction step. Thus, by the principle of mathematical induction, the result holds for every cycle.

Example $(1,2,3,4,5)= (1,5)\circ(1,4)\circ(1,3)\circ(1,2)$.

We obtain the following corollary of Theorem 2.

Corollary 1: Every permutation of a finite set with at least two elements can be written as a product of transpositions.

Theorem 3: If a permutation of a finite set can be written as a product of an even number of transpositions, then it can never be written as a product of an odd number of transpositions, and conversely.

A permutation of a finite set is called **even** if it can be written as a product of an even number of transpositions, and it is called **odd** if it can be written as a product of an odd number of transpositions.

Theorem 4: Let be a finite set with n elements, $n \geqslant 2$. There are $n!/2$ even permutations and $n!/2$ odd permutations.

Proof: Let A_n be the set of all even permutations of A, and let B_n be the set of all odd permutations. We shall define a function $f: A_n \to B_n$, which we show is one to one and onto, and this will show that A_n and B_n have the same number of elements.

Since $n \geqslant 2$, we can choose a particular transposition q_0 of A. Say that $q_0=(a_{n-1},a_n)$. We now define the function $f: A_n \to B_n$ by

$$f(p)= q_0 \circ p,\ p \in A_n.$$

Observe that if $p \in A_n$, then p is an even permutation, so is an odd permutation and thus $f(p) \in B_n$. Suppose now that p_1 and p_2 are in A_n and

$$f(p_1)=f(p_2).$$

Then

$$q_0 \circ p_1 = q_0 \circ p_2. \qquad (2)$$

We now compose each side of equation (2) with q_0:

$$q_0 \circ (q_0 \circ p_1) = q_0 \circ (q_0 \circ p_2);$$

so, by the associative property,

$$(q_0 \circ q_0) \circ p_1 = (q_0 \circ q_0) \circ p_2$$

or, since $q_0 \circ q_0 = 1_A$,

$$1_A \circ p_1 = 1_A \circ p_2, \quad p_1 = p_2.$$

Thus f is one to one.

Now let $q \in B_n$. Then ,and

$$f(q_0 \circ q)=q_0 \circ (q_0 \circ q)=(q_0 \circ q_0) \circ q=1_A \circ q=q,$$

which means that f is an onto function. Since $f: A_n \to B_n$ is one to one and onto, we conclude that A_n and B_n have the same number of elements. Note that $A_n \cap B_n = \emptyset$ since no permutation can be both even and odd. Also, by Theorem 1, $|A_n \cup B_n| = n!$. Thus, by Theorem 2 of Section 1.2,

$$n!=|A_n \cup B_n|= |A_n|+|B_n|-|A_n \cap B_n|=2|A_n|.$$

We then have $|A_n| = |B_n| = \dfrac{n!}{2}.$

The end !